An Introduction to Algebraic Number Theory through Olympiad Problems

Elias Caeiro

Foreword

Here is a quick summary of how this book came to be. In July 2019, I attended a class by Gabriel Dospinescu where he exposed a bit of algebraic number theory (roughly chapter 1 of this book). Amazed by what I had seen, I started reading a bit of Ireland-Rosen [11] and in late 2019, the thought of writing a handout inspired by the content of Gabriel's class for the website https://mathraining.be crossed my mind. I submitted a first version in July 2020. Then, in March 2021, I had to make a few corrections. At that time, I knew significantly more than when I first wrote it, so I realised while doing these corrections that there was so much more that I wanted to add but couldn't (due to lack of space). This became the present book; which I wrote during the summer 2021 of my last year of high school.

This book is intended to serve as a transition from olympiads to higher mathematics, for high school students who are interested in learning more advanced theory but find regular textbooks too different from olympiads. **I stress that this book is not an efficient way to prepare for mathematical olympiads**.[1] As such, there is hardly any prerequisite[2], apart from some amount of (olympiad) mathematical maturity. Accordingly, there is an appendix providing background on polynomials at the end of the book. Most of the content of the first section should be familiar to the reader, but I still recommend to skim through it quickly to have a firm footing on the technicalities (e.g. a polynomial is not a polynomial function).[3] The second section of this appendix is dedicated to introducing notions of abstract algebra: no theory will be introduced there, it serves both as a way to explain what morphisms are and as a reference for the definitions of the algebraic structures which will be used throughout this book (you should not try to remember the actual algebraic structures, only the intuitive concept of a morphism).

I was aware of some excellent books on algebraic number theory (and related subjects) which helped me visualise how I wanted this book to be: Andreescu and Dospinescu's *Problems from The Book* [1] (PFTB) and *Straight from The Book* (SFTB) [2], Ireland and Rosen's *A Classical Introduction to Modern Number Theory* [11], and Murty's *Problems in Algebraic Number Theory* [19]. Here is a small summary of these books: PFTB presents miscellaneous mathematical gems in an (advanced) olympiad style, and SFTB has solutions to the first 12 chapters and amazing expositions of advanced topics in addenda. Ireland-Rosen discusses a wide variety of number theoretic topics with an algebraic flavor, and Murty is a classical first semester course in algebraic number theory but written from a problem-solving oriented approach. The problems in Ireland-Rosen are generally easier than the ones in PFTB, SFTB, and Murty.

As a consequence, I have tried to limit the intersection of the present book with these ones, since the exposition there was already extraordinary. Therefore, I strongly encourage the reader to have a look at them too. I particularly recommend the addenda 3B, 7A and 9B[4] of SFTB, chapter 9 and 13 on algebraic number theory and the geometry of numbers of PFTB as well as the chapters 8 and 9 on Gauss and Jacobi sums and on cubic and biquadratic reciprocity of Ireland-Rosen as they are particularly similar to the topics of this book, but of course one should read all of the chapters if possible.

[1] Except maybe chapters 3 and 5 on cyclotomic polynomials and polynomial number theory.

[2] If I had to state them, maybe the chinese remainder theorem, Fermat's little theorem, modular arithmetic, complex numbers, and the binomial expansion?

[3] It doesn't hurt to read it quickly even if you think you know everything, at best you learn something new, at worst you lose a few minutes (and there are cool exercises!).

[4] I have personally found 9A to be too dense for me (before reading Murty).

One could, for instance, read this book along with the the addenda from SFTB, and then start with Murty and Ireland-Rosen as they are a bit more abstract (although Ireland-Rosen starts very gently). This choice is also motivated by the fact that Murty (and some chapters of PFTB/SFTB) makes a fair use of linear algebra, which I have included an appendix on; for this reason as well as because it is useful in a fair amount of exercises. In a sense, this book can be thought as a prequel to Murty, and one should have (almost[5]) all the necessary prerequisites after finishing it. In particular, at no point[6] do I mention *ideals*, even though they are fundamental in algebraic number theory. As a consequence, some problems which are solved by tricky uses of the fundamental theorem of symmetric polynomials can be solved more easily with ideal theory. I hope this will not affect the reader once they learn ideal theory.

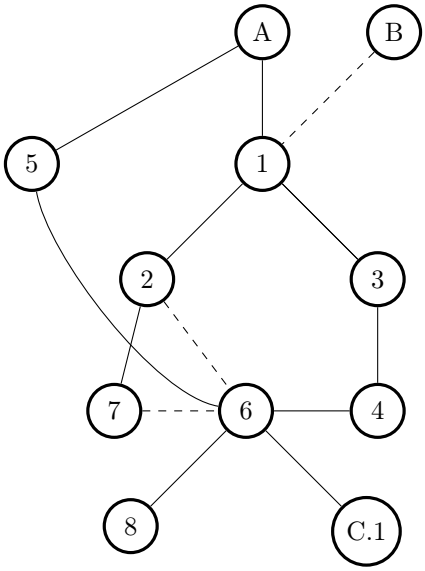
I will now talk more about the book itself. Chapter 1, which roughly corresponds to the Mathraining version of the book, starts with general definitions and properties of algebraic numbers. It also roughly corresponds to the chapter of PFTB[7]. I don't actually have much more to say briefly about the chapters than what the table of contents does, so I will focus on the last two appendices, on symmetric polynomials and linear algebra. Symmetric polynomials, and above all the fundamental theorem of symmetric polynomials, are used everywhere in the book. The knowledge of the proofs of these results however is not strictly required to progress through the book. I have thus arranged them in an appendix which the reader can read when they want (personally I recommend after reading the first chapter).

Regarding the appendix on linear algebra, I would recommend reading it after chapter 1 too, but since it is rather long, one can, say, read one section after each chapter. The first section on vector spaces and bases is fundamental and is necessary for chapter 6 on field theory. I would also recommend reading it before chapter 4 on finite fields since it is used to give a quick proof of the fact that the cardinality of a finite field is a power of a prime. Section 2 on linear maps is less important, but it cannot be skipped because this is where matrices are defined and where some properties of these matrices are established. Section 3 on determinants is extremely important and rather long; I suggest to first look at applications of the determinant and then have a more careful look at its construction. Section 4 uses the results of section 2 and 3 to derive the formula for linear recurrences. Since **many** exercises are about linear recurrences, this has to be seen in the beginning, even if one does not read the proof. Here is a diagram of chapter dependencies. Dashed lines indicate non-strict dependencies (some facts from the previous chapter might be used, or the previous chapter might provide some additional motivation, but it is still understandable without it). There is a weak dependency between 6 and 7 because some notations and results of chapter 6 will be used, but only in the last section, Section 7.4. Also, note that there is one forward dependency: in Section 7.4: at the end of the proof of the main result, one result from Chapter 8 is used. (This is intentional. Readers should not read Chapter 7 before Chapter 6. More generally, I think the best course of action is to read this book in order.)

[5]There might still be a few things which need a bit of googling, but they should not take too long to grasp. There is also some real analysis and geometry involved, mainly for the geometry of numbers part, but I trust the reader will manage (PFTB has a great chapter on the geometry of numbers which can be used to introduced the subject).

[6]Except in some remarks or footnotes.

[7]Along with section 1 of chapter 4 on the Frobenius morphism.



Finally, here are some miscellaneous remarks about the layout of the book. The layout of the theorems etc. comes from Mathraining. Murty has also inspired me a lot: I have followed its style of leaving parts of the theory as exercises for the reader. These exercises will be written in purple and in smaller font. This serves two purposes at once: it keeps the exposition neater (for instance it is easier to see the main ideas of a proof) and keeps the reader active in the learning process. Some of these purple exercises will have a star near them, this means that they are part of the theory. **In that case, they cannot be skipped**. Otherwise, it is usually an additional remark about an object that will not be important for the rest of the book but still good to do. Purple exercises are generally easy. They are all corrected at the end of the book to avoid the reader getting stuck at an early stage due to a misunderstanding[8]. The solutions are deliberately not linked to the exercises to encourage the reader to try them and not read the solution directly. However, the reader is encouraged to read the solutions to the exercises they had trouble with, and particularly so for the vagues ones such as the ones about motivation.

Similarly, a star after a proposition or corollary means that it's an important result.

Now, here are a few remarks about the supplementary exercises at the end of the chapters, i.e. black exercises. Some of these are pretty hard, so it is fine to move on to another chapter without having solved them all (or even almost none of them, it is not a problem[9]) and come back later. A dagger at the right of an exercise indicates that it is particularly instructive, beautiful, or interesting. These are all corrected at the end of the book. The exercises can also be seen as a companion to the theory: many exercises are theorems or classical results. If an exercise doesn't seem nice enough to attempt it, but nice enough to want to know the solution, it's fine[10] to read it without trying the problem. Also, I strongly encourage the reader to read the solutions at the end after solving an exercise: multiple solutions are often given so you may still learn something new.

I have decided to include all the objects which are defined in the book in the index at the end of it. This means that I cannot put all the occurences of words like "algebraic number" which are used almost everywhere. For such words, I chose to include the first occurence of the word where it's defined, as well as some more exotic occurences (e.g. embeddings arise everywhere in chapter 6 on field theory but are pretty rare in the other chapters so I have included all the later occurences). If words can appear in two indices, I chose to put them in both. For instance, "quadratic unit" appears both in the index for "quadratic" and the one for "unit". Another initiative I have taken is that I do not include words appearing in the solutions in the index unless they do not appear near the original exercise.

[8] Being implemented.

[9] Of course, I still recommend to try them.

[10] But don't do that too much! This is for exercises like the fact that a Galois extension L/K is solvable if and only if its Galois group is: it's a very nice result, but it has very little to do with number theory so it's understandable if you feel lazy.

There are a few notations or abbreviations which are not completely standard that I haven't defined in the book. The reader shall find a table with the notations of this book in the next section, but here they are for the sake of convenience. I use LHS and RHS to denote "left-hand side" and "right-hand side", $[n]$ to denote the set of integers from 1 to n and $:=$ to define an object. When S is a set and a an element of some ring, I use aS to denote $\{as \mid s \in S\}$. Similarly, $U+V$ and UV mean $\{u+v \mid u \in U, v \in V\}$ and $\{uv \mid u \in U, v \in V\}$.

Now comes the time of the acknowledgements. As I said in the beginning of the foreword, this book could not have existed without the classes of Gabriel Dospinescu and Bodo Lass at the Club de Mathématiques Discrètes in Lyon. I want to thank Nicolas Radu as well, the creator of Mathraining, for his very valuable comments on the Mathraining version. I also thank everyone involved in the French Olympiad Mathematics Preparation as well as in the website https://mathraining.be, for making me discover (olympiad) mathematics. Lastly, many thanks to Lucas Nistor for patching up solutions that should work but don't as well as to Vladimir Ivanov and Alexis Miller for their very careful proofreading[11].

Finally, I am still very inexperienced so I apologise in advance for all the poor expositions and mistakes in this book! In particular, I would be very grateful if you could email all the mistakes and typos you find as well as any suggestion you have (for instance, a very nice alternative solution to an exercise, or a better way to present the motivation of a solution) to caeiro.elias11@gmail.com (or pm me on AoPS or discord depending on where you found this book). The dropbox link should always be (mostly) up to date. The advantage is that you will always have the last version, but the drawback is that the numbering of theorems, etc. and results may change with time, because I add content thematically.

Paris — Elias Caeiro
October 2

[11] If you still see many mistakes, it means that they haven't finished proofreading the whole book yet, or that there were so many mistakes that they couldn't catch them all. The latter is probably true in all cases.

Notations

Sets

- $[\![a, b]\!]$: the set of integers $[a, b] \cap \mathbb{Z}$ between a and b.
- $[n]$: the set of integers $[\![1, n]\!]$ between 1 and n.
- $\mathbb{N}$: the set of natural integers $\{0, 1, 2, \ldots\}$.
- $\mathbb{N}^*$: the set of positive integers $\{1, 2, 3, \ldots, \}$.
- $\mathbb{Z}$: the ring of rational integers.
- $\mathbb{Q}$: the field of rational numbers.
- $\overline{\mathbb{Z}}$: the ring of algebraic integers.
- $\overline{\mathbb{Q}}$: the field of algebraic numbers.
- $\mathbb{H}$: the skew field of quaternions.
- H: the ring of Hurwitz integers.
- $\mathbb{F}_q$: the field with q elements.
- $\mathbb{Z}_p$: the ring of p-adic integers.
- $\mathbb{Q}_p$: the field of p-adic numbers.
- $\mathbb{Z}/n\mathbb{Z}$: $\mathbb{Z}$ modulo n.
- $R[\alpha_1, \ldots, \alpha_n]$: the ring of polynomial expressions in $\alpha_1, \ldots, \alpha_n$ with coefficients in R.
- $K(\alpha_1, \ldots, \alpha_n)$: the field of rational expressions in $\alpha_1, \ldots, \alpha_n$ (with non-zero denominator) with coefficients in K.
- $\mathcal{O}_K$: the ring of integers $K \cap \overline{\mathbb{Z}}$ of a number field K.
- $\mathfrak{S}_n$: the symmetric group of permutations of $[n]$.
- $R^{m \times n}$: the set of $m \times n$ matrices with coefficients in a commutative ring R. When $n = 1$ we simply write R^m.

Polynomials

- Φ_n: the nth cyclotomic polynomial.
- Ψ_n: the minimal polynomial of $2\cos\left(\frac{2\pi}{n}\right)$.
- e_k: the kth elementary symmetric polynomial.
- p_k: the kth power sum polynomial.

- h_k: the kth complete homogeneous polynomial.
- π_α: the minimal polynomial of an algebraic number α.
- f': the (formal) derivative of a rational function f.
- f^*: the primitive part $f/c(f)$ of $f \in \mathbb{Q}[X]$.

Sequences and Functions

- F_n: the nth Fibonacci number.
- L_n: the nth Lucas number.
- T_n: the nth Tribonacci number.
- $P(n)$: the greatest prime factor of a non-zero rational integer $n \in \mathbb{Z}$.
- $\mu(\cdot)$: the Möbius function.
- $\mathrm{rad}(\cdot)$: the squarefree part of the the prime factorisation of an element in a UFD. For $\mathbb{Z}$ you take it to be positive, for $\mathbb{Q}[X]$ monic and for $\mathbb{Z}[X]$ primitive with positive leading coefficient.
- $c(f)$: the content of a polynomial $f \in \mathbb{Z}[X]$.
- $\mathrm{N}(\alpha)$: the absolute norm of an algebraic number $\alpha \in \overline{\mathbb{Q}}$, i.e. the product of its conjugates.
- $N_{L/K}(\alpha)$: the norm of α in the extension L/K.
- $\overline{\alpha}$: the quadratic conjugate of an element α in a quadratic extension L/K. Without context it is the complex conjugate ($L = \mathbb{C}$ and $K = \mathbb{R}$).
- $\lfloor x \rfloor$: the floor of a real number x, i.e. the greatest integer $n \leq x$.
- $\lceil x \rceil$: the ceiling of a real number x, i.e. the smallest integer $n \geq x$.
- $\Re(z)$: the real part of a complex number $z \in \mathbb{C}$.
- $\Im(z)$: the imaginary part of a complex number $z \in \mathbb{C}$.
- v_p: p-adic valuation.
- $\left(\frac{\cdot}{p}\right)$: the Legendre symbol (or Jacobi symbol when p isn't prime).
- $\binom{n}{k}$: n choose k, the number of ways to select a subset of k elements from a set of n elements, i.e. $\frac{n!}{k!(n-k)!}$.

Algebra

- $|_R$: divides in R.
- $\lceil$: left-divisibility.
- $\rceil$: right-divisibility.
- $R^\times$: the multiplicative group of units of R.
- Frob_R: the Frobenius morphism of R.
- $\mathrm{Emb}_K(L)$: the set of K-embeddings of L.
- $\mathrm{Gal}(L/K)$: the Galois group of L/K.
- $\mathrm{Aut}_K(L) = \mathrm{Aut}(L/K)$: the group of automorphisms of L/K.

- L^H: the fixed field of H.
- $\mathrm{Res}(f, g)$: the resultant of two polynomials f and g.
- ker: the kernel of a morphism.
- im: the image of a morphism.
- det: the determinant of a matrix or a linear map.
- Tr: the trace of a matrix or a linear map.
- χ_M: the characteristic polynomial of a matrix M.

Miscellaneous

- ":=": a definition.
- LHS: left-hand side.
- RHS: right-hand side.
- f^n: the nth iterate of a function f unless otherwise specified.
- $U \star V$: the set $\{u \star v \mid (u, v) \in U \times V\}$ for some sets U, V and an operation $\star$ on $(U \cup V)^2$ (e.g. addition or multiplication on the complex numbers). When $U = \{a\}$ we also write $a \star V$ for $\{a\}V$ (and $U \star a$ for $U\{a\}$ when $\star$ is not commutative).

Contents

Theory

Chapter 1

Algebraic Numbers and Integers

Prerequisites for this chapter: Section A.1.

1.1 Definition

First of all, what is an algebraic number?

Definition 1.1.1 (Algebraic Numbers and Algebraic Integers)

Let $\alpha \in \mathbb{C}$ be a complex number. We say α is an *algebraic number* if it is a root of a **monic** polynomial with rational coefficients. Further, if this polynomial has integer coefficients, we say α is an *algebraic integer*.

The set of algebraic numbers will be denoted by $\overline{\mathbb{Q}}$, and the set of algebraic integers by $\overline{\mathbb{Z}}$.

Note that the "monic" part is very important, otherwise there would be no difference between algebraic numbers and algebraic integers for a number is a root of a polynomial with integer coefficients if and only if it is a root of a polynomial with rational coefficients.

Note also that every integer n is an algebraic integer since it's a root of $X - n$, and every rational number q is an algebraic number since it's a root of $X - q$. This partly explains the notations we chose.

We also say a complex number is *transcendental* if it isn't algebraic, but this won't be relevant in this book as we will only discuss properties of algebraic numbers.

Here are some examples of algebraic numbers:

- 1 is an algebraic integer (root of $X - 1$).
- i is an algebraic integer (root of $X^2 + 1$).
- $2 + \sqrt[4]{3}$ is an algebraic integer (root of $(X - 2)^4 - 3$).
- $\frac{1}{2}$ is an algebraic number (root of $X - \frac{1}{2}$). However, it is **not** an algebraic integer. This is a consequence of the following proposition.

Proposition 1.1.1 (Rational Algebraic Integers)*

The only rational algebraic integers are regular integers. In other words, $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

Proof

Firstly, it is clear that regular integers are algebraic integers since $n \in \mathbb{Z}$ is a root of $X - n \in \mathbb{Z}[X]$.

Let $f = \sum_{i=0}^{n} a_i X^i$ be a monic degree n polynomial with integer coefficients, and assume $\frac{u}{v}$ is a rational root of f, where u, v are coprime integers.

Then,

$$\sum_{i=0}^{n} a_i \left(\frac{u}{v}\right)^i = 0$$

is equivalent, after multiplication by v^n,

$$\sum_{i=0}^{n} a_i u^i v^{n-i} = 0.$$

Modulo v, we get $a_n u^n \equiv 0$, i.e. $u^n \equiv 0$ since f is monic. Since u and v are coprime by assumption, this must mean that $v = \pm 1$. Finally, this means that the root $\frac{u}{v}$ we started with was in fact an integer.

■

Exercise 1.1.1. Is $\frac{i}{2}$ an algebraic integer?

Exercise 1.1.2 (Rational Root Theorem)**.** Let $f \in \mathbb{Z}[X]$ be a polynomial. Suppose that u/v is a rational root of f, written in irreducible form. Prove that u divides the constant coefficient of f and v divides its leading coefficient. (This is a generalisation of Proposition 1.1.1.)

To distinguish algebraic integers from regular integers, we will call the latter *rational integers* since they are precisely the algebraic integers which are rational.

A deep fact about algebraic numbers and algebraic integers is that they're closed under addition and multiplication. This will be proven in Section 1.3, but we will already give an application of these results to a seemingly unrelated problem in order showcase their power.

Problem 1.1.1

Let q be a rational number. Which rational values can $\cos(q\pi)$ take?

Solution

The key point is that the numbers of the form $\cos(q\pi)$ are precisely the real parts of roots of unity. Indeed, any root of unity has its real part of this form, and if $q = \frac{a}{b}$ then $\cos(q\pi)$ is the real part of the $2b$th root of unity $\exp\left(\frac{2a\pi i}{2b}\right)$.

Thus, let $\omega = \exp(qi\pi)$ be a root of unity. Twice its real part is $\omega + \overline{\omega}$, where $\overline{\omega} = \frac{1}{\omega}$ is the complex conjugate of ω. Thus, $2\Re(\omega)$ is a sum of the roots of unity and hence of algebraic integers, which means it's an algebraic integer itself.

Finally, we conclude that if $2\cos(q\pi) = 2\Re(\omega)$ is rational it must be a rational integer. Since $2\cos(q\pi) \in [-2, 2]$ we must have

$$\cos(q\pi) \in \left\{0, \pm\frac{1}{2}, \pm 1\right\}$$

which, conversely, are all easily seen to work. ■

We may now define *divisibility* and *congruences* in algebraic integers, exactly like it is done in $\mathbb{Z}$.

Definition 1.1.2 (Divisibility in $\overline{\mathbb{Z}}$)

Let α and β be algebraic integers. We say α *divides* β and write $\alpha \mid \beta$ if there exists an algebraic integer γ such that $\beta = \alpha\gamma$.

Definition 1.1.3 (Congruences in $\overline{\mathbb{Z}}$)

Let α, β, γ be algebraic integers. We say say α is *congruent to* β *modulo* γ, and write $\alpha \equiv \beta \pmod{\gamma}$, if $\gamma \mid \alpha - \beta$.

Like in $\mathbb{Z}$, $\alpha \equiv \beta \pmod{0}$ is just equivalent to $\alpha = \beta$ since 0 only divides 0.

There is one thing that makes it very nice to work with congruences in algebraic integers: it is the fact that if a, b, n are rational integers, then $a \equiv b \pmod{n}$ in rational integers is the same thing as $a \equiv b \pmod{n}$ in algebraic integers (which is why we use the same notation). Assume n is non-zero, otherwise it is obvious by the previous remark. What does the former mean? It means that $\frac{a-b}{n}$ is a rational integer. What does the latter mean? It means that $\frac{a-b}{n}$ is an algebraic integer. Since we are given that $\frac{a-b}{n}$ is rational, it being a rational integer is equivalent to it being an algebraic integer by Proposition 1.1.1.

As stated before, in Section 1.3, we will prove that the algebraic integers are closed under addition and multiplication (thus forming a ring) which means that we can manipulate these congruences like we would in $\mathbb{Z}$.

1.2 Minimal Polynomial

The goal of this section is to provide an abstract framework to manipulate algebraic numbers better, most of the results will not have any direct application but will help simplify proofs and provide a more conceptual way of thinking about algebraic numbers.

In the first chapter we saw that $2 + \sqrt[4]{3}$ was a root of $(X-2)^4 - 3$, but is it the smallest polynomial having this property? It is natural to ask oneself, given an algebraic number α, what is the least degree non-zero polynomial (with integer coefficients) vanishing at α.

Definition 1.2.1 (Minimal Polynomial)

Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number. We say a least degree monic polynomial vanishing at α is a *minimal polynomial* of α. We also say α is an algebraic number of *degree* n, where n is the degree of any of its minimal polynomials.

The following proposition shows that the minimal polynomial is unique.

Proposition 1.2.1*

Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number and π_α be one of its minimal polynomial. Then, for any polynomial $f \in \mathbb{Q}[X]$, $f(\alpha) = 0$ if and only if $\pi_\alpha \mid f$. In particular, π_α is unique.

Proof

Clearly, if $\pi_\alpha \mid f \in \mathbb{Q}[X]$, then f vanishes at α. For the converse, assume that $f \in \mathbb{Q}[X]$ vanishes at α. Then, perform the Euclidean division of f by π_α: $f = g\pi_\alpha + h$ with $\deg h < \deg \pi_\alpha$. If h is non-zero, then, after dividing it by its leading coefficient, we are left with a monic polynomial with rational coefficients vanishing at α of degree less than $\deg \pi_\alpha$, a contradiction.

Therefore, $\pi_\alpha \mid f$. Now, if π'_α is another minimal polynomial of α, we get $\pi_\alpha \mid \pi'_\alpha$ and $\pi'_\alpha \mid \pi_\alpha$ so $\pi_\alpha = \pi'_\alpha$ since they are both monic.

■

We will thus use π_α to denote the minimal polynomial of an algebraic number α. Notice that a minimal polynomial is always irreducible in $\mathbb{Q}[X]$, and, conversely, an irreducible polynomial is always the minimal polynomial of its roots.

Exercise 1.2.1*. Prove that the minimal polynomial of an algebraic number is irreducible and that an irreducible polynomial is always the minimal polynomial of its roots.

We can now answer our original question. The minimal polynomial of $2+\sqrt[4]{3}$ is in fact $(X-2)^4-3$ as Y^4-3 is easily seen to be irreducible in $\mathbb{Q}[X]$.

Exercise 1.2.2. Prove that Y^4-3 is irreducible in $\mathbb{Q}[X]$.

Given an algebraic number α, it is often particularly useful to look at the other roots of its minimal polynomials ; these are called the *conjugates* of α. This is because α and its conjugates are all symmetric because of Proposition 1.2.1: if α satisfies a certain polynomial equation with rational coefficients, then so do its conjugates.

Definition 1.2.2 (Conjugates)

Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number. Its *conjugates* are defined as the roots of its minimal polynomial: $\alpha_1, \ldots, \alpha_n$ with $n = \deg \pi_\alpha$ (we include α).

For instance, the conjugates of $\sqrt{d}$ where d is non-perfect-square rational number are $\sqrt{d}$ and $-\sqrt{d}$. A more elaborate example is the one of a primitive pth roots of unity, i.e. a pth root of unity $\omega \neq 1$ (where p is some prime number). By Theorem 3.2.1 or Corollary 5.1.5, $\frac{X^p-1}{X-1}$ is irreducible so its conjugates are all the primitive pth roots.[1]

Note that an algebraic number of degree n always has n distinct conjugates, because an irreducible polynomial always has distinct roots.

Exercise 1.2.3*. Prove that any algebraic number of degree n has n distinct conjugates.

Notice also that $\overline{\alpha}$, the complex conjugate of α, is always a conjugate of α (see Appendix A). It is of interest to discuss a bit more the link between the conjugates we just defined and the complex conjugate of a number.

Imagine that, instead of being interested with the field of rational numbers, we were interested in the field of real numbers and we wanted to do algebraic number theory with it. Thus, we define algebraic numbers as roots of polynomials with real coefficients, etc. Now, every minimal polynomial has degree 1 or 2, because any irreducible polynomial in $\mathbb{R}[X]$ has degree 1 or 2 (see Appendix A). Thus, the conjugates are α are either $\{\alpha\} = \{\alpha, \overline{\alpha}\}$ in the first case, or $\{\alpha, \overline{\alpha}\}$ in the second. In fact, this can be generalised a lot, see Chapter 6.

[1] I know forward references are annoying, but I need this fact for one of the worked examples. It is also useful to know as roots of unity are absolutely fundamental in algebraic number theory. For now, you can just take my word on it until you reach Chapter 3.

Finally, we focus a bit on the algebraic integers. Can we say anything about the minimal polynomial of an algebraic integer? We know that the minimal polynomial of an algebraic number which isn't an algebraic integer can't have only integer coefficients, but what about the converse? The answer is yes, as proven by the following proposition.

Proposition 1.2.2

Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number. Then, $\pi_\alpha \in \mathbb{Z}[X]$ if and only if $\alpha \in \overline{\mathbb{Z}}$.

Proof

It is clear that if $\pi_\alpha \in \mathbb{Z}[X]$, α is an algebraic integer. Thus, assume α is an algebraic integer for the reverse implication. We will make the assumption that $\overline{\mathbb{Z}}$ is closed under addition and multiplication, see Section 1.3 for a proof.

Let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α. By Vieta's formulas A.1.4, the coefficient of X^k of π_α is

$$(-1)^{n-k} \cdot \sum_{i_1 < \ldots < i_{n-k}} \alpha_{i_1} \cdot \ldots \cdot \alpha_{i_{n-k}}.$$

This is an algebraic integer by Theorem 1.3.2 and Exercise 1.2.4* but by assumption it is also rational. Therefore, it is a rational integer and $\pi_\alpha \in \mathbb{Z}[X]$ as wanted.

■

Exercise 1.2.4*. Prove that the conjugates of an algebraic integer are also algebraic integers.

Exercise 1.2.5. We call an algebraic number of degree 2 a *quadratic number*. Characterise quadratic integers.

1.3 Symmetric Polynomials

Given a commutative ring R (in our case we will consider $\mathbb{Z}$ and $\mathbb{Q}$) and an integer $n \geq 0$, we can consider the symmetric polynomials in n variables with coefficients in R. These are defined as the polynomials in n variables invariant under all permutations of these variables.

Definition 1.3.1 (Symmetric Polynomials)

We say a polynomial $f \in R[X_1, \ldots, X_n]$ is *symmetric* if $f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$ for any permutation σ of $[n]$.

As an example, $f = X^2Y + XY^2 + X^2 + Y^2$ is a symmetric polynomial in two variables, and

$$g = X^2YZ + XY^2Z + XYZ^2 + XY^2 + X^2Y + XZ^2 + X^2Z + YZ^2 + Y^2Z$$

is a symmetric polynomial in three variables.

Definition 1.3.2 (Elementary Symmetric Polynomials)

The kth *elementary symmetric polynomial* for $k \geq 0$, $e_k \in R[X_1, \ldots, X_n]$, is defined by

$$e_k = \sum_{1 \leq i_1 < \ldots < i_k \leq n} X_{i_1} \cdot \ldots \cdot X_{i_k}.$$

Further, if $k > n$ then $e_k = 0$ (the empty sum) and if $k = 0$ then $e_0 = 1$ (the sum of the empty product).

The two-variable symmetric polynomials are thus simply $e_1 = X + Y$ and $e_2 = XY$. The three-variable ones are $e_1 = X + Y + Z$, $e_2 = XY + YZ + ZX$ and $e_3 = XYZ$.

We now state the fundamental theorem of symmetric polynomials. See Appendix B for a proof.

Theorem 1.3.1 (Fundamental Theorem of Symmetric Polynomials)

Suppose $f \in R[X_1, \dots, X_n]$ is a symmetric polynomial. Then $f \in R[e_1, \dots, e_n]$. In other words, there is a polynomial $g \in R[X_1, \dots, X_n]$ such that

$$f(X_1, \dots, X_n) = g(e_1, \dots, e_n).$$

This theorem explains why we called e_k "elementary symmetric polynomials": because they generate all symmetric polynomials.

Exercise 1.3.1. Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number with conjugates $\alpha_1, \dots \alpha_n$ and $f \in \mathbb{Q}[X_1, \dots, X_n]$ be a symmetric monic polynomial. Show that $f(\alpha_1, \dots, \alpha_n)$ is rational. Further, prove that if α is an algebraic integer and f has integer coefficients, $f(\alpha_1, \dots, \alpha_n)$ is in fact a rational integer.

We can now prove that algebraic integers are closed under addition and multiplication.

Theorem 1.3.2

Let α and β be two algebraic integers. Then, $\alpha\beta$ and $\alpha + \beta$ are also algebraic integers.

Proof

The idea is to construct a monic polynomial whose coefficients are symmetric in both the conjugates of α and the conjugates of β. By Exercise 1.3.1, they will thus be rational integers which will imply that $\alpha + \beta$ is an algebraic integer.

We thus consider the conjugates $\alpha_1, \dots, \alpha_m$ of α and $\beta_1, \dots, \beta_n$ of β and let

$$f(X) = \prod_{i,j}(X - (\alpha_i + \beta_j)) = \prod_i \prod_j ((X - \alpha_i) - \beta_j) = \prod_i \pi_\beta(X - \alpha_i).$$

If we define

$$g(X, X_1, \dots, X_n) = \prod_i \pi_\beta(X - X_i),$$

it is symmetric as a polynomial in $X_1, \dots, X_m$ (over the ring $R = \mathbb{Z}[X]$). We can thus write

$$g = h(X, e_1, \dots, e_m)$$

for some $h \in \mathbb{Z}[X, X_1, \dots, X_n]$ by the fundamental theorem of symmetric polynomials. Finally, our original polynomial f is

$$f = h(X, e_1(\alpha_1, \dots, \alpha_m), \dots, e_m(\alpha_1, \dots, \alpha_m)).$$

But, by Vieta's formulas A.1.4, $e_k(\alpha_1, \dots, \alpha_m)$ is an integer as it is $\pm$ the coefficient of X^{m-k} of π_α! We thus conclude that f has integer coefficients which means that $\alpha + \beta$ is an algebraic integer.

The $\alpha\beta \in \overline{\mathbb{Z}}$ part is handled similarly and we thus omit it.

■

Remark 1.3.1

Our proof also shows that the conjugates of $\alpha+\beta$ and $\alpha\beta$ are among $\alpha_i+\beta_j$ and $\alpha_i\beta_j$ respectively.

Exercise 1.3.2*. Prove that $\overline{\mathbb{Z}}$ is closed under multiplication.

The following straightforward consequence of the fundamental theorem of symmetric polynomials 1.3.1 is sometimes useful.

Proposition 1.3.1

Let $f = a \cdot \prod_{k=1}^{n} X - \alpha_k$ and $g = b \cdot \prod_{k=1}^{n} X - \beta_k$ be two polynomials with integer coefficients, and let $m \in \mathbb{Z}$ be a rational integer which is coprime with a and b. Suppose that $f \equiv g \pmod{m}$. Then,

$$S(\alpha_1, \ldots, \alpha_n) \equiv S(\beta_1, \ldots, \beta_n) \pmod{m}$$

for any symmetric $S \in \mathbb{Z}[X_1, \ldots, X_n]$.

Exercise 1.3.3*. Prove Proposition 1.3.1.

Here is why this proposition is interesting. It lets us use a *local-global* principle. Suppose we have a monic polynomial $f \in \mathbb{Z}[X]$ and you know a bunch of information about its roots modulo prime numbers p. Then, Proposition 1.3.1 lets us deduce information about symmetric sums of the **complex** roots of f, modulo p. If we let p vary, we can thus get information about symmetric sums of the roots of f, and hence information about the roots of f themselves.

We illustrate this by an example. Problem 1.4.1 and Exercise 3.5.33† provide more elaborate applications.

Question

Let $f \in \mathbb{Z}[X]$ be a polynomial. Suppose that f has a double root in $\mathbb{F}_p$ for infinitely many primes p. Must it follow that f has a complex double root?

Answer

We prove that it does. Clearly, f needs to have degree at least 2 for it to have a double root modulo some prime so we may assume that it does. Suppose that f has a double root $\beta \in \mathbb{Z}$ modulo a rational prime p. Consider the polynomial

$$g(X) = f(X) - (X - \beta)f'(\beta) - f(\beta).$$

This may seem unmotivated, but this is just a polynomial congruent to f modulo p (by assumption) which now has β as a **complex** double root.

We may now consider the complex roots $\alpha_1, \ldots, \alpha_n$ of f and $\beta = \beta_1, \ldots, \beta_n = \beta$ of g. By Proposition 1.3.1, we thus have

$$\prod_{i \neq j} \alpha_i - \alpha_j \equiv \prod_{i \neq j} \beta_i - \beta_j \pmod{p}.$$

Since g has a double root, the RHS is zero. Thus, p divides the LHS. Since this is true for infinitely many primes p, we deduce that the LHS is also zero: f has a complex double root.

■

Remark 1.3.2

The number

$$\Delta = (-1)^{\frac{n(n-1)}{2}} a^{2n-2} \cdot \prod_{i \neq j} \alpha_i - \alpha_j = \left(a^{n-1} \prod_{i<j} \alpha_i - \alpha_j \right)^2$$

is called the *discriminant* of f. We can easily check that it agrees with the usual definition when $n = 2$. We have thus shown that if f has a double root mod m then $m \mid \Delta$.

1.4 Worked Examples

In this section, we present two complicated problems where our previous results come to the spotlight. However, exercises in Section 1.5 will show that the theory we have developed applies to a wide variety of situations. Although the full power of our results is often not needed, they provide a more conceptual framework to solve these problems.

Problem 1.4.1 (AMM 10748)

Let q be a prime number and $q \nmid r$ be a positive integer. Suppose that $p > r^{q-1}$ is a prime number congruent to 1 mod q and $a_1, \ldots, a_r$ are rational integers such that

$$p \mid \sum_{i=1}^{r} a_i^{\frac{p-1}{q}}.$$

Prove that p divides one of the a_i.

Solution

Suppose for the sake of a contradiction that none of a_i are zero modulo p. Notice that $a_i^{\frac{p-1}{q}}$ is a qth root of unity modulo p. Let z be an element of order q modulo p; there must exist one otherwise

$$r \equiv \sum_{i=1}^{r} a_i^{\frac{p-1}{q}} \equiv 0 \pmod{p}$$

which is impossible as $p > r^{q-1}$. (In fact there must always exist one if $p \equiv 1 \pmod{q}$ but this is proven in Chapter 3. In fact, as you will see in Chapter 4, even if there did not exist one the argument would still work.)

Then, as $\mathbb{F}_p$ is a field, the roots of $X^q - 1$ are $1, z, \ldots, z^{q-1}$ as these are all roots and this polynomial has at most q roots. Thus, consider k_i such that $z^{k_i} \equiv a_i^{\frac{p-1}{q}}$.

Let f be the polynomial $\sum_{i=1}^{r} X^{k_i}$. By assumption, $p \mid f(z)$ so

$$\prod_{k=1}^{q-1} f(z^k) \equiv 0.$$

Also, by Proposition 1.3.1 we know this is congruent to

$$\prod_{k=1}^{q-1} f(\omega^k)$$

modulo p where $\omega \neq 1$ is a **complex** qth root of unity. However, by the triangular inequality,

$$\left| \prod_{k=1}^{q-1} f(\omega^k) \right| \leq \prod_{k=1}^{q-1} |1| + \ldots + |1| = r^{q-1}.$$

Since $p > r^{q-1}$, this means that this product must be zero.

To conclude, as mentioned after Definition 1.2.2, we know that the minimal polynomial of ω is $\frac{X^q-1}{X-1}$ by Theorem 3.2.1 or Corollary 5.1.5. Thus, by Proposition 1.2.1, this means that

$$X^{q-1} + \ldots + 1 \mid f.$$

Hence, we have

$$f = (X^{q-1} + \ldots + 1)g$$

for some $g \in \mathbb{Z}[X]$ as $X^{q-1} + \ldots + 1$ is monic. Finally, this means that $q \mid f(1) = r$ which is a contradiction. ■

Problem 1.4.2 (Problems from the Book)

Let $a_1, \ldots, a_m \in \mathbb{R}$ be positive real numbers such that $\sqrt[n]{a_1} + \ldots + \sqrt[n]{a_m}$ is rational for any integer $n \geq 1$. Prove that $a_1 = \ldots = a_m = 1$.

Solution

We will proceed in two steps. First, we show that $a_1, \ldots, a_m$ are all algebraic numbers. Let $b_i = \sqrt[m!]{a_i}$. Then, by assumption, for $k \in [m]$,

$$p_k(b_1, \ldots, b_m) := \sum_{i=1}^{m} b_i^k$$

is a rational number. Thus, by Corollary B.2.1 of Newton's formulas (with $K = \mathbb{Q}$), the elementary symmetric polynomials evaluated $b_1, \ldots, b_m$ are all rational: $b_1, \ldots, b_m$ are algebraic. Our claim follows: $a_i = b_i^{m!}$ is also algebraic.

Finally, let N be a positive rational integer such that $Na_1, \ldots, Na_m$ are all algebraic integers. There exists one by Exercise 1.4.1*. Notice that

$$N(\sqrt[n]{a_1} + \ldots + \sqrt[n]{a_m}) = \sqrt[n]{N^{n-1}}(\sqrt[n]{Na_1} + \ldots + \sqrt[n]{Na_m})$$

is an algebraic integer. Since by assumption it is rational, by Proposition 1.1.1 it is a rational integer. Call it u_n. Since $\sqrt[n]{a_i} \to 1$, (u_n) converges to Nm. As it is a sequence of integers, it must be eventually constant. Take a sufficiently large n so that $u_n = Nm = u_{2n}$.

By the Cauchy-Schwarz inequality we have

$$m = \sqrt{1^2 + \ldots + 1^2}\sqrt{\sum_{i=1}^{m} \sqrt[n]{a_i}} \geq \sum_{i=1}^{m} \sqrt[2n]{a_i} = m$$

with equality if and only if all a_i are the same. This is the conclusion that we wanted: since $\sum_{i=1}^{m} \sqrt[n]{a_i} = m$, they must all be equal to 1. ■

Exercise 1.4.1*. Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number. Prove that there exists a rational integer $N \neq 0$ such that $N\alpha$ is an algebraic integer.

1.5 Exercises

Elementary-Looking Problems

Exercise 1.5.1†**.** Find all non-zero rational integers $a, b, c \in \mathbb{Z}$ such that $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ and $\frac{b}{a} + \frac{c}{b} + \frac{a}{c}$ are also integers.

Exercise 1.5.2. Find all rational integers $a, b \neq 1$ such that $\frac{a^4-1}{b^2+1} + \frac{b^4-1}{a^2+1}$ is also an integer.

Exercise 1.5.3† (USAMO 2009)**.** Let $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ be two non-constant sequences of rational numbers such that $(a_i - a_j)(b_i - b_j) \in \mathbb{Z}$ for any i, j. Prove that there exists a non-zero rational number r such that $r(a_i - a_j)$ and $\frac{b_i - b_j}{r}$ are integers for any i, j.

Exercise 1.5.4 (AMM E 2998)**.** Let $x \neq y \in \mathbb{C}$ be complex numbers such that $\frac{x^n - y^n}{x-y}$ is a rational integer for 4 consecutive values of n. Prove that it is always an integer for $n \geq 0$.

Exercise 1.5.5† (Adapted from Irish Mathematical Olympiad 1998)**.** Let $x \in \mathbb{R}$ be a real number such that both $x^2 - x$ and $x^n - x$ for some $n \geq 3$ are rational. Prove that x is rational.

Exercise 1.5.6. Suppose that $a_1, \ldots, a_m \in \mathbb{Z}$ are positive rational integers such that

$$\sum_{i=1}^{m} \sqrt[n_i]{a_i}$$

also is a rational integer. Prove that $\sqrt[n_i]{a_i}$ is a rational integer for any $i = 1, \ldots, m$.

Exercise 1.5.7. Find the least n such that $\cos\left(\frac{\pi}{n}\right)$ can **not** be written in the form $a + \sqrt{b} + \sqrt[3]{c}$ for some rational numbers a, b, c. (More generally, all such n will be determined in Chapter 3.)

Exercise 1.5.8 (Miklós Schweitzer Competition 2015)**.** Let $f, g \in \mathbb{C}[X]$ be such that

$$f \circ g = X^n + X^{n-1} + \ldots + X + 2016$$

for some integer $n \geq 4$. Prove that one of them must have degree 1.

Exercise 1.5.9†**.** Let $|x| < 1$ be a complex number. Define

$$S_n = \sum_{k=0}^{\infty} k^n x^k.$$

Suppose that there is an integer $N \geq 0$ such that $S_N, S_{N+1}, \ldots$ are all rational integers. Prove that S_n is a rational integer for any integer $n \geq 0$.

Exercise 1.5.10†**.** Let $n \geq 3$ be an integer. Suppose that there exist a regular n-gon with integer coordinates. Prove that $n = 4$.

Exercise 1.5.11†**.** Let $\mathcal{P}$ be a polygon with rational sidelengths for which there exists a real number $\alpha \in \mathbb{R}$ such that all its angles are rational multiples of α, except possibly one. Prove that $\cos\alpha$ is algebraic.

Exercise 1.5.12 (Adapted from USA TST 2007)**.** Let $0 < \theta < \frac{\pi}{2}$ be a real number and m, n two coprime rational integers. Suppose that $\cos\theta$ is irrational but $\cos(m\theta)$ and $\cos(n\theta)$ are both rational. Prove that $\theta = \frac{\pi}{6}$.

Exercise 1.5.13 (IMC 2001)**.** Let k and n be positive integers and let f be a polynomial of degree n with coefficients in $\{-1, 0, 1\}$. Suppose that $(X-1)^k \mid f$ and that

$$\frac{p}{\log p} < \frac{k}{\log(n+1)}$$

for some rational prime p. Prove that all complex roots of unity of order p are roots of f.

Exercise 1.5.14 (IZHO 2021)**.** Let $f \in \mathbb{Q}[X]$ be an irreducible polynomial of degree n. Prove that there are at most n polynomials $g \in \mathbb{Q}[X]$ of degree less than n such that $f \mid f \circ g$.

Exercise 1.5.15†**.** Let $\omega_1, \ldots, \omega_m$ be nth roots of unity. Prove that $|\omega_1 + \ldots + \omega_n|$ is either zero or greater than m^{-n}.

Exercise 1.5.16†**.** Let $n \geq 1$ and $n_1, \ldots, n_k$ be integers. Prove that

$$\left|\cos\left(\frac{2\pi n_1}{n}\right) + \ldots + \cos\left(\frac{2\pi n_k}{n}\right)\right|$$

is either zero or greater than $\frac{1}{2(2k)^{n/2}}$.

Exercise 1.5.17† (USA TST 2014)**.** Let N be an integer. Prove that there exists a rational prime p and an element $\alpha \in \mathbb{F}_p^\times$ such that the orbit $\{1, \alpha, \alpha^2, \ldots\}$ has cardinality at least N and is sum-free, meaning that $\alpha^i + \alpha^j \neq \alpha^k$ for any i, j, k. (You may assume that, for any n, there exist infinitely many primes for which there is an element of order n in $\mathbb{F}_p$. This will be proven in Chapter 3.)

Properties of Algebraic Numbers

Exercise 1.5.18. Which of the following are algebraic integers?

- $\sqrt[5]{1+\sqrt[3]{3}} - \sqrt[17]{4-\sqrt[7]{2}}$.
- $\frac{\sqrt{5}+1}{2}$.
- $\frac{\sqrt{3}+1}{2}$.
- $\frac{7}{12}$.
- $\frac{\sqrt[3]{7}-i\sqrt[4]{5}}{6}$.
- $\sqrt{2} \cdot \frac{i+2}{2}$.

Exercise 1.5.19. Prove that $\overline{\mathbb{Q}}$ is a field.

Exercise 1.5.20†**.** Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number with conjugates $\alpha_1, \ldots, \alpha_n$ and $f \in \mathbb{Q}[X]$ be a polynomial. Prove that the m conjugates of $f(\alpha)$ are each represented exactly $\frac{n}{m}$ times among $f(\alpha_1), \ldots, f(\alpha_n)$.

Exercise 1.5.21. Let $\alpha_1, \ldots, \alpha_m \in \overline{\mathbb{Q}}$ be algebraic number and $f \in \mathbb{Q}[X_1, \ldots, X_m]$ a polynomial. Denote the conjugates of α_k by $\alpha_k^{(1)}, \ldots, \alpha_k^{(n_i)}$. Prove that the conjugates of $f(\alpha_1, \ldots, \alpha_k)$ are among

$$\{f(\alpha_1^{(i_1)}, \ldots, \alpha_m^{(i_m)}) \mid i_k = 1, \ldots, n_k\}.$$

Exercise 1.5.22†**.** Let $f \in \overline{\mathbb{Z}}[X]$ be a monic polynomial and α be one of its roots. Prove that α is an algebraic integer.

Exercise 1.5.23†**.** We say an algebraic integer $\alpha \in \overline{\mathbb{Z}}$ is a *unit* if there exists an algebraic integer $\alpha' \in \overline{\mathbb{Z}}$ such that $\alpha\alpha' = 1$. Characterise all units.

Exercise 1.5.24†**.** Let m be a rational integer. We say an algebraic integer $\alpha \in \overline{\mathbb{Z}}$ is a *unit mod* m if there exists an algebraic integer $\alpha' \in \overline{\mathbb{Z}}$ such that $\alpha\alpha' \equiv 1 \pmod{m}$. Characterise all units mod m.

Exercise 1.5.25. Let $\alpha \in \overline{\mathbb{Z}}$ be an algebraic integer which is not a unit. Prove that the set of residues of algebraic integers modulo α, denoted by $\overline{\mathbb{Z}}/\alpha\overline{\mathbb{Z}}$, is infinite.

Exercise 1.5.26†**.** Let $\alpha \in \overline{\mathbb{Z}}$ be an non-rational algebraic integer. Prove that there are a finite number of rational integers m such that α is congruent to a rational integer mod m.

Exercise 1.5.27† (Kronecker's Theorem)**.** Let $\alpha \in \overline{\mathbb{Z}}$ be a non-zero algebraic integer such that all its conjugates have module at most 1. Prove that it is a root of unity.

Exercise 1.5.28†. Determine all non-zero algebraic integers $\alpha \in \overline{\mathbb{Z}}$ such that all its conjugates are **real** and have module at most 2.

Exercise 1.5.29†. Suppose that ω is a root of unity whose real part is an algebraic integer. Prove that $\omega^4 = 1$.

Exercise 1.5.30†. Let $\omega_1, \ldots, \omega_n$ be roots of unity. Suppose that $\frac{1}{n}(\omega_1 + \ldots + \omega_n)$ is a non-zero algebraic integer. Prove that $\omega_1 = \ldots = \omega_n$.[2]

Exercise 1.5.31†. Let $\alpha \in \overline{\mathbb{Z}}$ be an algebraic number and let p be a rational prime. Must it follow that $\alpha^n \equiv 0 \pmod{p}$ or $\alpha^n \equiv 1 \pmod{p}$ for some $n \in \mathbb{N}$?[3]

[2] In fact, any algebraic integer that can be written as a linear combination of roots of unity with rational coefficients can also be written as a linear combination of roots of unity with integer coefficients. However, this is a difficult result to prove (see Exercise 3.5.26† for a special case).

[3] In Chapter 4, we prove that the answer is positive for sufficiently large p.

Chapter 2

Quadratic Integers

Prerequisites for this chapter: Chapter 1 and Section A.2.

It is best to start with an example. Suppose we want to solve the equation $x^2 + 1 = y^3$. Write this equation as

$$(x + i)(x - i) = y^3.$$

Imagine that we could conclude $x + i = (a + bi)^3$ (this is analogous to the rational integers case: if a product of two coprime integers is a cube, then each factor is a cube[1]). Thus, after expanding this, we find $x = a(a^2 - 3b^2)$ and $1 = -b(b^2 - 3a^2)$. This is now very easy to solve: $b = \pm 1$ since it divides 1, so $3a^2 = 1 \pm 1$ since $b^2 - 3a^2$ also divides 1. Thus, this implies $a = 0$ which finally means $x = 0$. We conclude that the only solution is $(x, y) = (0, 1)$.

It is remarkable to see that we have solved a problem about rational integers by introducing a certain class of non-rational algebraic integers. The following sections aim to formalize this approach.

Exercise 2.0.1. Why is the "naive" approach of factorising the equation as $x^2 = (y - 1)(y^2 + y + 1)$ difficult to conclude with? Why does our solution not work as well for the equation $x^2 - 1 = y^3$?

2.1 General Definitions

Given a quadratic **integer** α (meaning an algebraic integer of degree 2), we define the set

$$\mathbb{Z}[\alpha] := \mathbb{Z} + \alpha\mathbb{Z} = \{a + b\alpha \mid a, b \in \mathbb{Z}\}.$$

Given a quadratic **number** α (meaning an algebraic number of degree 2), we define the set

$$\mathbb{Q}(\alpha) := \mathbb{Q} + \alpha\mathbb{Q} = \{a + b\alpha \mid a, b \in \mathbb{Q}\}.$$

The former is in fact a ring, while the latter is a field (called a *quadratic field*).

Remark 2.1.1

Normally, $\mathbb{Z}[\alpha]$ is defined as the smallest ring containing $\mathbb{Z}$ and α, i.e. the ring of all polynomials in α with integer coefficients. Similarly, $\mathbb{Q}(\alpha)$ is defined as the smallest **field** containing $\mathbb{Q}$ and α, i.e. the field of all rational functions in α with rational coefficients. We have chosen the previous definition for the sake of clarity. See Chapter 6 for the general definition.

It might be confusing to see square brackets used for $\mathbb{Z}[\alpha]$ while round brackets are used for $\mathbb{Q}(\alpha)$. In fact, $\mathbb{Q}[\alpha]$ also exists: this is the smallest ring containing α as well as $\mathbb{Q}$ (so polynomials in α with rational coefficients). It turns out that for algebraic numbers α, $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$ (Exercise 6.1.2*). Thus, while it is technically correct to use square brackets, we have used round brackets to

[1] However it remains to prove that $x + i$ and $x - i$ are indeed coprime, for a suitable definition of coprime. Or, if it's not the case, incorporate the gcd in the argument, again, for a suitable definition of gcd.

emphasise the fact that it is a field.

Exercise 2.1.1*. Prove that $\mathbb{Z} + \alpha\mathbb{Z}$ is a ring for any quadratic integer α. This amounts to checking that it is closed under addition, subtraction, and multiplication. What happens if α is a quadratic number which is not an integer?

Exercise 2.1.2*. Prove that $\alpha + \alpha\mathbb{Q}$ is a ring for any quadratic integer α. This amounts to checking that it is closed under addition, subtraction, multiplication, and division.

Exercise 2.1.3*. Let α be a quadratic number and $\beta \in \mathbb{Q}(\alpha)$. Show that β has degree 1 or 2.

Exercise 2.1.4*. Prove that a quadratic field K is equal to $\mathbb{Q}(\sqrt{d})$ for some squarefree rational integer $d \neq 1$. Moreover, prove that such fields are pairwise non-isomorphic (and in particular distinct), meaning that, for distinct squarefree $a, b \neq 1$, there does not exist a bijective function $f : \mathbb{Q}(\sqrt{a}) \to \mathbb{Q}(\sqrt{b})$ such that $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ for any $x, y \in \mathbb{Q}(\sqrt{a})$.

We have seen that algebraic integers have very important properties in algebraic number theory.

Definition 2.1.1 (Ring of Integers of Quadratic Fields)

Let α be a quadratic number. We define the *ring of integers* of $K = \mathbb{Q}(\alpha)$ to be the ring

$$\mathcal{O}_{\mathbb{Q}(\alpha)} := \mathbb{Q}(\alpha) \cap \overline{\mathbb{Z}}$$

consisting of the elements of $\mathbb{Q}(\alpha)$ which are also algebraic integers.

The following proposition characterises the ring of integers of a quadratic field since by Exercise 2.1.4* any quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ for some d.

Proposition 2.1.1*

Let $d \in \mathbb{Z}$ be a squarefree rational integer. We have

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$$

if $d \not\equiv 1 \pmod 4$, and

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$$

if $d \equiv 1 \pmod 4$.

Remark 2.1.2

There is no ambiguity in writing $\mathbb{Q}(\sqrt{d})$ for **negative** d as the square root of d we choose doesn't change that field. For instance, $\mathbb{Z}[i] = \mathbb{Z}[-i]$ so we can write $\mathbb{Z}[\sqrt{-1}]$.

Proof

This follows from Exercise 1.2.5, which we reproduce here for the sake of completeness. Let $x = a + b\sqrt{d}$ be an element of $\mathbb{Q}(\sqrt{d})$. If x is rational then it is a rational integer which is indeed in $\mathbb{Z}[\sqrt{d}]$ and $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Otherwise, x is an integer if and only if its minimal polynomial

$$X^2 - 2aX + (a^2 - db^2)$$

has integral coefficients, by Proposition 1.2.2. This means that $2a \in \mathbb{Z}$ and $a^2 - db^2 \in \mathbb{Z}$. Thus, $4b^2 d \in \mathbb{Z}$ so $2b \in \mathbb{Z}$ since d is a squarefree rational integer. Let $a = \frac{a'}{2}$ and $b = \frac{b'}{2}$ for some $a', b' \in \mathbb{Z}$. We see that x is an integer if and only if

$$a^2 - db^2 = \frac{(a')^2 - d(b')^2}{4} \in \mathbb{Z}.$$

This is now an easy exercise in congruences: if one of a', b' is odd then the other one must be too since $4 \nmid d$. However, an odd perfect square is always congruent to 1 modulo 4, thus if $d \equiv 1 \pmod 4$, (a', b') works if and only if they have the same parity, otherwise they must both even. This is exactly what we wanted to prove.

■

Since a quadratic number has exactly one conjugate distinct from itself, we will call it **the** conjugate.

Definition 2.1.2 (Conjugation in a Quadratic Field)

Let $d \neq 1$ be a squarefree rational integer, and let $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. The conjugate of α, denoted $\overline{\alpha}$, is $a - b\sqrt{d}$.

In particular, this conjugate is also defined for rational numbers, in which case we have $\alpha = \overline{\alpha}$. It is true that this is the same notation as the complex conjugate, but the context will make it clear what is meant. (Note that, when $d = -1$, this conjugate is exactly the complex conjugate, but this is the only time this happens.)

Exercise 2.1.5*. Prove that the conjugate is well defined.

Exercise 2.1.6*. Let $d \neq 1$ be a rational squarefree number. Prove that the conjugation satisifes $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$ and $\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$ for all $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$. Such a function is called an *automorphism* of $\mathbb{Q}(\sqrt{d})$ if it is also bijective.

Exercise 2.1.7. Let $d \neq 1$ be a rational squarefree number. Prove that the only automorphisms of $\mathbb{Q}(\sqrt{d})$ are the identity and conjugation.

We now define a very important map. See Chapter 6 for more.

Definition 2.1.3 (Absolute Norm)

Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number. Its *absolute norm* $\mathrm{N}(\alpha)$ is defined as the product of its conjugates.

In other words, the norm of α is $(-1)^n$ times the constant coefficient of its minimal polynomial by Vieta's formulas A.1.4. This norm however isn't convenient to work with in specific fields because it is not *homogeneous*: $\mathrm{N}(2) = 2^1\,\mathrm{N}(1)$ but $\mathrm{N}(2\sqrt{2}) = 2^2\,\mathrm{N}(\sqrt{2})$. This is because $\sqrt{2}$ has two conjugates while 1 has only one conjugate. We thus define

Definition 2.1.4 (Norm in Quadratic Fields)

Let $d \neq 1$ be a squarefree rational integer. We define the norm $N_{\mathbb{Q}(\sqrt{d})} : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ by

$$N_{\mathbb{Q}(\sqrt{d})}(\alpha) = \alpha\overline{\alpha}.$$

When the context makes it clear what the base field is, we will drop the $\mathbb{Q}(\sqrt{d})$ and simply write N.

This norm is now homogeneous, and even multiplicative! It corresponds to the absolute norm for quadratic integers, and to the square of the absolute norm for rational integers.

Exercise 2.1.8*. Let $d \neq 1$ be a squarefree rational integer, and $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$. Prove that $N(\alpha\beta) = N(\alpha)N(\beta)$.

Exercise 2.1.9. Prove Exercise 2.1.8* without any computations using Exercise 2.1.6*.

Exercise 2.1.10. Let $d < 0$ be a squarefree integer. Prove that the conjugate of an element of $\mathbb{Q}(\sqrt{d})$ is the same as its complex conjugate. In particular, the norm over $\mathbb{Q}(\sqrt{d})$ is the module squared.

2.2 Unique Factorisation

Thia section will be a bit of abstract nonsense. I hope the reader doesn't get too confused.

Our goal is to have an analogue of the fundamental theorem of arithmetic in quadratic rings of integers. This, however, will not hold over every such ring (in fact it hasn't even been proven that it holds for infinitely many ones!) but it will still yield substantial applications such as the diophantine equation we "solved" in the beginning of the chapter. First we have to define what "unique factorisation" means. It's not just "each element can be written in a unique way as a product of primes", because in $\mathbb{Z}$ we need to add a sign for negatives. This is because $\mathbb{Z}$ has two *units* (1 and -1), while $\mathbb{N}$ only has one (1).

Definition 2.2.1 (Unit)

We say en element α of a ring R is a *unit* if it's invertible: i.e., there exists some β such that $\alpha\beta = \beta\alpha = 1$.

Exercise 2.2.1*. Let $d \neq 1$ be a squarefree rational integer. Prove that the product of two units of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is still a unit, and that the conjugate of a unit is also a unit.

Exercise 2.2.2*. Let $d \neq 1$ be a squarefree rational integer. Prove that $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a unit if and only if $|N(\alpha)| = 1$.

Exercise 2.2.3*. Determine the units of the ring $\mathbb{Z}[i]$.

Definition 2.2.2 (Unique Factorisation Domain)

We say an integral domain R has *unique factorisation* and is a *unique factorisation domain* (UFD) if there exists a set of elements of R called *primes* such that each non-zero element $\alpha \in R$ can be written in a unique way as a product of primes

$$\alpha = p_1 \cdot \ldots \cdot p_n$$

up to permutation and multiplication by units.

Indeed, the factorisation $6 = (-2)(-3)$ doesn't bring anything new to the factorisation $6 = 2 \cdot 3$. In $\mathbb{Z}$, there is a canonical way to say which of -2 and 2 is prime, but in general there isn't (and it is actually more useful to say they are both prime). Thus, we say two primes p and q are *associates* if there is a unit u such that $q = up$. Having unique factorisation then means that it is unique up to permutations and associates.

We now discuss some ways to prove an integral domain is a UFD. Recall how unique factorisation is proven $\mathbb{Z}$. We define prime numbers as usual, then prove Bézout's lemma (if a and b are coprime there are x and y such that $ax + by = 1$) and from this deduce the fundamental Euclid lemma: if some prime divides a product, it divides one of the factors. Finally, we induct on the natural integers to show that a prime factorisation always exists and, using Euclid's lemma, that it's unique up to permutation.

We wish to imitate this process. It suggests that the fundamental fact about prime numbers is the Euclid lemma, and not that it can't be written as a non-trivial product. It also suggests that Bézout's lemma is the fundamental step. We thus make the following definitions.

We first take care of our "objection" about primes: they should be defined as having the Euclid property instead of not being writable as a non-trivial product.

Definition 2.2.3 (Prime Element)

We say a non-unit $p \in R$ is a *prime element* if it is non-zero and, for all $a, b \in R$, $p \mid ab$ implies $p \mid a$ or $p \mid b$. (Divisibility is defined as usual: $\alpha \mid \beta$ if there exists a $\gamma \in R$ such that $\beta = \alpha\gamma$.)

Definition 2.2.4 (Irreducible Element)

We say a non-unit $x \in R$ is an *irreducible element* if it is non-zero and $x = \alpha\beta$ implies that α is a unit or β is one.

The usual definition of a prime in $\mathbb{Z}$ is thus as an irreducible element, instead of as a prime one. To further distinguish prime elements from prime numbers, we will thus call the latter *rational primes* (because they are rational integers). This is somewhat contradictory as the primes of $\mathbb{Z}$ are $\pm p$, but by "rational prime" we will always mean a prime of $\mathbb{N}$, i.e. a positive prime number.

Exercise 2.2.4*. Prove that an associate of a prime is also prime.

Exercise 2.2.5*. Prove that the conjugate of a prime is also a prime.

Exercise 2.2.6*. Prove that primes are irreducible.

Exercise 2.2.7*. Let $d \neq 1$ be a squarefree rational integer and let $x \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ be a quadratic integer. Suppose that $|N(x)|$ is a rational prime. Prove x is irreducible.

Exercise 2.2.8*. Suppose a prime p divides another prime q. Prove that p and q are associates.

Exercise 2.2.9*. Prove that p is a prime element of R if and only if it is non-zero and $R \pmod p$ is an integral domain (this means that the product of two non-zero elements is still non-zero). In particular, if $R \pmod p$ is a field (this means that elements which are not divisible by p have an inverse mod p), p is prime.

Exercise 2.2.10. Let $d \neq 1$ be a squarefree rational integer and let $p \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ be a prime. Prove that p divides exactly one rational prime $q \in \mathbb{Z}$.

Exercise 2.2.11. Prove that 2 is irreducible in $\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ but not prime.

Exercise 2.2.12. Show that the primes of Definition 2.2.2 must all be prime elements, and that there is at least one associate of each prime element in that set. (Conversely, if we have unique factorisation, any such set of primes work. This explains why we consider all primes defined in Definition 2.2.3.)

We now define formally the "Bézout property".

Definition 2.2.5 (Bézout Domain)

We say an integral domain R is *Bézout Domain* if, for any $\alpha, \beta \in R$ there exist $\gamma \in R$ such that

$$\alpha R + \beta R = \gamma R.$$

We say such a γ is a *greatest common divisor* (gcd) of α and β.

Exercise 2.2.13*. Prove that a greatest common divisor γ of α and β really is a greatest common divisor of α and β, in the sense that if $\gamma \mid \alpha, \beta$ and $\delta \mid \alpha, \beta$ then $\delta \mid \gamma$.

Exercise 2.2.14*. Prove that an associate greatest common divisor is also a greatest common divisor, and that the greatest common divisor of two elements is unique up to association.

Now that we have defined rings where Bézout's lemma holds, let's see how we can prove that the rings we are interested in have this property. Here is the usual proof that $\mathbb{Z}$ is a Bézout Domain.

Proof that $\mathbb{Z}$ is a Bézout Domain

Let $a, b \in \mathbb{Z}$ be rational integers, without loss of generality positive. Let c be the minimal positive element of $a\mathbb{Z} + b\mathbb{Z}$. We wish to show that $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$. Suppose that it is not the case: there exists some $c \nmid d \in a\mathbb{Z}+b\mathbb{Z}$. Perform the Euclidean division of d by c: $d = cq+r$ where $0 < r < c$. Thus, we have a positive element $r \in a\mathbb{Z} + b\mathbb{Z}$ smaller than c, a contradiction since we assumed c was the smallest.

■

Aha! What we need is a Euclidean division! More specifically, we need to be able to write $\alpha = \rho\beta+\tau$ for some τ which is "smaller" in some sense than β. This yields the following definition.

Definition 2.2.6 (Euclidean Domain)

We say an integral domain R is *Euclidean* if there exists a function $f : R \to \mathbb{N}$ such that for any $\alpha, \beta \in R$ with $\beta \neq 0$ there exist $\rho, \tau \in R$ such that $\alpha = \rho\beta + \tau$ and $f(\tau) < f(\beta)$. Such a function f will be called a *Euclidean function*.

Remark 2.2.1

The remainder doesn't have to be unique.

Exercise 2.2.15. Let R be a Euclidean domain with Euclidean function f. Show that, if $f(\alpha) = 0$, then $\alpha = 0$, and if $f()\alpha) = 1$, then α is a unit or zero.

The reason why we introduced a function $f : R \to \mathbb{N}$ is to get a measure of the size an element of R. This is the role of $f(n) = n$ over $\mathbb{N}$, and $f(n) = |n|$ over $\mathbb{Z}$ (if one wishes to prove directly that unique factorisation holds there). Over quadratic rings of integers, this function will usually be the absolute value of the norm. If $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is Euclidean for the absolute value of the norm, we say it is *norm-Euclidean*. By abuse of terminology we will also sometimes say $\mathbb{Q}(\sqrt{d})$ is norm-Euclidean.

The same proof as the proof that $\mathbb{Z}$ is a Bézout domain shows the following very important proposition.

Proposition 2.2.1*

Any Euclidean domain is a Bézout domain.

Exercise 2.2.16*. Prove that a Euclidean domain is a Bézout domain.

Exercise 2.2.17*. Prove that irreducible elements are prime in a Bézout domain.

We can now state our main theorem. It might seem a bit restrictive but it works over any ring of integer, and we invite the reader to prove it after reading Chapter 6.

Theorem 2.2.1

Any quadratic ring of integers which is a Bézout domain is a UFD.

Proof

Let $\mathcal{O}$ be that ring of integers. We proceed exactly like in $\mathbb{Z}$. First, we prove the existence of a prime factorisation. Suppose that a non-zero element $\alpha \in \mathcal{O}$ has no prime factorisation and choose its norm $N(\alpha)$ to be the smallest in absolute value. Clearly, α isn't a unit since units are their own prime factorisation (the empty factorisation) and isn't prime either. Since irreducible elements are primes by Exercise 2.2.17*, α is not irreducible so $\alpha = \beta\gamma$ for some non-units β, γ. Since $N(\alpha) = N(\beta)N(\gamma)$, we have $|N(\beta)|, |N(\gamma)| < |N(\alpha)|$ because $|N(\beta)|, |N(\gamma)| \neq 1$ by Exercise 2.2.2*. Thus, since α was the smallest element with no prime factorisation, β and γ have one: this means that $\beta\gamma = \alpha$ also has one, a contradiction.

It remains to prove the uniqueness of this factorisation. Suppose an element α has two different prime factorisations

$$p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots q_m$$

and take $m + n$ to be minimal. Since p_n is prime, by definition, it must divide one of the q_i, say, q_m. By Exercise 2.2.8*, $up_n = q_m$ for some unit u. Finally, this means that

$$p_1 \cdot \ldots \cdot p_{n-1} = q_1 \cdot \ldots \cdot (uq_{m-1})$$

so we have two different factorisations of smaller length for the same element. This is a contradiction since we assumed $m + n$ was minimal.

■

Combining this with Proposition 2.2.1, we have proven that it suffices to find a Euclidean function to show that a quadratic ring of integers has unique factorisation. By abuse of notation, we will also say that $\mathbb{Q}(\sqrt{d})$ has unique factorisation if $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ does.

Remark 2.2.2

Most quadratic rings of integers are **not** Euclidean domains, Bézout domains, or even UFD. In fact, it has only been conjectured that there are infinitely many squarefree $1 \neq d \in \mathbb{Z}$ such that $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is UFD! For negative d there is a complete list

$$\{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$$

but the problem is still open for positive d.

Similarly, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is norm-Euclidean only for

$$d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

On the other hand, it has been conjectured that, for positive d, if $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a UFD then is Euclidean for some exotic Euclidean function! This has been proven recently for $d = 14$ and $d = 69$. Note that these are not part of the previous list. For negative d, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is Euclidean if and only if $d \in \{-1, -2, -3, -7, -11\}$.

2.3 Gaussian Integers

Time for applications! We go back to the Gaussian integers $\mathbb{Z}[i]$ which we used at the beginning. The norm in $\mathbb{Q}(i)$ is $N(a + bi) = a^2 + b^2$.

Proposition 2.3.1*

$\mathbb{Z}[i]$ is norm-Euclidean.

Proof

Let $\alpha = a + bi \in \mathbb{Z}[i]$ and $\beta = c + di \in \mathbb{Z}[i]$. Consider the number $x + yi = \frac{\alpha}{\beta}$. Choose rational integers m and n such that $|x - m| \leq \frac{1}{2}$ and $|y - n| \leq \frac{1}{2}$. Thus, $|N(x + yi - (m + ni))| \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$.

Hence,

$$|N(\alpha - \beta(m + ni))| = |N(\beta)| \cdot |N(x + yi - (m + ni))| \leq \frac{|N(\beta)|}{2}$$

which means that the remainder $\tau = \alpha - \beta(m + ni)$ works since it has norm less than $|N(\beta)|$.

■

Corollary 2.3.1*

$\mathbb{Z}[i]$ has unique factorisation.

We shall now analyse the prime elements of $\mathbb{Z}[i]$. Suppose $\alpha \in \mathbb{Z}[i]$ is prime. Then $N(\alpha) = \alpha\overline{\alpha}$ must have at most two rational prime factors since it has exactly two prime factors in $\mathbb{Z}[i]$ (by Exercise 2.2.5*). Moreover, if it has exactly two rational prime factors, then α is an associate of one of them and we may assume without loss of generality that it is a rational prime.

The problem of finding the primes of $\mathbb{Z}[i]$ is therefore reduced to finding when a rational prime $p \in \mathbb{Z}$ stays prime in $\mathbb{Z}[i]$, and when it splits as a product of two Gaussian primes $\alpha\overline{\alpha}$. Indeed, if $N(\alpha) = -p$ then $N(i\alpha) = p$ so we may assume p is positive.

Theorem 2.3.1 (Gaussian Primes)

The primes of $\mathbb{Z}[i]$ are, up to multiplication by a unit,

- $1 - i$.
- $a + bi$ and $a - bi$ where $a^2 + b^2 = p$ for some (positive) rational prime $p \equiv 1 \pmod 4$.
- p where $p \equiv -1 \pmod 4$ is some (positive) rational prime.

In algebraic number theory terminology, we say

- 2 *ramifies* because it becomes non-squarefree ($2 = i(1 - i)^2$),
- $p \equiv 1 \pmod 4$ *splits*, and
- $p \equiv -1 \pmod 4$ stays *inert* because it stays prime.

Proof

First, we see that $2 = (1 + i)(1 - i) = i(1 - i)^2$ and that $N(1 - i) = 2$ so these are primes by Exercise 2.2.7*.

Suppose an odd rational prime $p \in \mathbb{Z}$ does not stay inert in $\mathbb{Z}[i]$. Then, by the previous discussin, there is an $\alpha = a + bi \in \mathbb{Z}[i]$ such that $a^2 + b^2 = N(\alpha) = p$. The numbers a and b are clearly not divisible by p, so $(a \cdot b^{-1})^2 + 1 \equiv 0 \pmod p$. By Exercise 2.3.1*, we must have $p \equiv 1 \pmod 4$.

Thus, $p \equiv 3 \pmod 4$ stays inert. It remains to prove that $p \equiv 1 \pmod 4$ splits. This follows from Exercise 2.3.2*: let n be an integer such that $p \mid n^2 + 1$. Then,

$$p \mid (n + i)(n - i)$$

but $p \nmid n+i, n-i$ so p isn't prime in $\mathbb{Z}[i]$ as wanted. To show that it doesn't ramify, write $p = \pi\overline{\pi}$ for some Gaussian prime π and notice that the gcd of $a+bi = \pi$ and $a-bi = \overline{\pi}$ divides $2a$ and $2b$ so divides 2. However, for $p \neq 2$, π doesn't divide 2 so they have gcd 1, i.e. π and $\overline{\pi}$ are not associates.

■

Exercise 2.3.1*. Let $n \in \mathbb{Z}$ be a rational integer and p an odd rational prime. If $n^2 \equiv -1 \pmod{p}$, prove that $p \equiv 1 \pmod{4}$.

Exercise 2.3.2*. Let $p \equiv 1 \pmod{4}$ be a rational prime. Prove that there exist a rational integer n such that $n^2 \equiv -1 \pmod{p}$. (Hint: Consider $(p-1)!$.)

As a corollary, we get

Corollary 2.3.2 (Fermat's Two Square Theorem)

Any rational prime congruent to 1 modulo 4 is a sum of two squares of rational integers.

Exercise 2.3.3. Which rational integers can be written as a sum of two squares of rational integers?

Exercise 2.3.4*. Find all rational integer solutions to the equation $x^2 + 1 = y^3$. (This is the example we considered in the beginning of the chapter.)

2.4 Eisenstein Integers

In this section we look at the field of Eisenstein numbers $\mathbb{Q}(j)$ where $j = \exp\left(\frac{2i\pi}{3}\right) = \frac{-1+i\sqrt{3}}{2}$ satisfies

$$0 = \frac{j^3 - 1}{j - 1} = j^2 + j + 1.$$

By Proposition 2.1.1, we have $\mathcal{O}_{\mathbb{Q}(j)} = \mathbb{Z}[j]$ since $-3 \equiv 1 \pmod{4}$.

Remark 2.4.1

A small word of warning: the notations we use for a primitive third root of unity j, along with the notation for a primitive fourth root of unity i are the same as the ones we usually use for indexing sums, sets, etc. Which notation is being used should be clear from the context, and, generally (but not always), we shall also redefine j before using it, as it is less standard than i.

Exercise 2.4.1*. Prove that the norm of $a+bj$ is $a^2 - ab + b^2$. (Bonus: do it without any computations using cyclotomic polynomials from Chapter 3.)

Exercise 2.4.2*. Determine the units of $\mathbb{Z}[j]$.

Exercise 2.4.3*. Prove that $\mathbb{Z}[j]$ is norm-Euclidean.

Exercise 2.4.4. Characterise the primes of $\mathbb{Z}[j]$. Conclude that when $p \equiv 1 \pmod{3}$ there exist rational integers a and b such that $p = a^2 - ab + b^2$. (You may assume that there is an $x \in \mathbb{Z}$ such that $x^2 + x + 1 \equiv 0 \pmod{p}$ if $p \equiv 1 \pmod{3}$. This will be proven in Chapter 3, as a corollary of Theorem 3.3.1.)

We now look at a very interesting application of Eisenstein integers: Fermat's last theorem for $n = 3$. In fact, we will even show the following stronger result.

Theorem 2.4.1

There do not exist non-zero Eisenstein integers $\alpha, \beta, \gamma \in \mathbb{Z}[j]$ such that $\alpha^3 + \beta^3 + \gamma^3 = 0$.

Let $\lambda = 1 - j$. Since $3 = N(1-j) = (1-j)(1-j^2) = \lambda^2(1+j)$ we see that λ is prime and that λ^2 is the prime factorisation of 3 (up to a unit) because $1 + j = -j^2$ is a unit.

Exercise 2.4.5*. Let $\theta \in \mathbb{Z}[j]$ be an Eisenstein integer. Prove that, if $\lambda \nmid \theta$, then $\theta \equiv \pm 1 \pmod{\lambda}$. In that case, prove that we also have $\theta^3 \equiv \pm 1 \pmod{\lambda^4}$.

Proof

We will in fact prove that the equation

$$\alpha^3 + \beta^3 + \varepsilon\gamma^3 = 0$$

where ε is a unit does not have non-zero solutions in $\mathbb{Z}[j]$ where $\lambda \nmid \alpha, \beta$. This will imply that $\alpha^3+\beta^3+\gamma^3 = 0$ does not have non-zero solutions either. Indeed, suppose (α, β, γ) is a solution of the latter. Without loss of generality, suppose they are pairwise coprime. Then, either $\lambda \nmid \alpha, \beta, \gamma$ in which case it is also a solution to the former, or we can suppose $\lambda \mid \gamma$ by symmetry which again makes it a solution of the former as λ can't divide α or β.

Thus, suppose for the sake of a contradiction that (α, β, γ) is a solution of $\alpha^3 + \beta^3 + \varepsilon\gamma^3 = 0$ for some unit ε and where $\lambda \nmid \alpha, \beta$. Without loss of generality, assume they are pairwise coprime.

Suppose also $v_\lambda(\gamma)$ is minimal among the solutions. If it is zero, by Exercise 2.4.5*,

$$\alpha^3 + \beta^3 + \varepsilon\gamma^3 \in \{\pm\varepsilon, \pm 2 \pm \varepsilon\} \pmod{\lambda^4}$$

and we can check that this is never divisible by λ^4: the norm of the former is in $\{1, 3, 9, 7\}$ while the norm of λ^4 is $3^4 = 81$. Thus, we already reach a contradiction: $\alpha^3 + \beta^3 + \varepsilon\gamma^3$ can't be zero if $\lambda \nmid \alpha, \beta, \gamma$.

Now, suppose $\gamma = \lambda^n\delta$ for some $\lambda \nmid \delta$ and $n \geq 1$. Write

$$\alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \beta j)(\alpha + \beta j^2) = -\varepsilon\lambda^{3n}\delta^3.$$

By Exercise 2.4.6*, the gcd of each pair of factors is λ. By replacing β by βj^k for a suitable k, we may assume that $v_\lambda(\alpha + j^\ell\beta) = 1$ for $\ell \in \{1, 2\}$. Then, by unique factorisation, there exist units u, v, w and Eisenstein integers $\lambda \nmid x, y, z \in \mathbb{Z}[j]$ such that

$$\begin{cases} \alpha + \beta = u\lambda^{3n-2}x^3 \\ \alpha + \beta j = v\lambda y^3 \\ \alpha + \beta j^2 = w\lambda z^3 \end{cases} \iff \begin{cases} \alpha + \beta = u\lambda^{3n-2}x^3 =: u'\lambda^{3n-2}x^3 \\ \alpha j + \beta j^2 = vj\lambda y^3 =: v'\lambda y^3 \\ \alpha j^2 + \beta j = wj^2\lambda z^3 =: w'\lambda z^3 \end{cases}.$$

To conclude, notice that $(\lambda x, \lambda y, \lambda^{3n-2}z)$ is another smaller solution: by summing the three lines we get

$$u'\lambda x^3 + v'\lambda y^3 + w'\lambda^{3n-2}z^3 = 0$$

for some units u', v', w' since $j^2 + j + 1 = 0$.

Now, divide everything by $u'\lambda$ to get

$$x^3 + \mu y^3 + \eta\lambda^{3(n-1)}z^3 = 0$$

for units μ, η. If $n = 1$, we get, modulo λ^4, $\pm 1 \pm \mu \pm \eta \equiv 0$ which is easily seen to be impossible. Thus $n - 1 \geq 1$. Modulo λ^3, we get $\pm 1 \pm \mu \equiv 0$ so μ must be ± 1. Finally, we get $x^3 + (\pm y)^3 + \eta\lambda^{3m}z^3 = 0$ for some smaller $1 \leq m < n$ which contradicts the minimality of n. In other words, there are no solutions.

■

Exercise 2.4.6*. Let $\alpha, \beta \in \mathbb{Z}[j]$ be coprime Eisenstein integers non-divisible by λ. Prove that, if

$$\lambda \mid \alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \beta j)(\alpha + \beta j^2),$$

each pair of factors has gcd λ.

Exercise 2.4.7. Check the computational details: $\pm 1 \pm \mu \pm \eta$ is never zero mod λ^4 for units μ, η and $\pm 1 \pm \mu \equiv 0 \pmod{\lambda^3}$ implies $\mu = \pm 1$.

Remark 2.4.2

The reason why Eisenstein integers turned out to be so useful to solve Fermat's last theorem for $n = 3$ is that $a^3 + b^3$ factorises completely there. See Exercise 3.5.30† for more cases.

Remark 2.4.3

The part where we looked at the equation modulo λ^4 is completely analogous to the proof that $a^3 + b^3 + c^3 = 0$ does not have rational integers solution where $3 \nmid a, b, c$ by looking at the equation modulo 9. In fact it is exactly the same as λ^4 is a unit times 9.

2.5 Hurwitz Integers

In this section we discuss the Hurwitz integers. These are not algebraic numbers as they are not even complex numbers, but they fit perfectly in this chapter as the reader will quickly see. They will allow us to prove the four square theorem, stating that any positive integer is a sum of four squares, in a similar manner as our proof of the two square theorem. First, we define the quaternion numbers, which were introduced by Hamilton. Recall that a skew fiel is like a field but where multiplication is not necessarily commutative (see Definition A.2.6).

Definition 2.5.1 (Quaternions)

The skew field of the *quaternion numbers* $\mathbb{H}$ is defined as the algebra $\mathbb{R}[\mathbf{i}, \mathbf{j}, \mathbf{k}] := \mathbb{R} + \mathbf{i}\mathbb{R} + \mathbf{j}\mathbb{R} + \mathbf{k}\mathbb{R}$ where $\mathbf{i}, \mathbf{j}, \mathbf{k}$ satisfy the following multiplication rules:

$$\begin{cases} \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1 \\ \mathbf{ij} = \mathbf{k} = -\mathbf{ji} \\ \mathbf{jk} = \mathbf{i} = -\mathbf{kj} \\ \mathbf{ki} = \mathbf{j} = -\mathbf{ik} \end{cases}.$$

Remark 2.5.1

One usually sees the quaternion with the equations $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$.

Exercise 2.5.1*. Prove that $\mathbf{ij} = \mathbf{k} = -\mathbf{ji}$, $\mathbf{jk} = \mathbf{i} = -\mathbf{kj}$ and $\mathbf{ki} = \mathbf{j} = -\mathbf{ik}$ follows from $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{ijk} = -1$ and associativity of the multiplication.

Remark 2.5.2

One may also represent quaternions by the algebra of two by two complex matrices of the form

$$\begin{bmatrix} a + di & b + ci \\ -b + ci & a - di \end{bmatrix} = a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + c \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} + d \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} := a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}.$$

It is then an easy exercise to check that $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$.

Exercise 2.5.2. Prove that $\mathbf{i}, \mathbf{j}, \mathbf{k}$ are distinct.

In particular, we deduce from Exercise 2.5.1* that multiplication is not commutative in $\mathbb{H}$! This is also why $X^2 + 1$ has 3 distinct roots when its degree is only 2: almost all the theory developped in Appendix A, and in particular Corollary A.1.1, fails when multiplication is not commutative.

Exercise 2.5.3*. Let $\alpha, \beta, \gamma \in \mathbb{H}$ be quaternions. Prove that $(\alpha\beta)\gamma = \alpha(\beta\gamma)$. (We say multiplication is *associative*. This is why we can write $\alpha\beta\gamma$ without ambiguity.)

Exercise 2.5.4. Prove that there are infinitely many square roots of -1 in $\mathbb{H}$.

Definition 2.5.2 (Quaternion Conjugate)

Let $\alpha = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}$. The *conjugate* of α, denoted $\overline{\alpha}$ is $a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$.

Exercise 2.5.5*. Prove that, for any $\alpha, \beta \in \mathbb{H}$, $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$ and $\overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}$ (this is because multiplication is not commutative anymore).

Definition 2.5.3 (Quaternion Norm)

Let $\alpha = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}$. The *norm* of α, $N(\alpha)$ is

$$\alpha\overline{\alpha} = a^2 + b^2 + c^2 + d^2.$$

Exercise 2.5.6*. Check that $(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k})$ is indeed $a^2 + b^2 + c^2 + d^2$.

Exercise 2.5.7*. Prove that $\mathbb{H}$ is a skew field. This amounts to checking that elements have multiplicative inverses (i.e. for any α there is a β such that $\alpha\beta = \beta\alpha = 1$).

Exercise 2.5.8*. Prove that the norm is multiplicative: for any $\alpha, \beta \in \mathbb{H}$, $N(\alpha\beta) = N(\alpha)N(\beta)$.

Our object of study will be the ring of *Hurwitz integers*[2]

$$H = \mathbb{Z}\left[\mathbf{i}, \mathbf{j}, \mathbf{k}, \frac{1 + \mathbf{i} + \mathbf{j} + \mathbf{k}}{2}\right] := \mathbb{Z} + \mathbf{i}\mathbb{Z} + \mathbf{j}\mathbb{Z} + \mathbf{k}\mathbb{Z} + \left(\frac{1 + \mathbf{i} + \mathbf{j} + \mathbf{k}}{2}\right)\mathbb{Z}$$

as a subring of the skew field

$$\mathbb{Q}(\mathbf{i}, \mathbf{j}, \mathbf{k}) := \mathbb{Q} + \mathbf{i}\mathbb{Q} + \mathbf{j}\mathbb{Q} + \mathbf{k}\mathbb{Q}.$$

Exercise 2.5.9*. Prove that $H = \{\frac{a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}}{2} \mid a \equiv b \equiv c \equiv d \pmod 2\}$. Deduce that the elements of H have integral norms.

Exercise 2.5.10*. Determine the units of H.

Although multiplication is not commutative anymore, this does not mean we lose all the theory built previously. We can still define divisibility, associates, Euclidean domains and Bézout domains. We just need to incorporate "left" or "right" in the definition to indicate from which side we multiply. The definitions for irreducible elements and units do not change as the first one did not use the commutativity of multiplication while for the second one left and right units are the same since left and right inverses are the same.

[2]One might wander why we defined H as $\mathbb{Z}\left[\mathbf{i}, \mathbf{j}, \mathbf{k}, \frac{1+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}\right]$ instead of simply $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$. This is because they form *maximal order* while $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$ doesn't. More concretely, we will see in Exercise 2.5.14 that $\mathbb{Z}\left[\mathbf{i}, \mathbf{j}, \mathbf{k}, \frac{1+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}\right]$ has a Euclidean division while $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$ does not.

Definition 2.5.4 (Left and Right Divisibility)

Let R be a ring and $\alpha, \beta \in R$. We say α *left-divides* β and write $\alpha \lceil \beta$ if there exists a $\gamma \in R$ such that $\beta = \alpha\gamma$. Similarly, if there exists a $\gamma \in H$ such that $\beta = \gamma\alpha$, we say α *right-divides* β and write $\alpha \rceil \beta$.

Remark 2.5.3

The notations $\lceil$ and $\rceil$ for divisibility are non-standard.

Exercise 2.5.11*. Let $\alpha, \beta, \gamma \in H$. Prove that $\alpha \lceil \beta$ implies $\alpha \lceil \beta\gamma$ but does not always imply $\alpha \lceil \gamma\beta$.

Definition 2.5.5 (Left and Right Associates)

Let R be a ring and $\alpha, \beta \in R$. We say α is a *left-associate* (resp. *right-associate*) of β if there exists a unit ε such that $\alpha = \beta\varepsilon$ (resp. $\alpha = \varepsilon\beta$).

Exercise 2.5.12*. Prove that being left-associate is an *equivalence relation*, i.e., for any α, β, γ, α is a left-associate of itself, α is a left-associate of β if and only if β is a left-associate of α, and if α is a left-associate of β and β is a left associate of γ then α is a left-associate of γ.

Definition 2.5.6 (Left and Right Euclidean Domains)

We say a domain R is *left-Euclidean* (resp. *right-Euclidean*) if there exists a function $f : R \to \mathbb{N}$ such that for any $\alpha, \beta \in R$ with $\beta \neq 0$ there exist $\rho, \tau \in R$ such that $\alpha = \beta\rho + \tau$ (resp. $\alpha = \rho\beta + \tau$) and $f(\tau) < f(\beta)$. Such a function f will be called a *left-Euclidean* (resp. *right-Euclidean*) *function*.

Definition 2.5.7 (Left and Right Bézout Domains)

We say a domain R is *left-Bézout* (resp. *right-Bézout*) if, for any $\alpha, \beta \in R$, there exists a $\gamma \in R$ such that $\alpha R + \beta R = \gamma R$ (resp. $R\alpha + R\beta = R\gamma$). Such a γ will be called a *left-gcd* (resp. *right-gcd*) of α and β.

Left and right definitions are completely symmetric so we will focus primarly on left ones.

Exercise 2.5.13*. Prove that a left-gcd γ of α and β satisifies the following property: $\gamma \lceil \alpha, \beta$ and if $\delta \lceil \alpha, \beta$ then $\delta \lceil \gamma$.

Exercise 2.5.14. Prove that $1+\mathbf{i}$ and $1-\mathbf{j}$ do not have a left-gcd in $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$. In particular, it is not left-Bézout and thus not left-Euclidean too (and the same holds for being right-Bézout and right-Euclidean by symmetry).

As before, we have the following proposition.

Proposition 2.5.1*

A left-Euclidean (resp. right-Euclidean) domain R is a left-Bézout (resp. right-Bézout) domain.

Exercise 2.5.15*. Prove Proposition 2.5.1.

However, being left or right Euclidean does not garantee unique factorisation anymore. That said, some of our results will still hold for rational primes which stay prime in H because rational numbers commute with every quaternion (we will paradoxically use this to show that they do not exist).

We first prove that H is norm-Euclidean.

Proposition 2.5.2*

H is both left and right norm-Euclidean.

Proof

Let $\alpha, \beta \in H$, with $\beta \neq 0$. Consider the quotient $\gamma = \frac{\alpha}{\beta} = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. Choose $x, y, z, t \in \mathbb{Z}$ such that

$$|a - x|, |b - y|, |c - z|, |d - t| \leq \frac{1}{2}$$

and let $\delta = x + y\mathbf{i} + z\mathbf{j} + t\mathbf{k}$. Then,

$$N(\gamma - \delta) \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = 1$$

with equality if and only if $|a - x| = |b - y| = |c - z| = |d - t| = \frac{1}{2}$. If the inequality is strict, then $N(\alpha - \beta\delta) < N(\beta)$, otherwise $\gamma \in H$ so $N(\alpha - \beta\gamma) = 0 < N(\beta)$ as wanted.

The right-Euclidean proof is exactly the same with the order of factors reversed by symmetry.

■

As a corollary, we get that H is left and right Bézout. Now, we show that any Hurwitz integer has a factorisation in irreducible Hurwitz integers.

Proposition 2.5.3

Any Hurwitz integer has a factorisation in irreducible Hurwitz integers. (When it is a unit it is the empty factorisation.)

Exercise 2.5.16*. Prove Proposition 2.5.3.

Exercise 2.5.17. Prove that there is an irreducible Hurwitz integer $x \in H$ for which there exist α and β such that $x \mid \alpha\beta$ but x left-divides neither α nor β.

We can now prove our main result: the Lagrange four square theorem.

Theorem 2.5.1 (Lagrange's Four Square Theorem)

Any non-negative rational integer is a sum of four squares of rational integers.

Proof

This is equivalent to showing that any integer arises as a norm of an element of $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$. Consider the prime case first. We wish to find a non-trivial factorisation $p = \alpha\beta$ in Hurwitz integers. Suppose that p is irreducible, which implies that it is odd as $2 = (1 + \mathbf{i})(1 - \mathbf{i})$.

Then, p is in fact also prime because p commutes with any quaternion since it's real, which means left and right divisibility by p are the same. Indeed, suppose that $p \mid \alpha\beta$ and $p \nmid \beta$. Since H is left-Bézout, there are some $\gamma, \delta \in H$ such that

$$p\gamma + \beta\delta = 1.$$

Thus, β is right-invertible modulo p which means that

$$p \mid \alpha\beta\delta = \alpha - p\gamma\delta$$

so $p \mid \alpha$. The $p \nmid \alpha$ case is handled similarly. (This could be phrased more efficiently using modular arithmetic, but we did it that way to emphasise how the commutativity of p and H made this possible.)

However, by Exercise 2.5.18*, there exist rational integers a and b such that

$$p \mid 1 + a^2 + b^2 = (1 + a\mathbf{i} + b\mathbf{j})(1 - a\mathbf{i} - b\mathbf{j})$$

but $p \nmid 1 + a\mathbf{i} + b\mathbf{j}, 1 - a\mathbf{i} - b\mathbf{j}$ as it is odd. Thus it can't be prime and therefore irreducible too.

This means that there exist non-units Hurwitz integers α and β such that $p = \alpha\beta$. By taking the norm we get $p^2 = N(\alpha)N(\beta)$. Since neither of α, β are units, $N(\alpha), N(\beta)$ must both be equal to p as they are different from 1.

We are almost done: we have represented p as the norm of a Hurwitz integer α and we just want to have $\alpha \in \mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$. Suppose that it is not the case. Consider the unit $\varepsilon = \frac{\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k}}{2}$ where the $\pm$ signs are chosen so that $\rho := \alpha - \varepsilon \in 2\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$. Then,

$$p = \alpha\overline{\alpha} = (\varepsilon + \rho)\overline{\varepsilon}\varepsilon(\overline{\varepsilon} + \overline{\rho}) = (1 + \rho\overline{\varepsilon})(1 - \varepsilon\overline{\rho}) =: \alpha'\overline{\alpha'}$$

where α' now has rational integer coordinates since the coordinates of ρ are even so $\rho\overline{\varepsilon} \in \mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$.

The general case follows from the multiplicativity of the norm: if $p_i = N(\alpha_i)$ and $n = \prod_{i=1}^{k} p_i^{m_i}$, then

$$n = N\left(\prod_{i=1}^{k} \alpha_i^{m_i}\right).$$

■

Exercise 2.5.18*. Let p be a rational prime. Prove that there exist rational integers a and b such that $p \mid 1 + a^2 + b^2$.

2.6 Exercises

Diophantine Equations

Exercise 2.6.1. Solve the equation $x^2 + 4 = y^3$ over $\mathbb{Z}$.

Exercise 2.6.2†. Prove that $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ and $\mathcal{O}_{\mathbb{Q}(\sqrt{-2})}$ are Euclidean.

Exercise 2.6.3. Solve the equations $x^2 + 2 = y^3$ and $x^2 + 8 = y^3$ over $\mathbb{Z}$..

Exercise 2.6.4†. Prove that $\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}$ is Euclidean.

Exercise 2.6.5. Solve the equation $x^2 + x + 2 = y^3$ over $\mathbb{Z}$.

Exercise 2.6.6†. Solve the equation $x^2 + 11 = y^3$ over $\mathbb{Z}$.

Exercise 2.6.7. Let $a, b, c \in \mathbb{Z}$ be rational integers. Prove that $a^2 + b^2 = c^3$ if and only if there exist rational integers m and n such that $a = m^3 - 3mn^2$, $b = -n^3 + 3m^2n$ and $c = m^2 + n^2$. More generally, if $k \geq 1$ is an integer, find all the solutions $a, b, c \in \mathbb{Z}$ to the equation $a^2 + b^2 = c^k$.

Exercise 2.6.8†. Let n be a non-negative rational integer. In how many ways can n be written as a sum of two squares of rational integers? (Two ways are considered different if the ordering is different, for instance $2 = 1^2 + (-1)^2$ and $2 = (-1)^2 + 1^2$ are different.)

Exercise 2.6.9. Which rational integers can be written in the form a^2+2b^2 for some rational integers a and b? What about a^2+2b^2? In how many ways? (You may assume that, for an odd rational prime p, there exists a rational integer such that $x^2 \equiv 2 \pmod{p}$ if and only if $p \equiv \pm 1 \pmod{8}$, and there exists a rational integer x such that $x^2 \equiv -2 \pmod{p}$ if and only if $p \equiv 1 \pmod{8}$ or $p \equiv 3 \pmod{8}$. This will be proven in Chapter 4, as a corollary of the quadratic reciprocity law 4.5.2.)

Exercise 2.6.10 (Saint-Petersbourg Mathematical Olympiad 2013)**.** Find all rational primes p and q such that $2p-1$, $2q-1$, and $2pq-1$ are all perfect squares.

Exercise 2.6.11† (Euler)**.** Let $n \geq 3$ be an integer. Prove that there exist unique positive **odd** rational integers x and y such that $2^n = x^2+7y^2$.

Exercise 2.6.12† (Fermat's Last Theorem for $n=4$)**.** Show that the equations $\alpha^4+\beta^4=\gamma^2$ and $\alpha^4-\beta^4=\gamma^2$ have no non-zero solution $\alpha,\beta,\gamma \in \mathbb{Z}[i]$.

Exercise 2.6.13 (Chinese Mathematical Olympiad 2006)**.** Positive integers k,m,n satisfy $mn = k^2+k+3$. Prove that at least one of the equations

$$x^2+11y^2 = 4m$$

and

$$x^2+11y^2 = 4n$$

has a solution in odd rational integers.

Exercise 2.6.14†**.** Prove that $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ is Euclidean.

Hurwitz Integers and Jacobi's Four Square Theorem[3]

Exercise 2.6.15†**.** Let $\alpha \in H$ be a *primitive* Hurwitz integer, meaning that there does not exist a non-zero $m \in \mathbb{Z}$ such that $\frac{\alpha}{m} \in H$ and let $N(\alpha) = p_1 \cdot \ldots \cdot p_n$ be its prime factorisation. Then, the factorisation of $\alpha = \pi_1 \cdot \ldots \cdot \pi_n$ for irreducible elements π_i of norm p_i is unique up to *unit-migration*, meaning that if if $\tau_1 \cdot \ldots \cdot \tau_k$ is another such factorisation, then $k=n$ and

$$\begin{cases} \tau_1 & = \pi_1 u_1 \\ \tau_2 & = u_1^{-1}\pi_2 u_2 \\ \ldots & \\ \tau_{n-1} & = u_{n-1}^{-1}\pi_n u_n \\ \tau_n & = u_n^{-1}\pi_n. \end{cases}$$

for some units $u_1,\ldots,u_n$. Deduce that α is irreducible if and only if its norm is a rational prime.

Exercise 2.6.16†**.** Prove that $(1+\mathbf{i})H = H(1+\mathbf{i})$[4]. Set $\omega = \frac{1+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}$. We say a Hurwitz integer $\alpha \in H$ is *primary* if it is congruent to 1 or $1+2\omega$ modulo $2+2\mathbf{i}$.[5] Prove that, for any Hurwitz integer α of odd norm, exactly one of its right-associates is primary.

Exercise 2.6.17†**.** Let $m \in \mathbb{Z}$ be an odd integer. Prove that the Hurwitz integers modulo m, H/mH, are isomorphic to the algebra of two by two matrices modulo m, $(\mathbb{Z}/m\mathbb{Z})^{2\times 2}$. In addition, prove that the determinant of the image is the norm of the quaternion.

Exercise 2.6.18†**.** Let m be an odd integer. We say a Hurwitz integer $\alpha = a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$ is *primitive modulo* n if $\gcd(2a,2b,2c,2d,m)=1$. Compute the number $\psi(m)$ of primitive Hurwitz integers modulo m with norm zero (modulo m).

[3]The following series of exercises comes from the work of Hurwitz, but our presentation follows the PhD thesis of Nikolaos Tsopanidis, see [30].

[4]This means that we can manipulate congruences modulo $1+\mathbf{i}$ normally. Note that the choice of $\mathbf{i}$ is not arbitrary at all, since $1-\mathbf{i} = -\mathbf{i}(1+\mathbf{i})$ and $1-\mathbf{j} = (1-\omega)(1+\mathbf{i})$ are associates. By $\alpha \equiv \beta \pmod{\gamma}$, we mean that γ divides $\alpha-\beta$ from the left and from the right.

[5]Note that a primary Hurwitz integer is always in $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$.

Exercise 2.6.19†. Let p be an odd prime. Prove that any non-zero $\alpha \in H/pH$ of zero norm modulo p has a representative of the form $\rho\pi$, where π is a primary element of norm p and $\rho \in H$, and that this π is unique. Conversely, let $\pi \in H$ have norm p. Prove that the equation $\rho\pi \equiv 0 \pmod{p}$ has exactly p^2 solutions $\rho \in H/pH$. Deduce that there are exactly $p+1$ primary irreducible Hurwitz integers with norm p.

Exercise 2.6.20† (Jacobi's Four Square Theorem)**.** Let n be a positive rational integer. In how many ways can n be written as a sum of four squares of rational integers. (Two ways are considered different if the ordering is different, for instance $2 = 1^2 + 0^2 + 0^2 + (-1)^2$ and $2 = (-1)^2 + 0^2 + 0^2 + 1^2$ are different.)

Domains

Exercise 2.6.21. Prove that there are finitely many rational integers $d \equiv 2 \pmod{4}$ or $d \equiv 3 \pmod{4}$ such that $\mathbb{Q}(\sqrt{d})$ is norm-Euclidean.

Exercise 2.6.22. Let R be an integral domain such that for any set $S \subseteq R$ there exists a $\beta \in R$ such that

$$\sum_{\alpha \in S} \alpha R = \beta R.$$

Such a ring is called a *principal ideal domain* (PID). Prove that it is a UFD. (The sum $\sum_{\alpha\in S} \alpha R$ is defined as the union of $\sum_{\alpha\in S'} \alpha R$ over all finite subsets $S' \subseteq S$.)

Exercise 2.6.23. Let R be a Euclidean domain. Prove that it is a PID (and thus a UFD as well).

Exercise 2.6.24. Let $R = \mathbb{Z} + X\mathbb{Q}[X]$ be the ring of polynomials with rational coefficients and integral constant coefficient. Prove that R is a Bézout domain but not a UFD, and hence not a PID either.

Miscellaneous

Exercise 2.6.25†. Let $(F_n)_{n\in\mathbb{Z}}$ be the Fibonacci sequence defined by $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for any integer n. Prove that, for any integers m and n, $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

Exercise 2.6.26. Let $(L_n)_{n\in\mathbb{Z}}$ be the Lucas sequence defined by $L_0 = 2$, $L_1 = 1$, and $L_{n+2} = L_{n+1} + L_n$ for any integer n. Given two integers m and n, find a formula for $\gcd(L_m, L_n)$ analogous to Exercise 2.6.25†.

Exercise 2.6.27†. Let n be a rational integer. Prove that $(1 + \sqrt{2})^n$ is a unit of $\mathbb{Z}[\sqrt{2}]$. Moreover, prove that any unit of $\mathbb{Z}[\sqrt{2}]$ has that form, up to sign.

Exercise 2.6.28† (IMO 2001)**.** Let $a > b > c > d$ be positive rational integers. Suppose that

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Prove that $ab + cd$ is not prime.

Exercise 2.6.29†. Let $x \in \mathbb{R}$ be a non-zero real number and $m, n \geq 1$ coprime integers. Suppose that $x^m + \frac{1}{x^m}$ and $x^n + \frac{1}{x^n}$ are both rational integers. Prove that $x + \frac{1}{x}$ is also one.

Exercise 2.6.30. Find all automorphisms of the quaternions $\mathbb{H}$, i.e. additive and multiplicative bijections $\varphi : \mathbb{H} \to \mathbb{H}$.

Chapter 3

Cyclotomic Polynomials

Prerequisites for this chapter: Chapter 1.

Quadratic numbers and roots of unity are very important in algebraic number theory; they were one of the first objects studied in detail. We have studied a bit the former in Chapter 2, here we will look at the minimal polynomials of the latter and their properties.

3.1 Definition

We say an nth root of unity ω is a *primitive* nth root if its order is n, i.e. $\omega^k \neq 1$ for $k = 1, 2, \ldots, n-1$. Note that, if $\omega = \exp\left(\frac{2ki\pi}{n}\right)$, ω is a primitive nth root if and only if $\gcd(k, n) = 1$.

We may now define cyclotomic polynomials. These are the polynomials with roots primitive nth roots of unity for some n.

Definition 3.1.1 (Cyclotomic Polynomials)

Let $n \geq 1$ be an integer. The nth *cyclotomic polynomial*, Φ_n, is the polynomial of degree $\varphi(n)$

$$\prod_{\omega \text{ primitive } n\text{th root}} X - \omega = \prod_{\gcd(k,n)=1} X - \exp\left(\frac{2ki\pi}{n}\right).$$

For instance, $\Phi_1 = X - 1$, $\Phi_2 = X - (-1)$ and $\Phi_4 = (X - i)(X + i) = X^2 + 1$. Below are the first few cyclotomic polynomials.

- $\Phi_1 = X - 1$.
- $\Phi_2 = X + 1$.
- $\Phi_3 = X^2 + X + 1$.
- $\Phi_4 = X^2 + 1$.
- $\Phi_5 = X^4 + X^3 + X^2 + X + 1$.
- $\Phi_6 = X^2 - X + 1$.

There is one striking thing about these polynomials: they all have integer coefficients![1] In fact, this is true for any n, despite the fact that our definition involved complex numbers. This is a consequence of the following fundamental proposition.

[1] Which makes sense, since we said they were the minimal polynomials of roots of unity.

Proposition 3.1.1*

Let $n \geq 1$ be an integer. Then,

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

Remark 3.1.1

In general, unless otherwise specified, when we write index something (e.g. a sum or a product) by $d \mid n$ we mean that the indexing is done over the **non-negative** divisors of n.

Proof

This is a simple root counting exercise. We have to show that any nth root of unity is a primitive dth root for exactly one $d \mid n$, which is clearly true as this d is the order of the root. Conversely it is clear that any primitive dth root for some $d \mid n$ is an nth root of unity.

■

Exercise 3.1.1*. Let ω be an nth root of unity. Prove that its order divides n.

Exercise 3.1.2*. Let p be a rational prime. Prove that $\Phi_p = X^{p-1} + \ldots + 1$.

Exercise 3.1.3*. Let $n \geq 1$ be an integer. Prove that $\Phi_n(0) = -1$ if $n = 1$ and 1 otherwise.

Exercise 3.1.4. Let $n > 1$ be an integer. Prove that $\Phi_n(1) = p$ if n is a power of a prime p, and $\Phi_n(1) = 1$ otherwise.

From this, we get the following

Corollary 3.1.1*

Cyclotomic polynomials have integer coefficients.

Exercise 3.1.5*. Prove the Corollary 3.1.1 by induction.

By looking at the degrees of both sides of Proposition 3.1.1, we also get the

Corollary 3.1.2

For any integer $n \geq 1$, we have

$$\sum_{d|n} \varphi(d) = n.$$

Let us examine more closely why Proposition 3.1.1 is amazing. It gives us a very good factorisation of $X^n - 1$, so much better than $(X-1)(X^{n-1} + \ldots + 1)$. We can also get a factorisation for $a^n - b^n$ by rewriting it as $b^n((a/b)^n - 1)$. Indeed, define the two-variable homogeneous polynomial $\Phi_n(a, b) := b^{\varphi(n)}\Phi_n(a)$. Then,

$$a^n - b^n = \prod_{d|n} \Phi_d(a, b).$$

Exercise 3.1.6*. Prove that $\Phi_n(1/X) = \Phi_n(X)/X^{\varphi(n)}$ for $n > 1$.

Exercise 3.1.7*. Prove that, for $n > 1$, $\Phi_n(X, Y)$ is a two-variable symmetric and homogeneous, i.e. where all monomials have the same degree, polynomial with integer coefficients.

Exercise 3.1.8*. Prove that

$$\Phi_n(X, Y) = \prod_{\omega \text{ primitive } n\text{th root}} X - \omega Y.$$

We can already use this on a problem.

Problem 3.1.1

Let $n \geq 0$ be an integer. Prove that the number $2^{2^{n+1}} + 2^{2^n} + 1$ has at least $n+1$ prime factors counted with multiplicity.

Solution

Let $x = 2^{2^n}$. The number $2^{2^{n+1}} + 2^{2^n} + 1$ then becomes

$$x^2 + x + 1 = \frac{x^3 - 1}{x - 1} = \frac{2^{3 \cdot 2^n} - 1}{2^{2^n} - 1}.$$

We factorise the numerators and denominators using Proposition 3.1.1:

$$x^2 + x + 1 = \frac{\prod_{d \mid 3 \cdot 2^n} \Phi_d(2)}{\prod_{d \mid 2^n} \Phi_d(2)} = \prod_{d \mid 3 \cdot 2^n, d \nmid 2^n} \Phi_d(2).$$

Notice that the divisors of $3 \cdot 2^n$ that do not divide 2^n are precisely the divisors of the form $3d$ where $d \mid 2^n$, i.e. of the form $3 \cdot 2^k$ for some $0 \leq k \leq n$. Thus,

$$2^{2^{n+1}} + 2^{2^n} + 1 = \prod_{k=0}^{n} \Phi_{3 \cdot 2^k}(2).$$

We have found our $n+1$ divisors! It remains, however, to check that they are non-trivial, i.e. greater than 1. For this, we return to the definition of cyclotomic polynomials:

$$|\Phi_n(2)| = \left| \prod_{\omega \text{ primitive } n\text{th root}} 2 - \omega \right| \geq \prod_{\omega \text{ primitive } n\text{th root}} 1 = 1$$

since $|2 - \omega| \geq 2 - |\omega| = 1$ for any $|\omega| = 1$ by the triangular inequality. In addition, this inequality is strict if $n \neq 1$. ■

Finally, we give a formula to compute cyclotomic polynomials, a lot more efficient than just using Proposition 3.1.1.

Proposition 3.1.2*

Let p be a prime number and $n \geq 1$ an integer. If $p \mid n$ then $\Phi_{pn}(X) = \Phi_n(X^p)$, otherwise $\Phi_{pn}(X) = \frac{\Phi_n(X^p)}{\Phi_n(X)}$.

Proof

This is again a simple root counting exercise. Note first that both sides have the same degree: if $p \mid n$ the RHS has degree $p\varphi(n) = \varphi(pn)$ and if $p \nmid n$ the LHS has degree

$$p\varphi(n) - \varphi(n) = (p-1)\varphi(n) = \varphi(pn).$$

Note also that the quotient makes sense. Indeed, for any primitive nth root ω, ω^p is also a primitive nth root of unity iff $\gcd(n,p) = 1$, i.e. $p \nmid n$. Thus, it suffices to show that each root of the LHS is a root of the RHS.

This is very easy: let ω be a primitive pnth root of unity. Then, ω^p is a primitive nth root as wanted (and ω isn't so the denominator is non-zero).

■

As a corollary, we get

Corollary 3.1.3

Let $n > 1$ be an odd integer. Then, $\Phi_{2n}(X) = \Phi_n(-X)$.

Exercise 3.1.9*. Prove that, for odd $n > 1$, $\Phi_n(X)\Phi_n(-X) = \Phi_n(X^2)$ and deduce Corollary 3.1.3.

Exercise 3.1.10. Prove that, for any polynomial f, $f(X)f(-X)$ is a polynomial in X^2.

Exercise 3.1.11*. Let p be a prime number and $n \geq 1$ an integer. Prove that if $p \mid n$ then $\Phi_{pn}(X,Y) = \Phi_n(X^p, Y^p)$, and that $\Phi_{pn}(X,Y) = \frac{\Phi_n(X^p,Y^p)}{\Phi_n(X,Y)}$ otherwise.

Exercise 3.1.12*. Let $k \geq 1$ be an integer. Prove that $\Phi_{2^k} = X^{2^{k-1}} + 1$.

3.2 Irreducibility

In fact, the factorisation we got for $X^n - 1$ is not only very good, it is **the best possible**: cyclotomic polynomials are irreducible! In algebraic-number-theoretic terminology, the conjugates of a primitive nth root of unity are all primitive nth roots of unity. It is a notoriously hard problem to prove certain polynomials are irreducible, so such a result is remarkable.

Theorem 3.2.1

For any integer $n \geq 1$, Φ_n is irreducible in $\mathbb{Q}[X]$.

We present a proof using algebraic number theory, and leave another one as an exercise.

Proof

Let ω be a primitive nth root of unity with minimal polynomial π. We will show that, for any rational prime $p \nmid n$, ω^p is also a root of π. Thus, ω^k will also be a root of π for any $\gcd(n,k) = 1$. Since all primitive nth roots have this form by Exercise 3.2.1*, we have $\pi = \Phi_n$ as wanted. The key point for this is the congruence $\pi(\omega^p) \equiv \pi(\omega)^p \equiv 0 \pmod{p}$, given by Exercise 3.2.3*.

Let $p \nmid n$ be a rational prime. Suppose for the sake of a contradiction that $\pi(\omega^p) \neq 0$. Then, π

divides (in $\overline{\mathbb{Z}}[X]$, as π is monic)

$$\frac{X^n-1}{X-\omega^p}=\prod_{k\neq p} X-\omega^k.$$

Thus, $\pi(\omega^p)$ divides

$$\prod_{i\neq j}\omega^i-\omega^j=\prod_{i=0}^{n-1}\prod_{j\neq i}\omega^i-\omega^j.$$

By Exercise 3.2.2*, for a fixed i, $\prod_{j\neq i}\omega^i-\omega^j$ is the derivative of $\prod_{j=0}^{n-1} X-\omega^j = X^n-1$ evaluated at ω^i, i.e. $n(\omega^i)^{n-1}$. Thus, our double product is

$$\prod_{i=0}^{n-1} n(\omega^i)^{n-1}=\pm n^n$$

since $\prod_{i=0}^{n-1}\omega^i=(-1)^{n-1}$ by Vieta's formulas A.1.4.

Finally, since $p\mid\pi(\omega^p)$, we also have $p\mid n^n$: this is a contradiction since we assumed $p\nmid n$.

■

Exercise 3.2.1*. Let $n\geq 1$ be an integer and ω be a primitive nth root of unity. Prove that any primitive nth root can be written in the form ω^k for some $\gcd(k,n)=1$.

Exercise 3.2.2*. Let $f=\prod_{k=1}^{n} X-\alpha_i$ be a polynomial. Prove that, for any $k=1,\dots,n$, $f'(\alpha_k)=\prod_{i\neq k}\alpha_k-\alpha_i$.

Exercise 3.2.3* (Frobenius Morphism)**.** Prove the following special case of Proposition 4.1.1: for any rational prime p and any polynomial $f\in\mathbb{Z}[X]$, $f(X^p)\equiv f(X)^p \pmod p$.

Exercise 3.2.4 (Alternative Proof of Theorem 3.2.1)**.** Let ω be a primitive nth root of unity with minimal polynomial π and let $p\nmid n$ be a rational prime. Suppose τ is the minimal polynomial of $\pi(\omega^p)$. Prove that $p\mid\tau(0)$ and that $\tau(0)$ is bounded when p varies. Deduce that ω^p is a root of π for sufficiently large p, and thus that ω^k is a root of π for any $\gcd(n,k)=1$.

An interesting corollary of this theorem is that we can know the conjugates of $\cos\left(\frac{2k\pi}{n}\right)$ for anygcd$(k,n)=1$: they are precisely the numbers $\cos\left(\frac{2k'\pi}{n}\right)$ for $\gcd(k',n)=1$.

However, unlike the primitive nth roots of unity which have degree $\varphi(n)$, they have degree 1 for $n=1,2$ and degree $\frac{\varphi(n)}{2}$ for $n\geq 3$ as $\cos\left(\frac{2k\pi}{n}\right)=\cos\left(\frac{-2k\pi}{n}\right)$.

In particular, this gives an alternative proof of Problem 1.1.1: $\cos\left(\frac{2k\pi}{n}\right)$ is rational iff $\frac{\varphi(n)}{2}=1$ or $n=1,2$, i.e. $n=1,2,4,6$ and we can easily check that $\cos\left(\frac{2k\pi}{n}\right)=0,\pm 1,\pm\frac{1}{2}$ for these n.

Exercise 3.2.5. Let k and $n\geq 1$ be coprime integers. Prove that the conjugates of $\cos\left(\frac{2k\pi}{n}\right)$ are the numbers $\cos\left(\frac{2k'\pi}{n}\right)$ for $\gcd(k',n)=1$. What is its degree? What about $\sin\left(\frac{2k\pi}{n}\right)$, what are its conjugates and what is its degree?

Exercise 3.2.6. Find all quadratic cosines.

3.3 Orders

We will now see very important arithmetic properties of cyclotomic polynomials. This is the fundamental result.

Theorem 3.3.1

Let p be a rational prime and a a rational integer. Then, p divides $\Phi_n(a)$ if and only if the order of a modulo p is $\frac{n}{p^{v_p(n)}}$.

For instance, it is easy to see that $p \mid a-1$ means a has order 1 mod p, $p \mid a+1$ means a has order 2 mod p unless $p=2$, and $p \mid a^2+1$ means a has order 4 mod p unless $p=2$.

In fact, this theorem is perhaps not so surprising if one recalls the local-global principle from Proposition 1.3.1. Over the complex numbers $\mathbb{C}$, $\Phi_n(a)$ is zero if and only if a has order n (by definition). Thus, one can expect that the same holds over the integers mod p, which is exactly what this theorem says.

Proof

We do the case where $p \nmid n$ first. The general case will follow from Exercise 3.3.1* by induction on $v_p(n)$.

Note that the statement makes sense as $p \mid \Phi_n(a)$ implies $p \mid a^n - 1$ so $p \nmid a$. Thus, suppose $p \nmid a$. Let k be the order of a modulo p. Since

$$0 \equiv a^k - 1 = \prod_{d \mid k} \Phi_d(a),$$

there must exist a $p \nmid n$ such that $\Phi_n(a) \equiv 0$.

We show that this n is unique. Suppose that $p \nmid m \neq n$ satisifies $\Phi_m(a) \equiv 0$ too. Then,

$$X^{mn} - 1 = \prod_{d \mid mn} \Phi_d$$

has a double root at a. Thus, by Proposition A.1.3, the derivative mnX^{mn-1} is zero at a: this is impossible as $p \nmid a, m, n$.

Finally, notice that such an n must be the order of a modulo p. By construction, n divides the order of a. If it was distinct from it, then

$$\frac{a^k - 1}{a^n - 1} = \prod_{d \mid k, d \nmid n} \Phi_d(a)$$

would be zero thus there would be some $p \nmid m \neq n$ such that $\Phi_m(a) \equiv 0$ which is impossible.

■

Exercise 3.3.1*. Let p be a rational prime and a a rational integer. Prove that, for any $n \geq 1$, $p \mid \Phi_n(a)$ if and only if $p \mid \Phi_{pn}(a)$.

Exercise 3.3.2*. Let p be a rational prime. Prove that there always exists a *primitive root* or *generator* modulo p, i.e. an integer g such that g^k generates all integers $p \nmid m$ modulo p.

Exercise 3.3.3*. Let p be a rational prime and a, b two rational integers. Prove that $p \mid \Phi_n(a,b)$ if and only if $p \mid a, b$ or $\frac{n}{p^{v_p(n)}}$ is the order of ab^{-1} modulo p.

From this we get the following very important corollary.

Corollary 3.3.1*

Let p be a rational prime and a a rational integer. Suppose that $p \mid \Phi_n(a)$. Then, $p \equiv 1 \pmod{n}$ or p is the greatest prime factor of n.

Proof

If $p \nmid n$, then n is the order of a modulo p by Theorem 3.3.1 so $n \mid p-1$. Otherwise, $\frac{n}{p^{v_p(n)}} \mid p-1$ so all prime factors of the former are smaller than p. But the prime factors of $\frac{n}{p^{v_p(n)}}$ are exactly the prime factors of n distinct from p!

■

Exercise 3.3.4*. Let p be a rational prime and a an integer of order n modulo p. Prove that $a^k \equiv 1 \pmod{p}$ if and only if $n \mid k$. Deduce that n divides $p-1$.[2]

Exercise 3.3.5*. Let p be a rational prime and a, b two rational integers. Suppose that $p \mid \Phi_n(a,b)$. Prove that $p \mid a, b$, $p \equiv 1 \pmod{n}$ or p is the greatest prime factor of n.

Exercise 3.3.6*. Let p be a rational prime and a an integer. Suppose $p \mid \Phi_n(a), \Phi_m(a)$ and $n \neq m$. Prove that $\frac{m}{n}$ is a power of p.

Exercise 3.3.7. Prove the following strengthening of Problem 3.1.1: for any integer $n \geq 0$, the number $2^{2^{n+1}} + 2^{2^n} + 1$ has at least $n+1$ **distinct** prime factors.

We also get the following result. It is a special case of the celebrated theorem of Dirichlet on arithmetic progressions which asserts that, for any $\gcd(m,n) = 1$, there are infinitely many rational primes $p \equiv m \pmod{n}$. Its proof is significantly more involved.

Corollary 3.3.2*

For any integer $n \geq 1$, there are infinitely many rational primes $p \equiv 1 \pmod{n}$.

Exercise 3.3.8*. Let $n \geq 1$ be an integer. Prove that there exist infinitely many rational primes $p \equiv 1 \pmod{n}$.

Here is an example of problem that follows from the first corollary.

Problem 3.3.1 (ISL 2006 N5)

Prove that there doesn't exist integers $x \neq 1$ and y such that

$$\frac{x^7 - 1}{x - 1} = y^5 - 1.$$

Solution

Suppose for the sake of a contradiction that (x, y) is a solution. We rewrite the equation using

[2] This is the mod p version of Exercise 3.1.1*. In fact the proof should be the same as it works in any *group* (see Section A.2 and Theorem 6.3.2).

cyclotomic polynomials:

$$\Phi_7(x) = \Phi_1(y)\Phi_5(y).$$

By Corollary 3.3.1, a prime factor p of the LHS is either 7 of 1 mod 7. Suppose that $7 \nmid \Phi_7(x)$. Then, we must have $\Phi_1(y), \Phi_5(y) \equiv 1 \pmod 7$ by the previous remark. Thus, from $\Phi_1(y) \equiv 1 \pmod 7$ we get $y \equiv 2 \pmod 7$. This means that

$$\Phi_5(y) \equiv \frac{2^5 - 1}{2 - 1} \equiv 2 \pmod 7,$$

a contradiction.

Hence, we must have $7 \mid \Phi_7(x)$. Since 7 is distinct from 5 and not congruent to 1 mod 5, it can't divide $\Phi_5(y)$ which means it must divide $\Phi_1(y)$. Thus, $y \equiv 1 \pmod 7$. This implies that

$$\Phi_5(y) \equiv 1 + 1 + 1 + 1 + 1 \equiv 5 \pmod 7$$

which is again a contradiction. ■

3.4 Zsigmondy's Theorem

In this section, we formulate and prove the powerful Zsigmondy theorem.

Definition 3.4.1

Let $(u_n)_{n\geq 1}$ be a sequence of rational integers. We say a prime p is a *primitive* prime factor of a_n if $p \mid u_n$ but $p \nmid u_1, \ldots, u_{n-1}$.

In other words, a primitive prime factor is a new prime factor.

Theorem 3.4.1 (Zsigmondy)

Let $a > b$ be non-zero coprime positive integers. The sequence $(a^n - b^n)_{n\geq 1}$ always has a rational primitive prime factor for $n \geq 2$ **except** in the following cases: $n = 2$ and $a + b$ is $\pm$ a power of 2, and $n = 6$ and $(a, b) = (2, 1)$.

Exercise 3.4.1*. Check that the exceptions stated in Theorem 3.4.1 are indeed exceptions.

Exercise 3.4.2*. Prove that $a^2 - b^2$ has no primitive prime factor if and only if $a + b$ is $\pm$ a power of 2.

Here is how we will prove this theorem. The numbers $a^n - b^n$ have many prime factors in common. However, we have seen that the numbers $\Phi_n(a, b)$ have strong restrictions on their prime factors, and thus don't have many common prime factors (see e.g. Exercise 3.3.6*). Notice now that, since

$$a^n - b^n = \prod_{d|n} \Phi_d(a, b)$$

finding a primitive prime factor of $a^n - b^n$ reduces to finding a primitive prime factor of $\Phi_n(a, b)$!

Before delving into the proof, we need a lemma called the "lifting the exponent lemma" or "LTE".

Theorem 3.4.2 (Lifting the Exponent Lemma)

Let $p \mid n$ be an odd rational prime, where $n \geq 1$ is an integer. Then, for any rational integer a, $v_p(\Phi_n(a, b)) \leq 1$. Moreover, for $p = 2$, if $4 \mid n$ then $v_p(\Phi_n(a, b)) \leq 1$.

Proof

Notice that

$$\Phi_n(a,b) \mid \frac{a^n - b^n}{a^{n/p} - b^{n/p}}.$$

If $a^{n/p} \not\equiv b^{n/p} \pmod{p}$ then $a^n \not\equiv b^n \pmod{p}$ so $v_p(\Phi_n(a,b)) = 0$.

Thus, it suffices to show that for any distinct rational integers $u \equiv \pmod{p}$, $p^2 \nmid \frac{u^p - v^p}{u - v}$. Write $v = u + mp$. Then,

$$\frac{u^p - v^p}{u - v} = \sum_{k=0}^{p-1} u^{p-1-k} v^k = \sum_{k=0}^{p-1} u^{p-1-k}(u + mp)^k \equiv \sum_{k=0}^{p-1} u^{p-1-k}(u^k + kmpu^{m-1}) \pmod{p^2}$$

by the binomial expansion. However, this sum is just

$$\sum_{k=0}^{p-1} u^{p-1} + pmu^{p-2}k = pu^{p-1} + pmu^{p-2} \cdot \frac{p(p-1)}{2} \equiv pu^{p-1} \pmod{p^2}$$

which is indeed non-zero for odd p.

For $p = 2$, we have $v_2\left(\frac{a^n - b^n}{a^{n/2} - b^{n/2}}\right) = v_2(a^{n/2} + b^{n/2}) \leq 1$ when $2 \mid n/2$, i.e. $4 \mid n$.

■

Some might be more familiar with this version of the lemma:

Theorem 3.4.3 (Lifting the Exponent Lemma)

Let p be rational prime and $u \equiv v \not\equiv 0 \pmod{p}$. Then,

$$v_p(u^n - v^n) = v_p(u - v) + v_p(n).$$

Moreover, for $p = 2$, we have $v_2(u^n - v^n) = v_2(u - v)$ for odd n and $v_2(u^n - v^n) = v_2(u^2 - v^2) + v_2(n) - 1$ for even n.

Proof

Rewrite this as

$$v_p\left(\frac{u^n - v^n}{u - v}\right) = v_p(n).$$

Then, this follows from the following equality:

$$\frac{u^n - v^n}{u - v} = \prod_{d \mid n, d > 1} \Phi_d(u,v).$$

By Exercise 3.3.3*, $p \mid \Phi_d(u,v)$ if and only if $\frac{d}{p^{v_p(d)}}$ is the order of $u \cdot v^{-1}$. Since $u \equiv v$, the order of $u \cdot v^{-1}$ is just 1. Thus, $p \mid \Phi_d(u,v)$ if and only if d is a power of p. By our version of the lemma 3.4.2, each such factor adds 1 to the p-adic valuation since a power of p distinct from 1 is divisible by p. Finally, the p-adic valuation of $\frac{u^n - v^n}{u - v}$ is just the number of powers of p distinct from 1 dividing n: i.e. $v_p(n)$. For $p = 2$, we also need to take in account the contribution of Φ_2 so we get $v_2(u^n - v^n) = v_2(n) - 1 + v_2(u^2 - v^2)$ for $2 \mid n$ (and the case $2 \nmid n$ is the same as for p odd).

■

We can now start proving Zsigmondy's theorem.

Beginning of the Proof of Zsigmondy's Theorem 3.4.1

Suppose that $\Phi_n(a,b)$ does not have any primitive prime factor for some $n \geq 3$; the case $n = 2$ was done Exercise 3.4.2*. Then, let $p \mid \Phi_n(a,b)$ be a non-primitive prime factor, say that it also divides $\Phi_m(a,b)$ for some $m < n$. Since a and b are coprime integers, p cannot divide both of them so it divides neither and the order of ab^{-1} mod p is both $\frac{n}{p^{v_p(n)}}$ and $\frac{m}{p^{v_p(m)}}$ by Exercise 3.3.3*

Thus, n and m differ multiplicatively by a power of p. In particular, $p \mid n$ so p is the greatest prime factor of n by Exercise 3.3.5* and hence is unique!

Moreover, p can't be equal to 2, otherwise n would be a power of 2 but $\Phi_{2^k}(a,b) = a^{2^{k-1}} + b^{2^{k-1}}$ is a sum of two coprime squares hence not divisible by 4 but clearly at least 4 which means it can't be a power of 2. Thus, by the LTE lemma 3.4.2, $v_p(\Phi_n(a,b)) \leq 1$. We have reduced the problem to showing $|\Phi_n(a,b)|$ is not equal to the greatest prime factor of n!

If $|\Phi_n(a,b)|$ were equal to the greatest prime factor of n, it would in particular be at most n. Intuitively, this should not be the case as cyclotomic polynomials are exponential in n. We are thus led to find bounds on them. This is achieved in the following proposition.

Proposition 3.4.1*

Let $|a| > |b|$ be two real numbers and $n \geq 1$ an integer. Then,

$$(|a| - |b|)^{\varphi(n)} \leq |\Phi_n(a,b)| \leq (|a| + |b|)^{\varphi(n)}$$

with equality in either side only if $n = 1$ or $n = 2$. In addition, if $n > 2$,

$$|b|^{\varphi(n)} \leq \Phi_n(a,b)$$

with equality only if $|a| = |b|$.

Proof

The first part of this follows from the triangular inequality exactly like we did for Problem 3.1.1:

$$|\Phi_n(a,b)| = \prod_{\omega \text{ primitive } n\text{th root of unity}} |a + b\omega|$$

by Exercise 3.1.8* and each factor is between $|a| - |b|$ and $|a| + |b|$. The equality case are easy to work out: $|a + b\omega| = |a| \pm |b|$ implies ω is real so $n = 1$ or $n = 2$.

For the $|b|^{\varphi(n)}$ part, after dividing by it it reduces to $|\Phi_n(a/b)| > 1$ thus to showing $|\Phi_n(x)| > 1$ for all $|x| > 1$. Notice that, for any $|\omega| = 1$, $|x - \omega|$ is a strictly decreasing function in x if $x \leq -1$ and is a stricly increasing function in x if $x \geq 1$. Hence,

$$|\Phi_n(x)| = \prod_{\omega \text{ primitive } n\text{th root of unity}} |x - \omega|$$

is either at least $|\Phi_n(1)|$ or $|\Phi_n(-1)|$. But these are both non-zero integers so in both cases it is at least 1 and by strict monotony if we have equality $|a| = |b|$.

■

Exercise 3.4.3. Let $n \geq 3$ be an integer. Prove that Φ_n is positive on $\mathbb{R}$.

Back to the the Proof of Zsigmondy's Theorem 3.4.1

Suppose that $\Phi_n(a,b) = p$ where p is a prime factor of n. Then, by Proposition 3.4.1,

$$b^{\varphi(n)}, (a-b)^{\varphi(n)} \leq \Phi_n(a,n) = p.$$

In particular, since $p \mid n$,

$$b^{p-1}, (a-b)^{p-1} \leq p.$$

Exercise 3.4.4 therefore implies that $b = 1$ and $a - b = 1$ since $p \neq 2$, i.e. $b = 1$ and $a = 2$.

We now use Proposition 3.1.2:

$$\Phi_n(a) \geq \frac{\Phi_{n/p}(a^p)}{\Phi_n(a)} \geq \left(\frac{2^p - 1}{3}\right)^{\varphi(n/p)}.$$

By Exercise 3.4.4, since $\frac{2^p-1}{3} \leq p$, we must have $p = 3$. Since we also had $\left(\frac{2^p-1}{3}\right)^{\varphi(n/p)} \leq p$ this means that $\varphi(n/p) = 1$ so $n = p$ or $2p$.

Since $\Phi_1(2,1) = 1$ and $\Phi_2(2,1) = 3$, $\Phi_3(2,1) = 5$ has a primitive, which means that $n = 6$ and we have finally found our exception!

■

Remark 3.4.1

As Exercise 3.5.40† shows, we can still get an exponential bound for $\Phi_n(2)$ and make that case similar to the others, but this is technical so we preferred this approach.

Exercise 3.4.4. Prove that $2^{m-1} > m$ for any integer $m \geq 3$ and $2^m - 1 > 3m$ for any integer $m \geq 4$.

3.5 Exercises

Diophantine Equations

Exercise 3.5.1. Find all rational integers x and y such that $x^2 + 9 = y^3$.

Exercise 3.5.2† (USA TST 2008)**.** Let n be a rational integer. Prove that $n^7 + 7$ is not a perfect square.

Exercise 3.5.3. Solve the equation

$$x^3 = y^{16} + y^{15} + \ldots + y + 9$$

over $\mathbb{Z}$.

Exercise 3.5.4 (Japanese Mathematical Olympiad 2011)**.** Find all positive integers a, p, q, r, s such that

$$a^s - 1 = (a^p - 1)(a^q - 1)(a^r - 1).$$

Exercise 3.5.5† (French TST 1 2017)**.** Determine all positive integers a for which there exists positive integers m and n as well as positive integers $k_1, \ldots, k_m, \ell_1, \ldots, \ell_n$ such that

$$(a^{k_1} - 1) \cdot \ldots \cdot (a^{k_m} - 1) = (a^{\ell_1} + 1) \cdot \ldots \cdot (a^{\ell_n} + 1).$$

Divisibility Relations

Exercise 3.5.6 (IMO 2000)**.** Does there exist a rational integer n such that n has exactly 2000 distinct prime factors and n divides $2^n + 1$?

Exercise 3.5.7†**.** Find all coprime positive integers a and b for which there exist infinitely many integers $n \geq 1$ such that

$$n^2 \mid a^n + b^n.$$

Exercise 3.5.8. Prove that there exist infinitely many positive integers n such that

$$n^3 \mid 2^{n^2} + 1.$$

Exercise 3.5.9 (Iran TST 2013)**.** Prove that there does not exist positive rational integers a, b, c such that $3(ab + bc + ca) \mid a^2 + b^2 + c^2$.

Exercise 3.5.10 (ISL 1998)**.** Determine all positive integers n for which there is an $m \in \mathbb{Z}$ such that $2^n - 1 \mid m^2 + 9$.

Prime Factors

Exercise 3.5.11† (ISL 2002)**.** Let $p_1, \ldots, p_n > 3$ be distinct rational primes. Prove that the number

$$2^{p_1 \cdot \cdots p_n} + 1$$

has at least 2^{2^n} distinct prime factors.

Exercise 3.5.12† (Problems from the Book)**.** Let $a \geq 2$ be a rational integer. Prove that there exist infinitely many integers $n \geq 1$ such that the greatest prime factor of $a^n - 1$ is greater than $n \log_a n$.

Exercise 3.5.13† (Inspired by IMO 2003)**.** Let $m \geq 1$ be an integer. Prove that there is some rational prime p such that $p \nmid n^m - m$ for any rational integer n.

Exercise 3.5.14†**.** Prove that $\varphi(n)/n$ can get arbitrarily small. Deduce that $\pi(n)/n \to 0$, where $\pi(n)$ denotes the number of primes at most n.

Exercise 3.5.15†**.** Let $P(n)$ denote the greatest prime factor of any rational integer $n \geq 1$ ($P(1) = 0$). Let $\varepsilon > 0$ be a real number. Prove that there exist infinitely many rational integers $n \geq 2$ such that

$$P(n-1), P(n), P(n+1) < n^\varepsilon.$$

Exercise 3.5.16† (Brazilian Mathematical Olympiad 1995)**.** Let $P(n)$ denote the greatest prime factor of any rational integer $n \geq 1$. Prove that there exist infinitely many rational integers $n \geq 2$ such that

$$P(n-1) < P(n) < P(n+1).$$

Exercise 3.5.17. Let $a, b \in \mathbb{Z}[\sqrt{5}]$ be quadratic integers such that $a \equiv b \pmod{\sqrt{5}}$ and $n \geq 1$ an integer. Prove that

$$v_{\sqrt{5}}(a^n - b^n) = v_{\sqrt{5}}(a - b) + v_{\sqrt{5}}(n)$$

where $v_{\sqrt{5}}(x)$ denotes the greatest integer v such that $(\sqrt{5})^v \mid x$ but $(\sqrt{5})^{v+1} \nmid x$. Deduce that

$$v_5(F_n) = v_5(n)$$

for any $n \geq 1$, where $(F_n)_{n \geq 0}$ is the Fibonacci sequence defined by $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 0$.

Exercise 3.5.18† (Structure of units of $\mathbb{Z}/n\mathbb{Z}$)**.** Let p be an odd rational prime and $n \geq 1$ and integer. Prove that there is a primitive root modulo p^n, i.e. a number g which generates all the numbers coprime with p modulo p^n. Moreover, show that there doesn't exist a primitive root mod 2^n for $n \geq 3$, but that, in that case, there exist a rational integer g and a rational integer a such that each rational integer is congruent to either g^k for some k or ag^k modulo 2^n.[3]

[3] In group-theoretic terms, this says that $(\mathbb{Z}/p^n\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(p^n)\mathbb{Z}$ and that $(\mathbb{Z}/2\mathbb{Z})^n \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z})$ for $n \geq 2$. The Chinese remainder theorem then yields

$$(\mathbb{Z}/2^n p_1^{n_1} \cdots p_m^{n_m}\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z}) \times (\mathbb{Z}/\varphi(p_1^{n_1})\mathbb{Z}) \times \ldots \times (\mathbb{Z}/\varphi(p_m^{n_m})\mathbb{Z}).$$

Coefficients of Cyclotomic Polynomials

Exercise 3.5.19. Define the *Möbius function* $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$ by $\mu(n) = (-1)^k$ where k is the number of prime factors of n if n is squarefree, and $\mu(n) = 0$ otherwise. Prove that

$$\Phi_n = \prod_{d|n} (X^d - 1)^{\mu(n/d)}.$$

Exercise 3.5.20†. Let $m \geq 0$ be an integer. Prove that the coefficient of X^m of Φ_n is bounded when n varies.

Exercise 3.5.21†. Let $\psi(x) = \sum_{p^\alpha \leq x} \log p$. By noticing that

$$\exp(\psi(2n+1)) \int_0^1 x^n (1-x)^n \, \mathrm{d}x \leq \frac{\exp(\psi(2n+1))}{4^n},$$

prove that $\pi(n)$, the number of primes at most n, is greater than $Cn/\log n$ for some constant $C > 0$.

Exercise 3.5.22†. Let $m \geq 3$ be an odd integer and suppose that $p_1 < \ldots < p_m = p$ are rational primes such that $p_1 + p_2 > p_m$ and let $n = p_1 \cdot \ldots \cdot p_m$. What are the coefficient of X^p and X^{p-2} of Φ_n? Deduce that any rational integer arises as a coefficient of a cyclotomic polynomial.[4]

Exercise 3.5.23†. Let p and q be two rational primes. Prove that the coefficients of Φ_{pq} are in $\{-1, 0, 1\}$.

Cyclotomic Fields and Fermat's Last Theorem

Exercise 3.5.24† (Sophie-Germain's Theorem)**.** Let p be a *Sophie-Germain prime*, i.e. a rational prime such that $2p + 1$ is also prime. Prove that the equation $a^p + b^p = c^p$ does not have rational integer solutions $p \nmid abc$.

Exercise 3.5.25†. Let ω be an nth root of unity. Define $\mathbb{Q}(\omega)$ as $\mathbb{Q} + \omega\mathbb{Q} + \ldots + \omega^{n-1}\mathbb{Q}$. Prove that

$$\mathbb{Q}(\omega) \cap \mathbb{R} = \mathbb{Q}(\omega + \omega^{-1})$$

where $\mathbb{Q}(\omega + \omega^{-1}) = \mathbb{Q} + (\omega + \omega^{-1})\mathbb{Q} + \ldots + (\omega + \omega^{-1})^{n-1}\mathbb{Q}$.

Exercise 3.5.26†. Let ω be a primitive pth root of unity, where p is prime. Prove that the ring of integers of $\mathbb{Q}(\omega)$, $\mathcal{O}_{\mathbb{Q}(\omega)} := \mathbb{Q}(\omega) \cap \overline{\mathbb{Z}}$ is

$$\mathbb{Z}[\omega] := \mathbb{Z} + \omega\mathbb{Z} + \ldots + \omega^{n-1}\mathbb{Z}.$$

(In fact this holds for any nth root of unity but it is harder to prove.)

Exercise 3.5.27†. Let ω be a primitive pth root of unity, where p is prime. Prove that $p = u(1-\omega)^{p-1}$, where $u \in \overline{\mathbb{Z}}$ is a unit of $\overline{\mathbb{Z}}$, i.e. $1/u$ is also an algebraic integer. Deduce that $1 - \omega$ is prime in $\mathbb{Q}(\omega)$.

Exercise 3.5.28† (Kummer)**.** Let ω be a root of unity of odd prime order p and suppose ε is a unit of $\mathbb{Q}(\omega)$. Prove that $\varepsilon = \eta\omega^n$ for some $n \in \mathbb{Z}$ and $\eta \in \mathbb{R}$.

Exercise 3.5.29†. Let $\alpha \in \mathbb{Z}[\omega]$, where ω is a primitive pth root of unity. Prove that α^p is congruent to a rational integer modulo p.

Exercise 3.5.30† (Kummer)**.** Let p be an odd prime and ω a primitive pth root of unity. Suppose that $\mathbb{Z}[\omega]$ is a UFD.[5] Prove that there do not exist non-zero rational integers $a, b, c \in \mathbb{Z}$ such that

$$a^p + b^p + c^p = 0.$$

(You may assume that, if a unit of $\mathbb{Z}[\omega]$ is congruent to a rational integer modulo p, it is a pth power of a unit. This is known as "Kummer's lemma". See Borevich-Shafarevich [6] or Conrad [10] for a $(1-\omega)$-adic proof of this.)

[4] This may come off as a bit surprising considering that all the cyclotomic polynomials we saw had only ± 1 and 0 coefficients.

[5] Sadly, it has been proven that $\mathbb{Z}[\omega]$ is only a UFD when $p \in \{3, 5, 7, 11, 13, 17, 19, 23\}$. This approach works however almost verbatim when the *class number* h of $\mathbb{Q}(\omega)$ is not divisible by p. The case $h = 1$ corresponds to $\mathbb{Z}[\omega]$ being a UFD. That said, it has not been proven that there exist infinitely many p such that $p \nmid h$ (but it has been conjectured to be the case), while it has been proven that there exist infinitely many p such that $p \mid h$.

Exercise 3.5.31† (Fleck's Congruences)**.** Let $n \geq 1$ be an integer, p a prime number and $q = \left\lfloor \frac{n-1}{p-1} \right\rfloor$. Prove that, for any rational integer m,

$$p^q \mid \sum_{k \equiv m \pmod{p}} (-1)^k \binom{n}{k}.$$

Miscellaneous

Exercise 3.5.32. Prove a version of Zsigmondy where a and b are coprime rational integers (not necessarily positive).

Exercise 3.5.33† (Korea Winter Program Practice Test 1 2019)**.** Find all non-zero polynomials $f \in \mathbb{Z}[X]$ such that, for any prime number p and any integer n, if $p \nmid n, f(n)$, the order of $f(n)$ modulo p is at most the order of n modulo p.

Exercise 3.5.34† (Korea Mathematical Olympiad Final Round 2019)**.** Show that there exist infinitely many positive integers k such that the sequence $(a_n)_{n \geq 0}$ defined by $a_0 = 1$, $a_1 = k + 1$ and

$$a_{n+2} = k a_{n+1} - a_n$$

for $n \geq 0$ contains no prime number.

Exercise 3.5.35† (Iran Mathematical Olympiad 3rd round 2018)**.** Let a and b be positive rational integers distinct from $\pm 1, 0$. Prove that there are infinitely rational primes p such that a and b have the same order modulo p. (You may assume Dirichlet's theorem.)

Exercise 3.5.36 (All-Russian Mathematical Olympiad 2008)**.** Let S be a finite set of rational primes. Prove that there exists a positive rational integer n which can be written in the form $a^p + b^p$ for some $a, b \in \mathbb{Z}$ if and only if $p \in S$.

Exercise 3.5.37† (IMC 2010)**.** Let $f : \mathbb{R} \to \mathbb{R}$ be a function and $a < b$ two real numbers. Suppose that f is zero on $[a, b]$, and

$$\sum_{k=0}^{p-1} f\left(x + \frac{k}{p}\right) = 0$$

for any $x \in \mathbb{R}$ and any rational prime p. Prove that f is zero everywhere.

Exercise 3.5.38. What is the discriminant of Φ_n?

Exercise 3.5.39. Let k and $n \geq 1$ be coprime integers. Find the minimal polynomial of $\tan\left(\frac{2k\pi}{n}\right)$. Deduce that $\tan(q\pi)$ takes only the rational values 0 and ± 1 for rational q.

Exercise 3.5.40†**.** Let $n \geq 1$ be an integer. Prove that $\Phi_n(x) \geq (x-1)x^{\varphi(n)-1}$ with equality if and only if $n = 1$.[6]

[6] In particular, $\Phi_n(2) \geq 2^{\varphi(n)-1}$.

Chapter 4

Finite Fields

Prerequisites for this chapter: Chapters 1 and 3 and Section A.2.

The start of this chapter will be a bit technical, I hope the reader will bear with it.

Recall what a field is. We say a $(K, +, \cdot)$ is a field (we usually just write "K is a field" when the addition and multiplication are clear from the context) if $+$ and $\cdot$ have nice properties: commutativity, associativity, existence of additive identiy (0), existence of multiplicative identity (1), addition distributes over multiplication, existence of additive inverse, and, most importantly, **existence of multiplicative inverse** (except for 0). There is no need to remember all of these: a field is an integral domain where each element has a multiplicative inverse. This might seem a bit complicated, but just think of $\mathbb{Q}$ when you have to use fields.

Exercise 4.0.1. Suppose K is a field of *characteristic zero*, i.e.

$$\underbrace{1 + \ldots + 1}_{n \text{ times}}$$

(where 1 is the multiplicative identity) is never zero for any $n \geq 1$. Prove that K contains (up to relabelling of the elements) $\mathbb{Q}$.[1]

First, we discuss the simplest case of finite fields: the integers modulo p: $\mathbb{Z}/p\mathbb{Z}$. We will call this field $\mathbb{F}_p$ for "field with p elements". It is **very important** to understand that the elements of $\mathbb{F}_p$ are **not** rational integers! $p = 0$ in $\mathbb{F}_p$ (not that this is an equality and not a congruence: congruences are for rational integers while equality is just equality but in another field) while $p \neq 0$ in $\mathbb{Z}$. Thus, while we use the same notations for the elements of $\mathbb{F}_p$ and elements of $\mathbb{Z}$, **they are not the same**.

Exercise 4.0.2*. Let p be a rational prime. Prove that there exists a unique field with p elements (it's $\mathbb{Z}/p\mathbb{Z}$).

Now we can discuss what finite fields are. Their name is quite explicit: they are the fields which are also finite. However their is a way nicer characterisation of them: they are the finite extensions of some $\mathbb{F}_p$, i.e. $\mathbb{F}_p$ with some elements algebraic over $\mathbb{F}_p$ added. This is analogous to the construction of the complex numbers: you add an imaginary number i such that $i^2 = -1$ ot the real numbers $\mathbb{R}$. You can do exactly the same thing for $\mathbb{F}_3$: the polynomial $X^2 + 1$ doesn't have a root there so you can add an imaginary (formal) number i_3 such that $i_3^2 = -1$ (in $\mathbb{F}_3$), thus getting a field with 9 elements.

Exercise 4.0.3*. Prove that $F_3(i) := F_3 + iF_3$ is a field (with 9 elements). (The hard part is to prove that each element has an inverse.)

Why are we interested in finite fields other than $\mathbb{F}_p$? Well, for the same reason we are interested in algebraic numbers. It is nice to have polynomials factorise completely (we say they *split*), thus we create new fields by adding roots of polynomials to $\mathbb{F}_p$.

[1] Technically, it will usually not contain $\mathbb{Q}$ because $\mathbb{Q}$ is a very specific object. Indeed, the definition of a field is extremely sensitive: if you change the set K (relabel its elements) but keep everything else the same you get a different field. In that case we say the new field is *isomorphic* to the old one. So you must prove that K contains a field isomorphic to $\mathbb{Q}$, i.e. $\mathbb{Q}$ up to relabeling of its elements.

Let's explain a bit what we mean by that. Given an irreducible polynomial $f \in \mathbb{F}_p[X]$ of degree n, we let α be a formal object satisfying $f(\alpha)$ and then consider the field generated by α (and $\mathbb{F}_p$). It contains α so it must be also contain $\alpha^2, \ldots, \alpha^{n-1}$ and hence all the linear combinations of these elements. Conversely, Exercise 4.2.1* shows that $\mathbb{F}_p + \alpha\mathbb{F}_p + \ldots + \alpha^{n-1}\mathbb{F}_p$ is a field (has multiplicative inverses) and this is therefore what we mean by "adding a root of f to $\mathbb{F}_p$". We denote this field by $\mathbb{F}_p(\alpha)$. Iterating this process shows that, given any polynomial (not necessarily irreducible) f, we can construct a field containing $\mathbb{F}_p$ where f splits: these are exactly the finite fields we are interested in.

Finally, we come back to our earlier remark about elements of $\mathbb{F}_p$ not being integers. Here, the same is true for $\mathbb{F}_3(i_3)$: its elements are not Gaussian integers. You may protest and claim that $\mathbb{F}_3(i_3)$ is just $\mathbb{Z}[i]/3\mathbb{Z}[i]$, i.e. the Gaussian integers modulo 3. And that is true (up to relabelling of the elements) (see **??**). However imagine that we were working with $\mathbb{F}_5$ instead. Then, any i_5 satisfying $i_5^2 = -1$ must already be in $\mathbb{F}_5$ as $X^2 + 1 = (X + 2)(X - 2)$. Thus, $\mathbb{Z}[i]/5\mathbb{Z}[i]$ is very different from $\mathbb{F}_5(i_5)$ as the former has 25 elements while the latter only 5. (The former is not a field because the polynomial $X^2 + 1$ has 4 distinct roots. Equivalently, $i + 2$ has no inverse.)

You might argue that we need to distinguish the cases where the polynomial f already has a root in $\mathbb{F}_p$ and when it does not. This is not only ugly and artificial (having to distinguish these cases), but also false as what we want is for p to stay prime in $\mathbb{Q}(\alpha)$ where α is a root of f. Up to a finite number of exceptions, this is equivalent f staying irreducible in $\mathbb{F}_p[X]$ (see Exercise 6.5.35).[2]

As a last remark, I hope you are now convinced that a field with, say, p^2 elements is very different from $\mathbb{Z}/p^2\mathbb{Z}$! The latter is not even a field since p does not have an inverse!

4.1 Frobenius Morphism

Before constructing finite fields, we need to discuss some things about $\mathbb{F}_p$ itself.

Definition 4.1.1 (Frobenius)

Let p be a rational prime and R a commutative ring of *characteristic* p, meaning that $p = 0$ in R. The *Frobenius morphism* of R is $\mathrm{Frob}_R : x \mapsto x^p$.

$p = 0$ means that

$$\underbrace{1 + \ldots + 1}_{p \text{ times}} = 0;$$

this is for instance the case in $\mathbb{F}_p$ or $\overline{\mathbb{Z}}$ modulo p. The word "morphism" in this context that it's an additive map. Indeed,

$$(x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p$$

as

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = 0$$

for $k = 1, \ldots, p - 1$ (p divides the top but not the bottom).

Proposition 4.1.1*

The Frobenius morphism is indeed a morphism.

Exercise 4.1.1. Why is commutativity (of R) needed?

A direct corollary is the following.

[2] However, the intuition that finite fields are represented by algebraic integers is not completely wrong, but instead of rational primes, we need to look at $\mathcal{O}_{\mathbb{Q}(\alpha)}$ modulo a prime ideal $\mathfrak{p}$ (the definition of a prime ideal being an ideal such that $\mathcal{O}_{Q(\alpha)} \pmod{\mathfrak{p}}$ is a field). The ideal point of view is very rich and is actually the best point of view (compared to tricky uses of the fundamental theorem of symmetric polynomials), but we do not expand on this in this book. See [19].

Corollary 4.1.1*

The nth iterate of the Frobenius, Frob_R^n is also a morphism, i.e. $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ for any $x, y \in R$.

Let's see a quick application of this result.

Problem 4.1.1

Let $(a_n)_{n\geq 0}$ be the sequence defined by $a_0 = 3$, $a_1 = 0$, $a_2 = 2$ and $a_{n+3} = a_{n+1} + a_n$ for $n \geq 0$. Prove that $p \mid a_p$ for any prime number p.

Solution

A quick computation shows that $a_n = \alpha^n + \beta^n + \gamma^n \pmod p$ where $\alpha, \beta, \gamma \in \overline{\mathbb{Z}}$ are the roots of the characteristic polynomial $X^3 - X - 1$ (see Theorem C.4.1).

Thus, by Proposition 4.1.1,

$$a_p = \alpha^p + \beta^p + \gamma^p \equiv (\alpha + \beta + \gamma)^p = a_1^p = 0 \pmod p$$

as wanted. ■

Exercise 4.1.2*. Prove that $a_n = \alpha^n + \beta^n + \gamma^n$.

4.2 Existence and Uniqueness

Here, we show how to construct all finite fields and prove that there is a unique one of cardinality q for each prime power $q \neq 1$ ($\mathbb{F}_1$ doesn't exist because the definition of a field specifies that the multiplicative and additive identities are different). Although we can construct a field with p^n elements by adding a root of an irreducible polynomial $f \in \mathbb{F}_p[X]$ of degree n we do not do it that way because it is not obvious that such a polynomial exists (**??** provides a proof but uses itself finite fields), but we use this to show the field is unique (surprisingly). In fact, it is actually very surprising that it's the same for any irreducible f of degree n. Over $\mathbb{Q}$ for instance, this is completely false: $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$ (Exercise 2.1.2* shows that each $\mathbb{Q}(\sqrt{d})$ for integral squarefree d is distinct from the others).

It is useful to think of elements algebraic over $\mathbb{F}_p$ similarly to $\overline{\mathbb{Q}}$, as part of one big field and hence compatible with each other even if that is not trivial (for algebraic numbers it is as $\overline{\mathbb{Q}}$ is already part of $\mathbb{C}$, but how can we define roots of polynomials in $\mathbb{F}_p[X]$ which don't exist in $\mathbb{F}_p$?). It will be proven in Definition 4.3.1.

Proposition 4.2.1

For any rational prime p and integer $n \geq 1$, there exists a field with p^n elements.

Proof

Consider the polynomial $X^{p^n} - X$ over $\mathbb{F}_p[X]$. Factorise it as $f_1 \cdot \ldots \cdot f_k$ where $f_1, \ldots, f_k$ are irreducible in $\mathbb{F}_p[X]$ (not necessarily distinct).

We can construct a field F where $f_1, \ldots, f_n$ split (have all their roots in F) inductively using

Exercise 4.2.1*. Indeed, one can add a root of $X^{p^n} - X$ (hence a root of one of the f_i) which is not already in $\mathbb{F}_p$ to get a new field F' and repeat this process inductively until all f_i have roots in F. This must terminate as $X^{p^n} - X$ has at most p^n roots in any field.

We claim that this field has exactly p^n elements. Notice that the derivative of $X^{p^n} - X$ is 1 which is coprime with $X^{p^n} - X$ so all its roots are distinct. Denote them by $\alpha_1, \ldots, \alpha_{p^n}$. Since they all lie in F, it has at least p^n elements.

To conclude, we prove that any element of F is a root of $X^{p^n} - X$. The roots of $X^{p^n} - X$ are clearly closed under multiplication, multiplicative inverse and additive inverse, and Corollary 4.1.1 shows that they are also stable under addition. Since any element of F can be written that way, we conclude that they are all roots of $X^{p^n} - X$ and thus there are at most p^n of them.

■

Exercise 4.2.1*. Let K be a field and $f \in K[X]$ an irreducible polynomial of degree n. Prove that

$$K(\alpha) := K + \alpha K + \ldots + \alpha^{n-1} K$$

is a field, where α is defined as a formal root of f, i.e. an object satisfying $f(\alpha) = 0$.

Before proving the uniqueness of this field up to isomorphism, we need an analogue of Fermat's little theorem. Here $\mathbb{F}_q$ denotes a field with q elements.

Definition 4.2.1

For any ring R, we write $R^\times$ for the *multiplicative group* of R, i.e. the units of R.

When $R = K$ is a field, we thus have $R^\times = K \setminus \{0\}$.

Theorem 4.2.1 (Fermat's Little Theorem in Finite Fields)

For any non-zero $\alpha \in \mathbb{F}_q^\times$, we have $\alpha^{q^n - 1} = 1$. Equivalently, $\alpha^{q^n} = \alpha$ for any $\alpha \in \mathbb{F}_q$.

Proof

Let $\alpha \in \mathbb{F}_q^\times$ be a non-zero element. The function $\beta \mapsto \alpha\beta$ is a bijection from $\mathbb{F}_p$ to $\mathbb{F}_p$ since α is invertible. Thus,

$$\prod_{\beta \in \mathbb{F}_q^\times} \beta = \prod_{\beta \in \mathbb{F}_q^\times} \alpha\beta = \alpha^{q^n - 1} \prod_{\beta \in \mathbb{F}_q^\times} \beta.$$

Since $\prod_{\beta \in \mathbb{F}_q^\times} \beta \neq 0$, we conclude that $\alpha^{q^n - 1} = 1$.

■

Remark 4.2.1

For the reader knowing a bit of group theory, this can also be seen to be Lagrange's theorem applied to the multiplicative group $\mathbb{F}_p^\times$.

Before proving that finite fields are unique (up to isomorphism), we will present an application of Theorem 4.2.1 to the period of linear recurrences modulo p to further motivate the interest of finite fields.

We shall prove that the sequence $(a_n)_{n \geq 1}$ in Problem 4.1.1 has period (dividing) $p^6 - 1$ modulo p for any prime p. Try to find a proof for this seemingly elementary fact without appealing to finite fields!

Proof

$X^3 - X - 1$ factorises (in $\mathbb{F}_p[X]$!) either as three linear factors, one linear and one quadratic, or one cubic. In these cases the roots $\alpha_p, \beta_p, \gamma_p$ are respectively all in $\mathbb{F}_p$, one in $\mathbb{F}_p$ and two in $\mathbb{F}_{p^2}$, or all in $\mathbb{F}_{p^3}$. ($\alpha_p, \beta_p, \gamma_p$ are not algebraic numbers, they are (formal) algebraic elements over $\mathbb{F}_p$.)

We hence always have

$$\alpha_p^{p^6-1} = \beta_p^{p^6-1} = \gamma_p^{p^6-1} = 1$$

(as $p^2 - 1$ and $p^3 - 1$ divide $p^6 - 1$).

Finally, we conclude that

$$a_{n+p^6-1} \equiv \alpha_p^n \cdot \alpha_p^{p^6-1} + \beta_p^n \cdot \beta_p^{p^6-1} + \gamma_p^n \cdot \gamma_p^{p^6-1} = \alpha_p^n + \beta_p^n + \gamma_p^n \equiv a_n \pmod{p}$$

by Theorem 4.2.1 since $\alpha_p, \beta_p, \gamma_p \neq 0$.

In fact, we even get that the period divides $(p^2 - 1)(p^3 - 1)$.

■

By a similar argument, the Fibonacci sequence (F_n) has period dividing $p^2 - 1$ modulo any rational prime p.

Remark 4.2.2

This can actually be proven elementarily for $\mathbb{F}_{p^2}$. Indeed, any element of $\mathbb{F}_{p^2}$ can be written as $a + b\sqrt{d}$ where $d \in \mathbb{F}_p$ is not a square modulo p. Since Frob_p^2 is a morphism, it suffices to prove that $\mathrm{Frob}_p^2(\sqrt{d}) = \sqrt{d}$ to conclude that it fixes all of $\mathbb{F}_{p^2}$. But this is easy for odd p:

$$(\sqrt{d})^{p^2-1} = (d^{\frac{p+1}{2}})^{p-1} = 1.$$

Note that this argument can be written without appealing to finite fields to prove that (F_n) has period dividing $p^2 - 1$, but things already become more messy as we need to treat separately the cases where $p \in \{2, 5\}$ (because of the denominator or the square root). Also, this does not generalise to recurrences of order ≥ 3 as algebraic numbers of degree 3 are not simply of the form $a + b\sqrt[3]{d}$ (but over $\mathbb{F}_p$ they are by Theorem 4.2.2).

We now prove that finite fields are unique. For this, we shall need the fact that finite fields have prime characteristic and thus contain (a copy of) $\mathbb{F}_p$ where p is the characteristic. Indeed, if the characateristic of the finite field F is $c = \mathrm{char}\, F = ab$, then we must have $a = 0$[3] or $b = 0$ in F since $ab = 0$ in F and a field is an integral domain. By minimality of the characteristic, this means that $a = c$ or $b = c$, i.e. c is prime. F then naturally contains the copy of $\mathbb{F}_p$ where we send $a \in \mathbb{F}_p$ to[4]

$$\underbrace{1 + \ldots + 1}_{a \text{ times}}.$$

That way, we can consider finite fields as field extensions of some $\mathbb{F}_p$, as stated in the beginning of the chapter.

Theorem 4.2.2

Let q be an integer. If $q \neq 1$ is a power of a prime then there exists a unique (up to isomorphism) field with q elements, otherwise there is none.

[3] Here we abusively mean $\underbrace{1 + \ldots + 1}_{a \text{ times}}$.

[4] By this we mean that we take a representative $A \in \mathbb{N}$ of a and then add 1 A times. This is well defined since they $\mathbb{F}_p$ and F have the same characteristic.

This proof is not super instructive and slightly technical so it can be skipped upon a first reading. (However once understood, one sees that it only consists of more or less trivial technicalities. The key point is Fermat's little theorem.)

Proof

The fact that if F is a finite field of cardinality q then $q \neq 1$ is a prime power follows from Proposition C.1.4.

We now show that finite fields of cardinality p^n are unique, existence was proven in Proposition 4.2.1. We proceed by induction on n. It is clearly true for $n = 1$.

Suppose $\mathbb{F}_{p^m}$ is unique for $m < n$ and let F, F' be two fields with p^n elements. Since $p + p^2 + \ldots + p^{n-1} < p^n$, there is some element α of F which is not in any of the previous $\mathbb{F}_{p^m}$. (By this we mean that $\alpha^{p^m} \neq \alpha$ for any $m < n$. Indeed, this is the property that defines elements of $\mathbb{F}_{p^m}$. We do not actually need the induction hypothesis: the polynomial $(X^p - X) \cdot \ldots \cdot (X^{p^{n-1}} - X)$ has less than p^n roots so it doesn't vanish on all of $\mathbb{F}_{p^n}$.)

Let k be the degree of α so that $\mathbb{F}_p(\alpha)$ is a field with p^k elements. If $k < n$, by the induction hypothesis this must be $\mathbb{F}_k$ so $\alpha \in \mathbb{F}_k$ which is not the case. (Again, this means that $\alpha^{p^k} = \alpha$.) Conversely, if $k > n$, then $\mathbb{F}_p(\alpha)$ has $p^k > p^n$ elements which is impossible since it is contained in F, a field of cardinality p^n. Thus α has degree n (coincidentally this shows that there always exists an irreducible polynomial in $\mathbb{F}_p[X]$ of degree n).

Accordingly, we conclude that $F = \mathbb{F}_p(\alpha)$. By Theorem 4.2.1, we know that $f \mid X^{p^n} - X$. Again, by Theorem 4.2.1, we know that $X^{p^n} - X$ splits in F', so f must also split in F'.

To conclude, let β be a root of f in F'. Then, we again have $F' = \mathbb{F}_p(\beta)$. Since α and β have the same minimal polynomial, F and F' are the same except that α has been relabelled as β. Indeed, just relabel $g(\alpha) \in F$ as $g(\beta) \in F'$.

This gives us an *isomorphism* (a relabelling conserving the structure) between F and F': it is clear that it is additive and multiplicative (hence same field structure) so we just need to check that it is well-defined. This follows from the fact that α and β have the same minimal polynomials: if $g(\alpha) = h(\alpha)$ then $g \equiv h \pmod{f}$ so $g(\beta) = h(\beta)$.

■

Remark 4.2.3

Some readers might recognise that the proofs of uniqueness and existence are just saying that $\mathbb{F}_{p^n}$ is the *splitting field* of $X^{p^n} - X$.

Note that our proof also yields the following corollary.

Corollary 4.2.1

Any finite field $\mathbb{F}_{p^n}$ has the form $\mathbb{F}_p(\alpha)$ for some α, i.e. is generated by one element.

4.3 Properties

From the uniqueness of finite fields and Theorem 4.2.1 we can deduce a few fundamental corollaries.

Corollary 4.3.1*

The nth iterate of the Frobenius, Frob_p^n, fixes exactly $\mathbb{F}_{p^n}$.

Proof

Theorem 4.2.1 says that $\mathbb{F}_{p^n}$ is fixed by Frob_p^n. Conversely, this polynomial can have at most p^n roots, so any element satisfying $\alpha^{p^n} = \alpha$ must lie in $\mathbb{F}_{p^n}$.

■

This might seem trivial but is in fact very useful as it allows us to compare elements of different finite fields. For instance, α is in $\mathbb{F}_p$ if and only if $\alpha^p = \alpha$ (we will use this in Proposition 4.4.2).

Corollary 4.3.2*

Let m and n be positive integers. We have the inclusion $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if $m \mid n$.

By this, we mean that $\mathbb{F}_{p^n}$ has a subfield isomorphic to $\mathbb{F}_{p^n}$ if and only if $m \mid n$.

Proof

This amounts to saying that the roots of $X^{p^m} - X$ are all roots of $X^{p^n} - X$, i.e. that $X^{p^m-1} - 1 \mid X^{p^n-1} - 1$ since they are distinct. By Exercise 4.3.1* this means that $p^m - 1 \mid p^n - 1$. By the same exercise, this is equivalent to $m \mid n$.

■

Exercise 4.3.1*. Let a and b be positive integers and K a field. Prove that $X^a - 1$ divides $X^b - 1$ in K if and only if $a \mid b$. Similarly, if $x \geq 2$ is a rational integer, prove that $x^a - 1$ divides $x^b - 1$ in $\mathbb{Z}$ if and only if $a \mid b$.

Corollary 4.3.3*

Let α be a root of an irreducible polynomial $f \in \mathbb{F}_p[X]$ of degree m. Then, $\alpha \in \mathbb{F}_{p^n}$ if and only if $m \mid n$.

Proof

$\mathbb{F}_p(\alpha)$ is a field with p^m elements so is $\mathbb{F}_{p^m}$. Thus, $\alpha \in \mathbb{F}_{p^n}$ if and only if $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ which is equivalent to $m \mid n$ by Corollary 4.3.2.

■

In particular, from the uniqueness of finite fields, we deduce that any polynomial in $\mathbb{F}_p[X]$ of degree 2 splits in $\mathbb{F}_{p^2}$ which was not obvious at first. Over $\overline{\mathbb{Q}}$ this is again completely false: $\sqrt{2} + \sqrt{3}$ has degree $4 \neq 2$.

Remark 4.3.1

The uniqueness of $\mathbb{F}_{p^2}$ can actually be seen quite easily: if a and b are quadratic non-residues in $\mathbb{F}_p$ then there is some $c \in \mathbb{F}_p$ such that $a = c^2 b$ (so $\sqrt{a} = c\sqrt{b}$) (see Section 4.5). The degree 2 case in general is a bit pathological because a polynomial is either irreducible or splits. If this example didn't convince you, you can think about the fact that each polynomial of degree 3 has all its roots in $\mathbb{F}_{p^6}$ which is not obvious at all. Why would approximately $3p^3$ elements generate a field of cardinality only p^6 when one element (of degree 7) is sufficient to generate $p^7 - 1$ others?

Exercise 4.3.2*. Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree n. Prove that f splits over $\mathbb{F}_{p^{n!}}$.

With this we can define the *algebraic closure* of $\mathbb{F}_p$, consisting of the elements algebraic over $\mathbb{F}_p$ (roots of polynomials with coefficients in $\mathbb{F}_p$). Here is how this is done: we pick a field with p elements $\mathbb{F}_p$, a field with p^2 elements $\mathbb{F}_{p^2}$ which contains $\mathbb{F}_p$ (we can do this by relabelling the elements), a field with p^6 elements $\mathbb{F}_{p^6}$ which contains $\mathbb{F}_{p^2}$, etc. We thus get a chain of finite fields

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^6} \subseteq \ldots \subseteq \mathbb{F}_{p^{n!}} \subseteq \ldots$$

the union of which contains all finite fields since any n divides $n!$ so $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^{n!}}$. Thus, any polynomial $f \in \mathbb{F}_p[X]$ as a root in this union, and one can show that in fact all the roots must lie there, for instance using Exercise 4.3.2*. This is the algebraic closure of $\mathbb{F}_p$.

Definition 4.3.1

The *algebraic closure* of $\mathbb{F}_p$, $\overline{\mathbb{F}}_p$, is defined as the elements algebraic over $\mathbb{F}_p$, i.e. the union $\bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.

Note that this union makes sense as if $\alpha \in \mathbb{F}_{p^n}$ and $\beta \in \mathbb{F}_{p^m}$ then α and β are both in $\mathbb{F}_{p^{mn}}$ so their sum and product are well defined.

Remark 4.3.2

As said at the beginning of the chapter, $\overline{\mathbb{F}}_p$ is **not** $\overline{\mathbb{Z}}/p\overline{\mathbb{Z}}$, the ring of algebraic integers modulo p! Indeed, the latter is not a field since it's not an integral domain: $\sqrt{p} \cdot \sqrt{p} \equiv 0$ but $\sqrt{p} \not\equiv 0$ (as $\frac{\sqrt{p}}{p} = \frac{1}{\sqrt{p}} \notin \overline{\mathbb{Z}}$)! It can even be shown that any polynomial $f \in \overline{\mathbb{Z}}/p\overline{\mathbb{Z}}[X]$ has infinitely many roots in $\overline{\mathbb{Z}}/p\overline{\mathbb{Z}}$ (see Exercise 4.6.17).

Sometimes, when we want to evaluate a symmetric expression of algebraic numbers modulo p, it can be useful to replace these algebraic numbers by the corresponding elements of $\overline{\mathbb{F}}_p$ with the fundamental theorem of symmetric polynomials (analogous to Proposition 1.3.1) to use finite field theory. (Section 6.2 of Chapter 6 will show that any expression of algebraic numbers which is rational can be written as a symmetric expression of some algebraic numbers and their conjugates, implying that this replacement from $\overline{\mathbb{Q}}$ to $\overline{\mathbb{F}}_p$ can always be made (when p doesn't divide the denominator of the expression).)

Finally, we have one last result that again highlights how much better the situation is over $\overline{\mathbb{F}}_p$ compared to $\overline{\mathbb{Q}}$.

Theorem 4.3.1

Let $f \in \mathbb{F}_p[X]$ be an irreducible polynomial (in $\mathbb{F}_p[X]$) of degree n. Suppose $\alpha \in \mathbb{F}_{p^n}$ is one its roots (by Corollary 4.3.3). Then, all its roots are $\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}$.

In other words, if we know a root of f, we know all of its roots and they are generated by the Frobenius morphism! This is completely false over $\overline{\mathbb{Q}}$!

Proof

By Proposition 4.1.1, $f(X^{p^k}) = f(X)^{p^k}$ so α^{p^k} is always a root of f. In addition, these are all distinct as $\alpha^{p^i} = \alpha^{p^j}$ for some $i > j$ implies that

$$\alpha^{p^{i-j}} = \alpha$$

so α is fixed by Frob_{p^k} where $k = i - j < n$. Thus, α would be in $\mathbb{F}_{p^k}$ but this is impossible as

$\mathbb{F}_p(\alpha) := \mathbb{F}_p + \alpha\mathbb{F}_p + \ldots + \alpha^{n-1}\mathbb{F}_p$ has p^n elements while $\mathbb{F}_{p^k}$ has $p^k < p^n$ elements. ■

This proposition will in particular allow us to determine how cyclotomic polynomials factorise in $\mathbb{F}_p$.

4.4 Cyclotomic Polynomials

Recall Theorem 3.3.1 if $a \in \mathbb{F}_p$ and $\Phi_n(a) = 0$, the order of a is $\frac{n}{p^{v_p(n)}}$. This holds true over arbitrary finite fields too. We define the order of a non-zero element $\alpha \in \overline{\mathbb{F}}_p$ to be the smallest $k > 0$ such that $\alpha^k = 1$. Primitive mth roots over $\overline{\mathbb{F}}_p$ are defined as elements of order m. This time however, there are no primitive mth roots when $p \mid m$ as $\alpha^{m'p} = 1$ implies $(\alpha^{m'} - 1)^p = 0$ so $\alpha^{m'} = 1$. However, when $p \nmid m$, primitive mth roots always exist because $X^m - 1$ has distinct roots (its derivative mX^{m-1} is non-zero and thus coprime with $X^m - 1$). Theorem 3.3.1 thus takes the following form.

Proposition 4.4.1

Let $n = p^k m \geq 1$ be an integer where $k = v_p(n)$. Then, over $\overline{\mathbb{F}}_p$,

$$\Phi_n = \Phi_m^{\varphi(p^k)} = \left(\prod_{\omega \in \overline{\mathbb{F}}_p \text{ primitive } m\text{th root}} X - \omega \right)^{\varphi(p^k)}.$$

Exercise 4.4.1*. Prove Proposition 4.4.1.

In particular, there always exists a primitive root of $\mathbb{F}_{p^n}$, i.e. an element g of order $p^n - 1$ (which thus generates all the other ones): they are the roots of Φ_{p^n-1} (and these are all in $\mathbb{F}_{p^n}$ as $\Phi_{p^n-1} \mid X^{p^n} - X = \prod_{\alpha \in \mathbb{F}_{p^n}} X - \alpha$ by Theorem 4.2.1.)

Exercise 4.4.2*. Let $p \nmid m$ be a positive integer. Prove that Φ_m has a root in $\mathbb{F}_{p^n}$ if and only if $m \mid p^n - 1$.

Here is an application of Proposition 4.4.1.

Problem 4.4.1 (Brazilian Mathematical Olympiad 2017 Problem 6)

Let $3 \neq p \mid a^3 - 3a + 1$ be a rational prime where a is some rational integer. Prove that $p \equiv \pm 1 \pmod 9$.

Solution

Perform the substitution $a = \alpha + \frac{1}{\alpha}$ where $\alpha \in \mathbb{F}_{p^2}$. This is possible as the polynomial $X^2 - aX + 1$ has degree two and thus has its roots in $\mathbb{F}_{p^2}$. Then,

$$a^3 - 3a + 1 = \left(\alpha + \frac{1}{\alpha}\right)^3 - 3\left(\alpha + \frac{1}{\alpha}\right) + 1 = \alpha^3 + \frac{1}{\alpha^3} + 1.$$

Thus,

$$\Phi_9(\alpha) = \alpha^6 + \alpha^3 + 1 = 0.$$

We conclude that Φ_9 has a root in $\mathbb{F}_{p^2}$ which means that $9 \mid p^2 - 1$ by Exercise 4.4.2*. This is exactly equivalent to $p \equiv \pm 1 \pmod 9$! ■

Exercise 4.4.3. Prove that $p^2 \equiv 1 \pmod 9$ if and only if $p \equiv \pm 1 \pmod 9$.

Remark 4.4.1

This seems a bit miraculous and I don't really have a good explanation for the motivation apart from "$p \equiv \pm 1 \pmod 9$ is the same as $9 \mid p^2 - 1$ which makes us think of Φ_9 in $\mathbb{F}_{p^2}$" or "$a = \alpha + \frac{1}{\alpha}$ makes things cancel well".

We can in fact prove that the converse also holds: if $p \equiv \pm 1 \pmod 9$, $X^3 - 3X + 1$ has a root in $\mathbb{F}_p$. We have seen that the roots of this polynomial have the form $\omega + \frac{1}{\omega}$ where $\omega \in \overline{\mathbb{F}}_p$ is a primitive 9th root of unity. It remains to check that this is indeed an element of $\mathbb{F}_p$: by Corollary 4.3.1 this amounts to checking that

$$\left(\omega + \frac{1}{\omega}\right)^p = \omega + \frac{1}{\omega}.$$

Since $p \equiv \pm 1 \pmod 9$ and $\omega^9 = 1$, the LHS is

$$\omega^p + \frac{1}{\omega^p} = \omega^{\pm 1} + \omega^{\mp 1}$$

which is indeed equal to $\omega + \frac{1}{\omega}$.

In fact, we can generalise this problem to find, for any n, a polynomial Ψ_n which has a root in $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod n$ (with some possible exceptions if $p \mid n$). By adapting the previous solution, we wish to have

$$\Psi_n\left(X + \frac{1}{X}\right) = \frac{\Phi_n(X)}{X^{\varphi(n)/2}}$$

(for $n \geq 3$, the other cases are trivial). Such a polynomial indeed exists: the key point is that $\Phi_n(X)/X^{\varphi(n)/2}$ is symmetric in X and $1/X$ (Exercise 3.1.6*). Hence, by the fundamental theorem of symmetric polynomials, it is a polynomial in $X + \frac{1}{X}$ and $X \cdot \frac{1}{X}$, i.e. a polynomial in $X + \frac{1}{X}$.

Remark 4.4.2

One can also prove that there exists a polynomial T_n such that $T_n(X + 1/X) = X^n + 1/X^n$ by induction on n. This polynomial is called the nth *Chebyshev polynomial*.

Remark 4.4.3

The polynomial Ψ_n we have constructed is in fact the minimal polynomial of $2\cos\left(\frac{2\pi}{n}\right)$, see Exercise 3.2.5. For the sake of consistency we can thus also artifically define $\Psi_1 = X - 2$ and $\Psi_2 = X + 2$ (they also satisfy Proposition 4.4.2)

Exercise 4.4.4. Compute $\Psi_1, \ldots, \Psi_8$.

Proposition 4.4.2

Let $p \nmid n$ be a prime number. Then, Ψ_n has a root in $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod n$.

Proof

By definition, the roots of Ψ_n are $\omega + \frac{1}{\omega}$ where ω is a root of Φ_n, i.e. an element of order n. Let's see when this is in $\mathbb{F}_p$. We have

$$\left(\omega + \frac{1}{\omega}\right)^p = \omega^p + \frac{1}{\omega^p}.$$

Note that

$$X + 1/X - (\omega + 1/\omega) = (X - \omega)(X - 1/\omega)/X.$$

Thus, $\omega^p + \frac{1}{\omega^p} = \omega + \frac{1}{\omega}$ if and only if $\omega^p = \omega^{\pm 1}$. This is exactly equivalent to $p \equiv \pm 1 \pmod{n}$. ■

From this we get the following corollary, similar to Exercise 3.3.8*.

Theorem 4.4.1

For any positive rational integer n, there exist infinitely many rational primes congruent to -1 modulo n.

Proof

We do a Euclid-type proof. Suppose that there are only finitely many such primes $p_1, \ldots, p_k$. Let a be the constant coefficient of Ψ_n. We shall consider the polynomial $f = \Psi_n(aX)/a$, which now has constant coefficient 1. Consider $f(mnp_1 \cdot \ldots \cdot p_k)$ for some rational integer m. Since it is congruent to 1 modulo $np_1 \cdot \ldots \cdot p_k$, its prime factors are distinct from $p_1, \ldots, p_k$ and the ones dividing n. Thus, they must all be 1 modulo n by assumption. (If one doesn't want to compute $\Psi_n(0)$, they can also see it as a corollary of Theorem 5.2.1.)

How do we reach a contradiction from this? The key point is to go into **negatives**: if we manage to have $\Psi_n(mnp_1 \cdot \ldots \cdot p_k) < 0$, it will be congruent to -1 modulo n. Then, we can add a large multiple of $np_1 \cdot \ldots \cdot p_k$ to get back into positives (since the leading coefficient of Ψ_n is 1) while still being congruent to -1 modulo n. Thus, it must have a prime factor which isn't congruent to 1 modulo n and that will be the new prime factor we were looking for (and our contradiction).

For this, note that the complex roots of Ψ_n are all real and distinct as they are $\cos\left(\frac{2k\pi}{n}\right)$ for $\gcd(k, n) = 1$. In particular, there is some interval $[a, b]$ such that Ψ_n is negative there. The key point now is to consider $m \in \mathbb{Q}$ instead of $m \in \mathbb{Z}$, but with some restrictions. We ask that the prime factors of its denominator are congruent to 1 modulo n (and in particular distinct from $p_1, \ldots, p_k$ and the prime factors of n).

Consider such an m satisfying this and also $r := mnp_1 \cdot \ldots \cdot p_k \in [a, b]$ (this is possible by Exercise 4.4.5*). The prime factors of the numerator of $\Psi_n(r)$ are all congruent to 1 modulo n by assumption. Indeed, they're distinct from $p_1, \cdot, p_k$ and do not divide n as

$$\Psi_n(r) \equiv \Psi_n(0) \equiv \pm 1 \pmod{np_1 \cdot \ldots \cdot p_k}.$$

Thus, either they divide the numerator of m in which case they are congruent to 1 modulo n by assumption, or Ψ_n has a root in $\mathbb{F}_p$ which again means that $p \equiv 1 \pmod{n}$ (as it's not congruent to -1).

This means that $\Psi_n(r) \equiv -1 \pmod{n}$ since its negative and all its prime factors are congruent to 1 modulo n. We have reached the conclusion we wanted: $\Psi_n(r + Nnp_1 \cdot \ldots \cdot p_k)$ will be positive but still congruent to -1 modulo n for some large n and will thus have a new prime factor congruent to -1 (distinct from the prime factors of the denominator of r by assumption). ■

Exercise 4.4.5*. Let $p \neq 0$ be an integer. Prove that the numbers m/p^k with $m \in \mathbb{Z}$ and $k \in \mathbb{N}$ are dense in $\mathbb{R}$.

Exercise 4.4.6*. Prove that the leading coefficient of Ψ_n is 1.

Finally, we discuss the factorisation of cyclotomic polynomials in $\mathbb{F}_p[X]$. While they are irreducible in $\mathbb{Q}[X]$, over $\mathbb{F}_p$ the situation is quite different.

Proposition 4.4.3

Let $n \geq 1$ be an integer. The nth cyclotomic polynomial Φ_n factorises as a product of $\frac{\varphi(n)}{k}$ irreducible polynomials, where k is the order of p modulo n. In particular, it stays irreducible if and only if p is a primitive root modulo n.

Proof

It suffices to show that each irreducible factor has degrre k. By Theorem 4.3.1, this is equivalent to k being the smallest positive integer ℓ such that $\omega^{p^\ell} = 1$ for any element ω of order n. This is very easy to show: $\omega^{p^\ell} = 1$ if and only if $p^\ell \equiv 1 \pmod{n}$ since ω has order n by definition. Thus, ℓ is the smallest integer such that $p^\ell \equiv 1 \pmod{n}$ which is, by definition, the order of p modulo n.

■

As a perhaps surprising corollary, $\Phi_8 = X^4 + 1$ is irreducible in $\mathbb{Q}[X]$ but reducible in any $\mathbb{F}_p[X]$ as there is no primitive root modulo 8.

4.5 Quadratic Reciprocity

We are interested in knowing when an element $a \in \mathbb{F}_p$ is a perfect square, i.e. when there exists a $b \in \mathbb{F}_p$ such that $a = b^2$. Equivalently, we want to know how the polynomial $X^2 - a$ factorises in $\mathbb{F}_p[X]$. We thus make the following definitions.

Definition 4.5.1 (Quadratic Residues and Non-Residues)

Given a **non-zero** $a \in \mathbb{F}_p$, we say a is a *quadratic residue* if it is a square in $\mathbb{F}_p$. Otherwise, we say it is a *quadratic non-residue*.

Note that 0 is not a quadratic residue nor a non-residue (it's "zero"). The reason for this definition will become clear shortly. Using primitive roots, one can easily prove the following criterion.

Proposition 4.5.1 (Euler's Criterion)

An element $a \in \mathbb{F}_p$ is a quadratic residue if and only if $a^{\frac{p-1}{2}} = 1$. Similarly, a is a quadratic non-residue if and only if $a^{\frac{p-1}{2}} = -1$.

Exercise 4.5.1*. Prove Proposition 4.5.1.

Based on this result, we make the following definition.

Definition 4.5.2 (Legendre Symbol)

Let p be an odd rational prime. Given an $a \in \mathbb{F}_p$, we define the *Legendre symbol* of a, $\left(\frac{a}{p}\right)$ to be the integer among $\{-1, 0, 1\}$ which is congruent to $a^{\frac{p-1}{2}}$. We also define $\left(\frac{1}{2}\right) = 1$ and $\left(\frac{0}{2}\right) = 0$.

We could have also defined the Legendre symbol before stating Euler's criterion (0 if $a = 0$, 1 if a is quadratic residue, -1 otherwise) but one very nice property of this object is that it's *multiplicative* (by Euler's criterion).

Another way of thinking about the Legendre symbol is that $1+\left(\frac{a}{p}\right)$ counts (without multiplicity) the number of roots of X^2-a in $\mathbb{F}_p$: it's $1+0=1$ when $a=0$, $1+1=2$ when a is a quadratic residue, and $1-1=0$ when a is a quadratic non-residue.

Let's first analyze $\left(\frac{-1}{p}\right)$.

Theorem 4.5.1 (First Supplement of the Quadratic Reciprocity Law)

Let p be an odd prime. Then, $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

Proof

The polynomial $X^2-(-1)=\Phi_4$ has a root in $\mathbb{F}_p$ if and only if $4 \mid p-1$ which is exactly what we wanted to show.

■

We now state the quadratic reciprocity law. So far, we have only studied relations between finite fields of fixed characteristic p. This result provides a very beautiful link between the structure of $\mathbb{F}_p$ and $\mathbb{F}_q$ for distinct primes p and q.

Theorem 4.5.2 (Quadratic Reciprocity Law)

Let p and q be distinct odd rational primes. Then,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Remark 4.5.1

Technically, this statement doesn't make sense because $\left(\frac{p}{q}\right)$ is defined for $p\in\mathbb{F}_q$ and not $p\in\mathbb{Z}$, and $\left(\frac{q}{p}\right)$ is defined for $q\in\mathbb{F}_p$ and not $q\in\mathbb{Z}$. This is of course very easy to fix: we define $\left(\frac{a}{p}\right)$ for $a\in\mathbb{Z}$ as $\left(\frac{a \pmod p}{p}\right)$. We will make many such identifications throughout this book.

Theorem 4.5.3 (Second Supplement of the Quadratic Reciprocity Law)

Let p be an odd prime. Then, $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

Combined with the second supplement of this theorem, this allows us to compute (more or less efficiently) arbitrary Legendre symbols since the Legendre symbol is multiplicative,. Indeed, to compute $\left(\frac{a}{p}\right)$ we can suppose $a\in[p]$, then consider its prime factorisation $a=q_1\cdot\ldots\cdot q_n$ and use the quadratic reciprocity law and its second supplement to reduce the computation of $\left(\frac{a}{p}\right)$ to $\left(\frac{p}{q_k}\right)$ where $q_k<p$ and repeat the process sufficiently many times.

Exercise 4.5.2. Compute $\left(\frac{77}{101}\right)$.

In fact, we have already proven the second supplement with our Proposition 4.4.2.

Proof of the Second Supplement

Notice that $\Psi_8 = X^2 - 2$. But, by Proposition 4.4.2, this polynomial has a root in $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \pmod 8$ which is exactly equivalent to $(-1)^{\frac{p^2-1}{8}} = 1$.

■

Exercise 4.5.3. Prove that $\Psi_8 = X^2 - 2$ and that $(-1)^{\frac{p^2-1}{8}} = 1$ if and only if $p \equiv \pm 1 \pmod 8$.

Proof of the Quadratic Reciprocity Law

We shall make an ingenious use of the Frobenius morphism of $\overline{\mathbb{Z}} \pmod p$. Let $\omega \in \overline{\mathbb{Z}}$ be a primitive qth root of unity.

Define the ℓth quadratic *Gauss sum*

$$g_\ell = \sum_{k \in \mathbb{F}_q} \left(\frac{k}{q}\right) \omega^{k\ell} = \left(\frac{\ell}{q}\right) g$$

for $\ell \in \mathbb{F}_q$ where $g = g_1$. We will prove that $g^2 = \left(\frac{-1}{q}\right) q$. Note that we can already know, prior to the computation, that g^2 is a rational integer by Exercise 4.5.5*.

Since we wish to compute g^2, we expand g^2:

$$g^2 = \left(\sum_{i \in \mathbb{F}_q} \left(\frac{i}{q}\right) \omega^i\right) \left(\sum_{j \in \mathbb{F}_q} \left(\frac{j}{q}\right) \omega^j\right) = \sum_{i,j \in \mathbb{F}_q} \left(\frac{ij}{q}\right) \omega^{i+j}.$$

Now we use a well known trick: the unity root filter we encoutered in Exercise A.3.9†. The idea is that, when we sum ω^n for some fixed n over the other qth roots of unity raised to the nth power, i.e. consider $\sum_{k \in \mathbb{F}_q} \omega^{kn}$, we get massive simplification. Hence, consider the sum $\delta(n) := \sum_{k \in \mathbb{F}_q} \omega^{kn}$ for $n \in \mathbb{F}_q$. When $n = 0$ (in $\mathbb{F}_q$), this sum is q, otherwise it's

$$\frac{\omega^{qn} - 1}{\omega^n - 1} = 0.$$

We can know finish our computation of g^2:

$$\begin{aligned}
(q-1)g^2 &= \sum_{\ell \in \mathbb{F}_q} g_\ell^2 \\
&= \sum_{\ell \in \mathbb{F}_q} \sum_{i,j \in \mathbb{F}_q} \left(\frac{ij}{q}\right) \omega^{(i+j)\ell} \\
&= \sum_{i,j \in \mathbb{F}_q} \left(\frac{ij}{q}\right) \sum_{\ell \in \mathbb{F}_q} \omega^{(i+j)k} \\
&= \sum_{i,j \in \mathbb{F}_q} \left(\frac{ij}{q}\right) \delta(i+j) \\
&= \sum_{i \in \mathbb{F}_q} \left(\frac{-i^2}{q}\right) q \\
&= (q-1) \left(\frac{-1}{q}\right).
\end{aligned}$$

Hence, $g^2 = \left(\frac{-1}{q}\right) q$ as wanted.

On the one hand,

$$g^p = gq^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \equiv g\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \pmod p$$

by the previous computation. On the other hand, $g^p \equiv g_p = g\left(\frac{p}{q}\right) \pmod p$ by Frobenius. Therefore,

$$g\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \equiv g\left(\frac{p}{q}\right) \pmod p.$$

We want to divide both sides by g but we don't know if g is invertible (actually we do from Exercise 1.5.24†). Instead, we multiply both sides by g to transform g into $g^2 = \left(\frac{-1}{q}\right)q$ which is indeed invertible modulo p as $p \neq q$. Finally, we get

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right) \equiv \left(\frac{p}{q}\right) \pmod p.$$

Since both sides are ± 1, they must be equal which is exactly what we wanted to prove.

■

Exercise 4.5.4*. Prove that, for any $\ell \in \mathbb{F}_q$, $g_\ell = \left(\frac{\ell}{q}\right)g$.

Exercise 4.5.5*. Prove without computing g^2 that g has exactly 2 conjugates, i.e. is a quadratic number.

4.6 Exercises

Dirichlet Convolutions

Exercise 4.6.1† (Dirichlet Convolution)**.** A function f from $\mathbb{N}^*$ to $\mathbb{C}$ is said to be an *arithmetic function*. Define the *Dirichlet convolution*[5] $f * g$ of two arithmetic functions f and g as

$$n \mapsto \sum_{d|n} f(d)g(n/d) = \sum_{ab=n} f(a)g(b).$$

Prove that the Dirichlet convolution is associative. In addition, prove that if f and g are *multiplicative*[6], meaning that $f(mn) = f(m)f(n)$ and $g(mn) = g(m)g(n)$ for all **coprime** $m, n \in \mathbb{N}$, then so is $f * g$.

Exercise 4.6.2† (Möbius Inversion)**.** Define the *Möbius function* $\mu : \mathbb{Z}_{\geq 1} \to \{-1, 0, 1\}$ by $\mu(n) = (-1)^k$ where k is the number of prime factors of n if n is squarefree, and $\mu(n) = 0$ otherwise. Define also δ as the function mapping 1 to 1 and everything else to 0. Prove that δ is the identity element for the Dirichlet convolution: $f * \delta = \delta * f = f$ for all arithmetic functions f. In addition, prove that μ is the inverse of 1 for the Dirichlet convolution, meaning that $\mu * 1 = 1 * \mu = \delta$ where 1 is the function $n \mapsto 1$.[7]

Exercise 4.6.3† (Prime Number Theorem in Function Fields)**.** Prove that the number of irreducible polynomials in $\mathbb{F}_p[X]$ of degree n is

$$N_n = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)p^d$$

and show that this is asymptotically equivalent to $\frac{p^n}{\log_p(p^n)}$.

[5] The Dirichlet convolution appears naturally in the study of *Dirichlet series*: the product of two Dirichlet series $\sum_{n=1}^{\infty}\frac{f(n)}{n^s}$ and $\sum_{n=1}^{\infty}\frac{g(n)}{n^s}$ is the Dirichlet series corresponding to the convolution of the coefficients $\sum_{n=1}^{\infty}\frac{(f*g)(n)}{n^s}$.

[6] This terminology has conflicting meanings: in algebra, it means that $f(xy) = f(x)f(y)$ for all x, y, while for arithmetic functions, it only means that $f(xy) = f(x)f(y)$ for coprime x, y.

[7] This also explains how we found the formula for Φ_n from Exercise 3.5.19

Linear Recurrences

Exercise 4.6.4† (China TST 2008)**.** Define the sequence $(x_n)_{n\geq 1}$ by $x_1 = 2$, $x_2 = 12$ and $x_{n+2} = 6x_{n+1} - x_n$ for $n \geq 0$. Suppose p and q are rational primes such that $q \mid x_p$. Prove that, if $q \neq 2, 3$, then $q \geq 2p - 1$.

Exercise 4.6.5 (Korean Mathematical Olympiad 2013 Final Round)**.** Let a and b be two coprime positive rational integers. Define the sequences $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ by

$$(a + b\sqrt{2})^{2n} = a_n + b_n\sqrt{2}$$

for $n \geq 0$. Find all rational primes for which there is some positive rational integer $n \leq p$ such that $p \mid b_n$.

Exercise 4.6.6†**.** Let $p \neq 2, 5$ be a prime number. Prove that $p \mid \mathbb{F}_{p-\varepsilon}$ where $\varepsilon = \left(\frac{5}{p}\right)$.

Exercise 4.6.7†**.** Let $p \neq 2, 5$ be a rational prime. Prove that $p \mid F_p - \left(\frac{5}{p}\right)$.

Exercise 4.6.8†**.** Let $m \geq 1$ be an integer and p a rational prime. Find the maximal possible period modulo $p \geq m$ of a sequence satisfying a linear recurrence of order m.

Exercise 4.6.9†**.** Let $f \in \mathbb{Z}[X]$ be a polynomial and $(a_n)_{n\geq 0}$ be a linear recurrence of rational integers. Suppose that $f(n) \mid a_n$ for any rational integer $n \geq 0$. Prove that $\left(\frac{a_n}{f(n)}\right)$ is also a linear recurrence.[8]

Polynomials and Elements of $\overline{\mathbb{F}}_p$

Exercise 4.6.10. Suppose $f \in \mathbb{F}_p[X]$ is such that $f \mid X^n - 1$ implies $n > p^{\deg f}$. Prove that f is irreducible in $\mathbb{F}_p[X]$.

Exercise 4.6.11†**.** Let $a \in \mathbb{F}_p$ be non-zero. Prove that $X^{p^n} - X - a$ is irreducible over $\mathbb{F}_p$ if and only if $n = 1$, or $n = p = 2$.

Exercise 4.6.12† (ISL 2003)**.** Let $(a_n)_{n\geq 0}$ be a sequence of rational integers such that $a_{n+1} = a_n^2 - 2$. Suppose an odd rational prime p divides a_n. Prove that $p \equiv \pm 1 \pmod{2^{n+2}}$.

Exercise 4.6.13. Let $f \in \mathbb{F}_p[X]$ be a polynomial. Prove that f has a double root in $\overline{\mathbb{F}}_p$ if and only if its discriminant is zero.

Exercise 4.6.14†**.** Let $f \in \mathbb{F}_p[X]$ be an irreducible polynomial of odd degree. Prove that its discriminant is a square in $\mathbb{F}_p$.

Exercise 4.6.15† (Chevalley-Warning Theorem)**.** Let $f_1, \ldots, f_m \in \mathbb{F}_{p^k}[X_1, \ldots, X_n]$ be polynomials such that $d_1 + \ldots + d_m < n$, where d_i is the degree of f_i. Prove that, if $f_1, \ldots, f_m$ have a common root in $\mathbb{F}_{p^k}$, then they have another one.

Exercise 4.6.16. Prove that

$$\overline{\mathbb{F}}_p = \mathbb{F}_p(\{\omega \in \overline{\mathbb{F}}_p \mid \omega \text{ has prime order}\}).$$

Exercise 4.6.17. Prove that any polynomial $f \in \overline{\mathbb{Z}}/p\overline{\mathbb{Z}}[X]$ has infinitely many roots in $\overline{\mathbb{Z}}/p\overline{\mathbb{Z}}$.

Exercise 4.6.18 (Miklós Schweitzer 2018)**.** Suppose $X^4 + X^3 + 2X^2 - 4X + 3$ has a root in $\mathbb{F}_p$. Prove that p is a fourth power modulo 13.

[8] In fact, the Hadamard quotient theorem states that if a linear recurrence b_n always divides another linear recurrence a_n then $\left(\frac{a_n}{b_n}\right)$ is also a linear recurrence.

Squares and the Law of Quadratic Reciprocity

Exercise 4.6.19†. Let q be a prime power, $a \in \mathbb{F}_q^\times$ and $m \geq 1$ an integer. Prove that a is an mth power in $\mathbb{F}_q$ if and only if $a^{\frac{p-1}{\gcd(p-1,m)}} = 1$.

Exercise 4.6.20†. Let a be a rational integer. Suppose a is quadratic residue modulo every rational prime $p \nmid a$. Prove that a is a perfect square.

Exercise 4.6.21†. Prove that 16 is an eighth power modulo every prime but not an eighth power in $\mathbb{Q}$.

Exercise 4.6.22†. Prove that, if a polynomial $f \in \mathbb{Z}[X]$ of degree 2 has a root in $\mathbb{F}_p$ for any rational prime p, then it has a rational root. However, show that there exists polynomials of degree 5 and 6 that have a root in $\mathbb{F}_p$ for every prime p but no rational root.[9]

Exercise 4.6.23† (Jacobi Reciprocity)**.** Define the *Jacobi symbol* $\left(\frac{\cdot}{n}\right)$ of an odd positive integer n as the product

$$\left(\frac{\cdot}{p_1^{n_1}}\right) \cdot \ldots \cdot \left(\frac{\cdot}{p_k^{n_k}}\right)$$

where $n = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$ is the prime factorisation of n. Prove the following statements: for any odd m, n

- $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$.
- $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$.
- $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.

(The Jacobi symbol $\left(\frac{m}{n}\right)$ is 1 if m is quadratic residue modulo n but may also be 1 if m isn't.)

Exercise 4.6.24†. Suppose $a_1, \ldots, a_n$ are distinct squarefree rational integers such that

$$\sum_{i=1}^{n} b_i \sqrt{a_i} = 0$$

for some rational numbers $b_1, \ldots, b_n$. Prove that $b_1 = \ldots = b_n = 0$.

Exercise 4.6.25†. Let $n \geq 2$ be an integer and p a prime factor of $2^{2^n} + 1$. Prove that $p \equiv 1 \pmod{2^{n+2}}$.

Exercise 4.6.26† (USA TST 2014)**.** Find all functions $f : \mathbb{Z} \to \mathbb{Z}$ such that $(m-n)(f(m) - f(n))$ is a perfect square for all $m, n \in \mathbb{Z}$.

Sums and Products

Exercise 4.6.27† (Tuymaada 2012)**.** Let p be an odd prime. Prove that

$$\frac{1}{0^2+1} + \frac{1}{1^2+1} + \ldots + \frac{1}{(p-1)^2+1} \equiv \frac{(-1)^{\frac{p+1}{2}}}{2} \pmod{p}$$

where the sum is taken over the k for which $k^2 + 1 \not\equiv 0$.

Exercise 4.6.28. How many pairs (x, y) of elements of $\mathbb{F}_p$ are there such that $x^2 + y^2 = 1$?

Exercise 4.6.29 (USAMO 2020)**.** What is the product of the elements a of $\mathbb{F}_p$ such that both a and $4 - a$ are quadratic non-residues?

Exercise 4.6.30†. Let $n \geq 1$ be an integer. Prove that, for any rational prime p,

$$\prod_{k=1}^{p-1} \Phi_n(k) \equiv \Phi_{n/\gcd(n,p-1)}(1)^{\frac{\varphi(n)}{\varphi(n/\gcd(n,p-1))}} \pmod{p}.$$

[9] The Chebotarev density theorem implies that such a polynomial must be reducible. In fact it even characterises polynomials which have a root in $\mathbb{F}_p$ for every rational prime p based on the Galois groups of their splitting field (see Chapter 6). In particular, it shows that 5 and 6 are minimal.

Miscellaneous

Exercise 4.6.31. Compute $\Psi_n(0)$ for $n \geq 1$.

Exercise 4.6.32† (Lucas's Theorem)**.** Let p be a prime number and

$$n = p^m n_m + \ldots + pn_1 + n_0$$

and

$$k = p^m k_m + \ldots + pk_1 + k_0$$

be the base p expansion of rational integers $k, n \geq 0$ (n_i and k_i can be zero). Prove that

$$\binom{n}{k} \equiv \prod_{i=0}^{m} \binom{n_i}{k_i}.$$

Exercise 4.6.33† (Carmichael's Theorem)**.** Let a, b be two coprime integers such that $a^2 - 4b > 0$, and let $(u_n)_{n\geq 1}$ denote the linear recurrence defined by $u_0 = 0$, $u_1 = 1$, and

$$u_{n+2} = aU_{n+1} - bU_n.$$

Prove that for $n \neq 1, 2, 6$, u_n always have a primitive prime factor, except when $n = 12$ and $a = b = \pm 1$ (corresponding to the Fibonacci sequence).

Exercise 4.6.34†**.** Suppose $p \equiv 2$ or $p \equiv 5 \pmod 9$ is a rational prime. Prove that the equation

$$\alpha^3 + \beta^3 + \varepsilon a \gamma^3 = 0$$

where $\varepsilon \in \mathbb{Z}[j]$ is a unit and $2 \neq a \in \{p, p^2\}$ does not have solutions in $\mathbb{Z}[j]$.

Exercise 4.6.35† (Class Equation of a Group Action and Wedderburn's Theorem)**.** Let G be a finite group, S a finite set, and $\cdot$ a *group action* of G on S.[10] Given an element $s \in S$, let $\mathrm{Stab}(s)$ and $\mathrm{Fix}(G)$ denote the set of elements of G fixing s and the elements of S fixed by all of G respectivelly. Finally, let $\mathcal{O}_i = Gs_i$ be the (disjoint) orbits of size greater than 1. Prove the class equation:

$$|S| = |\operatorname{Fix}(G)| + \sum_{|\mathcal{O}_i|>1} \frac{|G|}{|\operatorname{Stab}(s_i)|}.$$

Deduce Wedderburn's theorem: any finite skew field is a field.

Exercise 4.6.36 (USA TSTST 2016)**.** Does there exist a non-constant polynomial $f \in \mathbb{Z}[X]$ such that, for any rational integer $n > 2$,

$$f(\mathbb{Z}/n\mathbb{Z}) := \{f(0), \ldots, f(n-1)\} \pmod n$$

has cardinality at most $0.499n$?

[10] In other words, a map $\cdot : G \times S \to S$ such that $e \cdot s = s$ and $(gh) \cdot s = g \cdot (h \cdot s)$ for any $g, h \in G$ and $s \in S$. See also Exercise A.3.20†.

Chapter 5

Polynomial Number Theory

Prerequisites for this chapter: Section A.1.

Algebraic number theory is deeply linked with polynomials (already by definition!). Here we study some arithmetic properties of polynomials with rational coefficients.

5.1 Factorisation of Polynomials

We have already mentioned factorisation of polynomials as a unique product of irreducible polynomials in Chapter 2 (in an abstract context) and Chapter 4 (for $\mathbb{F}_p[X]$) but we restate the main results here since they are fundamental.

Theorem 5.1.1 (Factorisation in Irreducible Polynomials in $\mathbb{Q}[X]$)

Any non-zero polynomial $f \in \mathbb{Q}[X]$ has a unique factorisation as a constant times a product of monic irreducible polynomials.

Proof

$\mathbb{Q}$ is a field so $\mathbb{Q}[X]$ is Euclidean (for the degree map) (see Proposition A.1.1) which means it's a UFD by Proposition 2.2.1 and Theorem 2.2.1. To finish, any irreducible polynomial has a unique monic associate so just use them in the factorisation and collect the leading coefficient in the beginning.

■

Since we deal with arithmetic property of polynomials, we are interested in factorising polynomials over $\mathbb{Z}[X]$. However $\mathbb{Z}$ is not a field anymore, so is $\mathbb{Z}[X]$ really a UFD? Gauss's lemma shows that as long as R is a UFD, $R[X]$ also is one. Before proving this however, we expand a bit on irreducible polynomials in $\mathbb{Z}[X]$. The polynomial $2X$ is irreducible in $\mathbb{Q}[X]$ (if $2X = fg$ then either f or g is constant and non-zero, i.e. a unit of $\mathbb{Q}[X]$) but not anymore in $\mathbb{Z}[X]$. Indeed, it factorises as $2 \cdot X$ and 2 is not a unit anymore ($1/2 \notin \mathbb{Z}[X]$).

We are thus led to make the following definition.

Definition 5.1.1 (Primitive Polynomial)

We say a polynomial $f \in \mathbb{Z}[X]$ is *primitive* if the gcd of its coefficients is 1.

For instance, the only constant primitive polynomials are 1 and -1.

Theorem 5.1.2 (Gauss's Lemma)

The product of two primitive polynomials is primitive.

Proof

Suppose f and g are primitive but fg isn't. Let p be a prime dividing all coefficients of fg, i.e. $fg \equiv 0 \pmod{p}$. Since $\mathbb{F}_p[X]$ is an integral domain, this means $f \equiv 0 \pmod{p}$ or $g \equiv 0 \pmod{p}$ which is impossible as they are primitive.

■

We can also state Gauss's lemma with the notion of *content*. The primitive polynomials are polynomials of content 1.

Definition 5.1.2 (Content)

The *content* of a polynomial $f \in \mathbb{Z}[X]$, $c(f)$, is defined as the gcd of the coefficients of f. For $f \in \mathbb{Q}[X]$, it is $c(Nf)/|N|$ where $0 \neq N$ is such that $Nf \in \mathbb{Z}[X]$.

Exercise 5.1.1*. Prove that the content is well-defined: $c(Nf)/|N| = c(Mf)/|M|$ for any non-zero $M, N \in \mathbb{Z}$ such that $Nf, Mg \in \mathbb{Z}[X]$.

Proposition 5.1.1 (Equivalent Form of Gauss's Lemma)*

The content is completely multliplicative, i.e. $c(fg) = c(f)c(g)$ for any $f, g \in \mathbb{Q}[X]$.

Proof

Without loss of generality, we may assume $f, g \in \mathbb{Z}[X]$ as $c(Nf) = |N|c(f)$ for any $N \in \mathbb{Z}$ (Exercise 5.1.1*). Then, $f/c(f)$ and $g/c(g)$ are primitive so $\frac{fg}{c(f)c(g)}$ is too by Theorem 5.1.2. Accordingly,

$$c(fg) = c(f)c(g)c\left(\frac{fg}{c(f)c(g)}\right) = c(f)c(g).$$

■

Corollary 5.1.1 (Irreducible Polynomials in $\mathbb{Z}[X]$)*

A polynomial $f \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Z}[X]$ if and only if it is primitive and irreducible in $\mathbb{Q}[X]$.

Proof

Clearly, if f is primitive but reducible in $\mathbb{Z}[X]$, it is reducible in $\mathbb{Q}[X]$. Thus, it suffices to show that a primitive polynomial which is reducible in $\mathbb{Q}[X]$ also is reducible in $\mathbb{Z}[X]$. Suppose $f = gh$. By multiplicativity of the content, we also have

$$f = (g/c(g))(h/c(h))$$

which is a factorisation in $\mathbb{Z}[X]$ as wanted (by Exercise 5.1.2*).

■

Exercise 5.1.2*. Suppose $f \in \mathbb{Q}[X]$ has integral content. Prove that f has integer coefficients.

In fact, we even have the following more general result.

Proposition 5.1.2

Suppose $f, g \in \mathbb{Z}[X]$ are polynomials such that f divides g in $\mathbb{Q}[X]$. Then, f^* divides g in $\mathbb{Z}[X]$, where $f^* = f/c(f)$ is the primitive part of f.

Exercise 5.1.3*. Prove Proposition 5.1.2.

We finally get our factorisation in $\mathbb{Z}[X]$.

Corollary 5.1.2 (Factorisation in Irreducible Polynomials in $\mathbb{Z}[X]$)*

Any non-zero polynomial $f \in \mathbb{Z}[X]$ has a unique factorisation as a constant times a product of non-constant primitive irreducible polynomials with positive leading coefficient. Equivalently, $\mathbb{Z}[X]$ is a UFD.

Exercise 5.1.4*. Prove Corollary 5.1.2.

As another corollary of Proposition 5.1.2, we get a new proof of Proposition 1.2.2, asserting that the minimal polynomial of an algebraic integer has integer coefficients, which uses neither the fact that rational integers are the only rational algebraic integers nor the fact that $\overline{\mathbb{Z}}$ is closed under addition and multiplication.

Corollary 5.1.3

Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number. Then, $\pi_\alpha \in \mathbb{Z}[X]$ if and only if $\alpha \in \overline{\mathbb{Z}}$.

Proof

It is clear that if $\pi_\alpha \in \mathbb{Z}[X]$ then $\alpha \in \overline{\mathbb{Z}}$, thus suppose that $\alpha \in \overline{\mathbb{Z}}$. Let $f \in \mathbb{Z}[X]$ be a monic polynomial vanishing at α. Then, π_α^* divides f in $\mathbb{Z}[X]$ by Proposition 5.1.2 so the leading coefficient of π_α^* is ± 1 since it divides the leading coefficient of f which is 1. Finally, we have $\pi_\alpha^* = \pi_\alpha$ which means that it has integer coefficients as wanted.

■

Because of these results, from now on we will say "irreducible" to mean "irreducible in $\mathbb{Q}[X]$" and "primitive and irreducible" to mean "irreducible in $\mathbb{Z}[X]$", unless otherwise specified. By default, $f \mid g$ means that f divides g in $\mathbb{Q}[X]$ and we will specify if it's true in $\mathbb{Z}[X]$ too when needed. If necessary, we will use $|_{\mathbb{Q}[X]}$ for divisibility in $\mathbb{Q}[X]$ and $|_{\mathbb{Z}[X]}$ for divisibility in $\mathbb{Z}[X]$.

Before discussing another result, we will say one last thing on Gauss's lemma. One can see that its proof only uses the fact that $\mathbb{Z}$ is a UFD (see Chapter 2). Thus, we could restate it in the following form.

Proposition 5.1.3 (Gauss's Lemma)

Suppose that a ring R is a UFD. Then, $R[X]$ is also one.

It can also be seen from our proof of Corollary 5.1.2 that the primes of $R[X]$ are either primes of R or primitive irreducible polynomials in $\operatorname{Frac} R[X]$. A very important consequence is that, by induction, $R[X_1, \ldots, X_n]$ is a UFD when R is, and in particular $K[X_1, \ldots, X_n]$ is a UFD for every field K. In other words, we still have factorisation in irreducible polynomials with more variables.

Corollary 5.1.4

For any field K and any integer $n \geq 1$, $K[X_1, \ldots, X_n]$ is a UFD.

We end this section with a classical criterion for proving certain polynomials are irreducible.

Proposition 5.1.4 (Eisenstein's Criterion)

Suppose p is a rational prime and $f = a_n X^n + \ldots + a_0 \in \mathbb{Z}[X]$ is a polynomial such that $p \nmid a_n$, $p \mid a_{n-1}, \ldots, a_0$ and $p^2 \nmid a_0$. Then f is irreducible (in $\mathbb{Q}[X]$).

Proof

Suppose $f = gh$ where $g, h \in \mathbb{Z}[X]$ are non-constant. Then, modulo p, $gh \equiv X^p$ so $g \equiv X^i$ and $h \equiv X^j$ for some k. Moreover, we must have $\deg(g \pmod p) = \deg g$ as otherwise the leading coefficient of g is divisible by p which is impossible as $p \nmid a_n$.

Thus, $i, j \geq 1$. This must mean that $p \mid g(0), h(0)$ so $p^2 \mid g(0)h(0) = a_0$, a contradiction. Hence by Gauss's lemma f is irreducible in $\mathbb{Q}[X]$.

■

Corollary 5.1.5

The pth cyclotomic polynomial $\Phi_p = X^{p-1} + \ldots + X + 1$ is irreducible for any rational prime p.

Proof

Apply the Eisenstein criterion to

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = \binom{p}{p} X^{p-1} + \binom{p}{p-1} X^{p-2} + \ldots + \binom{p}{1} X.$$

■

Remark 5.1.1

If one finds this transformation a bit unnatural, one can also reprove Eisenstein for this polynomial: $\Phi_p = \frac{X^p - 1}{X - 1} \equiv (X-1)^{p-1}$ by Proposition 4.1.1 so if it were reducible p^2 would divide $\Phi_p(1)$.

More generally, there are two basic principles to prove a polynomial is irreducible in $\mathbb{Q}[X]$: find some (impossible) information about a hypothetical factorisation modulo some prime p, or find some bounds on its roots to get a contradiction if it were reducible (for instance if a monic

polynomial's constant coefficient is prime and it were reducible, one of the factors must have constant coefficient ± 1 and hence a root of absolute value less than 1). We do not explore the second idea in this book, see chapter 17 of PFTB [1] for an account of this. Note that, even if f is irreducible in $\mathbb{Q}[X]$, it is not always possible to find a rational prime p for which $f \pmod p$ is irreducible in $\mathbb{F}_p$ as Φ_8 shows (Proposition 4.4.3).

Exercise 5.1.5. Prove that Φ_{p^n} is irreducible with Eisenstein's criterion.

5.2 Prime Divisors of Polynomials

Given a polynomial $f \in \mathbb{Z}[X]$ are interested in knowing which rational primes p are such that f has a root in $\mathbb{F}_p$. In fact we can already see that it is deeply linked to algebraic number theory: if $f = \alpha(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n)$, we want to know whether the prime p divides the product

$$\alpha(a - \alpha_1) \cdot \ldots \cdot (a - \alpha_n)$$

for some $a \in \mathbb{Z}$. We will not answer this question however, as it goes beyond the scope of this book (see the chapter on density theorems of [19]). Instead, we will only prove that there are infinitely many such primes (we call them "prime divisiors of the polynomial" by abuse of terminology, as they divide one of the value taken by it.)

Theorem 5.2.1

For any non-constant polynomial $f \in \mathbb{Z}[X]$, there exists infinitely many rational primes p such that $p \mid f(a)$ for some a.

Proof

Suppose there were only finitely many such primes, $p_1, \ldots, p_m$. Clearly, $f(0) \neq 0$ as otherwise all primes divide $f(0)$ (or $f(p)$ if you prefer large numbers). Thus, let

$$N = p_1^{v_{p_1}(f(0))+1} \cdot \ldots \cdot p_m^{v_{p_m}(f(0))+1}.$$

Consider the numbers $f(kN)$ for $k \in \mathbb{Z}$: they are congruent to $f(0)$ modulo $p_i^{v_{p_i}(f(0))+1}$ so their v_{p_i} is $v_{p_i}(f(0))$. By assumption, their only prime factors are the p_i: we conclude that

$$f(kN) = \pm p_1^{v_{p_1}(f(0))} \cdot \ldots \cdot p_m^{v_{p_m}(f(0))} = \pm f(0).$$

Finally, the polynomial $f(X)^2 - f(0)^2$ has infinitely many roots so is zero which means that f is constant, a contradiction.

■

Remark 5.2.1

Perhaps a simpler proof is to consider the polynomial $f(aX)/a$, where $a = f(0)$ is the constant coefficient of f, to avoid problems with its constant coefficient (which is now 1). We have presented the other proof first because we find it to be more instructive (but the alternative one is instructive too). This is what we did in the proof of Theorem 4.4.1.

Remark 5.2.2

We can also prove a much stronger result analytically: if $(a_n)_{n\geq 0}$ is an increasing sequence of positive integers bounded by a polynomial, $a_n \leq f(n)$ for some $f \in \mathbb{R}[X]$, then there are infinitely many primes which divide at least one term of the sequence. Indeed, if there was only $p_1, \ldots, p_m$,

then, on the one hand

$$\sum_{n=1}^{\infty} \frac{1}{a_n^{1/\deg f}}$$

would diverge since it grows faster than (a constant) times the harmonic series. On the other hand, by assumption,

$$\begin{aligned}\sum_{n=1} 6\infty \frac{1}{a_n^{1/\deg f}} &\leq \prod_{k=1}^{m} \sum_{n=1}^{\infty} \frac{1}{p^{n/\deg f}} \\ &= \prod_{k=1}^{m} \frac{1}{1-\frac{1}{p^{1/\deg f}}} \\ &< \infty.\end{aligned}$$

An interesting corollary is that, if $f \in \mathbb{Z}[X]$ is a polynomial and $S \subseteq \mathbb{N}$ is a set of non-zero density (that is, $\frac{|S\cap[n]|}{n} \not\to 0$), then there are infinitely many primes p such that $p \mid f(s)$ for some $s \in S$.

If we define $\mathcal{P}(f)$ to be the set of primes p such that f has a root modulo p, this result becomes the fact that $\mathcal{P}(f)$ is infinite when f is non-constant.

Here is an application of this result.

Problem 5.2.1 (APMO 2021 Problem 2)

Find all polynomials $f \in \mathbb{Z}[X]$ such that, for any n, there are at most 2021 pairs of rational integers $0 < a < b \leq n$ for which $|f(a)| \equiv |f(b)| \pmod{n}$.

Solution

We shall show that if f has degree at least 2, one value will of f will be reached arbitrarily many times. Since $f(m)$ is always positive or always negative for large m, we may assume by translating f that its sign is constant on positive numbers.

Thus, we want to estimate the number of $(a, b) \in (\mathbb{Z}/n\mathbb{Z})^2$ such that $f(a) \equiv f(b) \pmod{n}$. By Theorem 5.2.1, there are infinitely many prime divisors of $f(X+1) - f$; let $p_1, \ldots, p_m$ be such primes.

Thus, for $n = p_i$, there is one value $f(a)$ which is reached twice modulo n. Hence, for $n = p_1 \cdot \ldots \cdot p_m$, by the Chinese remainder theorem (CRT), there is a value which is reached 2^m times modulo n. This indeed grows unbounded.

We conclude that f must have degree 1 (constant f clearly doesn't work), i.e. $f = uX + v$ for some $u, v \in \mathbb{Z}$ and now we need to take in account the absolute values. We show that $u = \pm 1$. Suppose for the sake of a contradiction that $|u| \geq 2$. Notice that the sign of $f(n)$ is constant for $n \geq v$.

Modulo u^n, $f(a) \equiv f(b)$ if and only if $a \equiv b \pmod{u^{n-1}}$. For each residue modulo u^{n-1}, there are $|u|$ residues modulo u^n. Thus, there are $|u|^{n-1} \cdot \binom{|u|}{2}$ pairs of $0 < a < b \leq u^n$ such that $f(a) \equiv f(b)$. Now subtract the contribution of the residues where the sign is potentially not the same to get at least

$$(|u|^{n-1} - |v|)\binom{|u|}{2}$$

pairs which indeed grows unbounded.

Finally, $f = \pm X + v$. It is easy to see that when v and the leading coefficient have the same sign there is no pair working since the sign of $f(a)$ is constant. When v has the opposite sign, f works if and only if $|v| \leq 2022$. ■

Exercise 5.2.1*. Why does CRT imply that there is a value reached 2^m times modulo $p_1 \cdot \ldots \cdot p_m$?

Exercise 5.2.2. Prove that $X - v$ works iff $0 \leq v \geq -2022$, and $-X + v$ works iff $0 \leq v \leq 2022$.

5.3 Hensel's Lemma

We have found (some results about) when a polynomial f has a root modulo p. Now suppose we want to know when f has a root modulo $n = p_1^{n_1} \cdot \ldots \cdot p_m^{n_m}$. By the Chinese remainder theorem, this is equivalent to knowing when f has a root modulo $p_i^{n_i}$ for each i. Indeed, $f(a) \equiv 0 \pmod{n}$ if and only if $f(a) \equiv 0 \pmod{p_i^{n_i}}$ for each i, i.e. a is congruent modulo $p_i^{n_i}$ to a root a_i of $f \pmod{p_i^{n_i}}$. A partial result is provided by the Hensel lemma.

Theorem 5.3.1 (Hensel's Lemma)

Let $f \in \mathbb{Z}[X]$ be a polynomial and p a rational prime. If $p \mid f(a)$ for some $a \in \mathbb{Z}$ and $p \nmid f'(a)$, then, for any k, there is a unique $b \in \mathbb{Z}/p^m\mathbb{Z}$ such that $p^m \mid f(b)$ and $b \equiv a \pmod{p}$.

Before proving this result, we need a lemma which is in fact even more important than Hensel. Rather than only remembering the statement of Hensel's lemma, the reader should also learn the method of proving it which can be useful in a larger variety of situations.

Proposition 5.3.1 (Taylor's Formula)*

Let $f \in \mathbb{Q}[X]$ be a polynomial of degree n. For any $h \in \mathbb{Q}$, we have

$$f(X+h) = f + hf + h^2 \cdot \frac{f}{2} + \ldots + h^n \cdot \frac{f^{(n)}}{n!}.$$

Remark 5.3.1

One can also write

$$f(X+h) = \sum_{k=0}^{\infty} h^k \cdot \frac{f^{(k)}}{k!}$$

as all terms after $k = n$ vanish (since f has degree n.)

Proof

It suffices to prove this when $f = X^n$, as it will then be true for any linear combination of these polynomials, i.e. for any polynomial.

Notice that

$$(X^n)^{(k)} = n(n-1) \cdot \ldots \cdot (n-(k-1))X^{n-k}$$

so that

$$\frac{f^{(k)}}{k!} = \binom{n}{k} X^{n-k}.$$

Finally,

$$\sum_k h^k \cdot \frac{f^{(k)}}{k!} = \sum_k \binom{n}{k} h^k X^{n-k} = (X+h)^n$$

as wanted.

■

Corollary 5.3.1*

Let p be a rational prime, k a positive integer and $f \in \mathbb{Z}[X]$ a polynomial. For any rational integer h divisible by p^k, we have

$$f(X+h) \equiv f + hf' \pmod{p^{k+1}}.$$

Proof

It suffices to prove that $\frac{f^{(k)}}{k!}$ have integer coefficients by Proposition 5.3.1 (we evaluate both sides modulo p^{k+1}). But we have already shown that, if $f = \sum_i a_i X^i$, we have

$$\frac{f^{(k)}}{k!} = \sum_i a_i \binom{i}{k} X^{i-k}.$$

■

Here's an application of this result, before proving Hensel's lemma.

Problem 5.3.1 (USA TST 2010 Problem 1)

Let $f \in \mathbb{Z}[X]$ be a non-constant polynomial such that $\gcd(f(0), f(1), f(2), \ldots) = 1$ and $f(0) = 0$. Prove that there exist infinitely many integers rational integer $n \in \mathbb{Z}$ such that

$$\gcd(f(n) - f(0), f(n+1) - f(1), \ldots) = 1.$$

Solution

We take $n = p$ a rational prime. Suppose that a rational prime $q \neq p$ divides $f(p+k) - f(k)$ for all k. Then, $f(mp) \equiv f(0) \pmod{q}$ for any m by induction. But, since $q \neq p$, $mp \pmod{q}$ goes through every element of $\mathbb{F}_q$ which means that f is constant modulo q. Since $f(0) = 0$, this means $q \mid \gcd(f(0), f(1), f(2), \ldots)$ which is impossible.

Hence, we know that $\gcd(f(p)-f(0), f(p+1)-f(1), \ldots)$ is a power of p. It is clearly divisible by p; thus it remains to prove that it's not divisible by p^2. By Corollary 5.3.1, $f(p+k)-f(k) \equiv pf'(k) \pmod{p^2}$, this is equivalent to p not dividing at least one number of the form $f'(k)$.

This is very easy to have: f has degree at least 1, so f' is non-zero. Now, just pick a k such that $f'(k) \neq 0$ and any rational prime $p \nmid f'(k)$ (there are clearly infinitely many such primes). ■

Proof of Hensel's Lemma

We proceed by induction on k. For $k = 1$, the result is clear. Now, suppose there is a unique $b_k \in \mathbb{Z}/p^k\mathbb{Z}$ such that $f(b_k) \equiv 0 \pmod{p^k}$ and $b_k \equiv a \pmod{p}$. This means that any b_{k+1} satisfying $f(b_{k+1}) \equiv 0 \pmod{p^{k+1}}$ and $b_{k+1} \equiv a \pmod{p}$ must be congruent to b_k modulo p^k. We show that a unique $b_{k+1} \equiv b_k \pmod{p^k}$ which is a root of f modulo p^{k+1} exists (modulo p^{k+1}).

Write $b_{k+1} = b_k + up^k$. By Corollary 5.3.1, we have

$$f(b_{k+1}) \equiv f(b_k) + up^k f'(a) \pmod{p^{k+1}},$$

Accordingly, b_{k+1} is a root of f modulo p^{k+1} if and only if $u \equiv (f'(a))^{-1}(f(b_k)/p^k) \pmod{p}$ as $f'(a)$ is invertible modulo p by assumption. This exists and is unique modulo p, hence $b_{k+1} = b_k + up^k$ indeed exists and is unique modulo p^{k+1}.

■

Here's an application of Hensel itself.

Problem 5.3.2 (ISL 1995 N1)

Prove that, for any positive integer n, there exists a rational integer k such that $k \cdot 2^n - 7$ is a perfect square.

Solution

This is equivalent to -7 being a perfect square modulo 2^n. This makes us think of applying Hensel's lemma to the polynomial $X^2 + 7$. Unfortunately, its derivative $2X \equiv 0$ is zero modulo 2, thus the hypotheses can never be satisfied.

Nevertheless, we already know a root a of $X^2 - 17$ modulo 2^n must be odd. Thus, we can make the substitution $X = 2Y + 1$ to get

$$X^2 + 7 = (2Y + 1)^2 + 7 = 4(Y^2 + Y + 2).$$

We can now use Hensel's lemma on $Y^2 + Y + 2$: its derivative is $2Y + 1 \equiv 1$ which is never zero, hence we can lift the root 1 of $Y^2 + Y + 2$ modulo 2 to a (unique) root a modulo 2^{n-2}. Such an a will satisfy

$$(2a + 1)^2 \equiv -7 \pmod{2^n}$$

by what we have shown. ■

Exercise 5.3.1*. Let p be an odd prime and a a quadratic residue modulo p. Prove that a is a quadratic residue modulo p^n, i.e. a square modulo p^n (coprime with p^n), for any positive integer n.

Exercise 5.3.2*. Prove that an odd rational integer $a \in \mathbb{Z}$ is a quadratic residue modulo 2^n for $n \geq 3$ if and only if $a \equiv 1 \pmod{8}$.

5.4 Bézout's Lemma

We shall now see how irreducible polynomials really shine in polynomial number theory, with a few worked examples. Recall Bézout's lemma for $\mathbb{Q}[X]$ ($\mathbb{Q}[X]$ is Euclidean and hence a Bézout domain too).

Proposition 5.4.1 (Bézout's lemma for $\mathbb{Q}[X]$)

For any coprime polynomials $f, g \in \mathbb{Q}[X]$, there exists polynomials $u, v \in \mathbb{Q}[X]$ such that

$$fu + gv = 1.$$

Of course, this also holds for multiple polynomials: if $f_1, \ldots, f_n$ are coprime then some linear combination (with coefficients in $\mathbb{Q}[X]$) of them is 1 (just induct on n using Proposition 5.4.1).

Corollary 5.4.1*

For any coprime polynomials $f, g \in \mathbb{Z}[X]$, there exists polynomials $u, v \in \mathbb{Z}[X]$ and a non-zero constant $N \in \mathbb{Z}$ such that

$$fu + gv = N.$$

Exercise 5.4.1*. Prove Corollary 5.4.1.

Corollary 5.4.2

Suppose $f, g \in \mathbb{Z}[X]$ are such that, for any sufficiently large rational prime p, $p \mid f(n)$ implies $p \mid g(n)$ for any $n \in \mathbb{Z}$. Then, $\operatorname{rad} f \mid \operatorname{rad} g$, i.e. every irreducible factor of f in $\mathbb{Q}[X]$ divides g.

Proof

Suppose that π is a non-constant primitive irreducible factor of f which doesn't divide g.

Since π is irreducible, it is then coprime with g, so by Bézout's lemma there exist polynomials $u, v \in \mathbb{Z}[X]$ and a non-zero integer $N \in \mathbb{Z}$ such that

$$\pi u + gv = N.$$

In particular, any common prime factor of $\pi(n)$ and $g(n)$ must also divide N. Thus, if $p > N$ is a sufficiently large prime factor of $\pi(n) \mid f(n)$ (there exists one by Theorem 5.2.1), then $p \nmid N$ so $p \nmid g(n)$ which is a contradiction.

■

In other words, the prime divisors of a polynomial are controlled by the prime divisors of its irreducible prime factors, thanks to Bézout's lemma. Here is a more elaborate example, not involving irreducible polynomials in the statement.

Problem 5.4.1

Suppose $f \in \mathbb{Q}[X]$ is a polynomial which takes only perfect square values (in $\mathbb{Q}$). Prove that it is the square of a polynomial with rational coefficients.

Solution

By multiplying f by an appropriate integral perfect square, we may assume f has integer coefficients. Without loss of generality, we may assume f is squarefree. We shall show that f must be constant, since this clearly implies that it is the square of a polynomial with integer coefficients.

Consider its factorisation in non-constant primitive irreducible polynomials $f = a\pi_1 \cdot \ldots \cdot \pi_m$. Suppose for the sake of a contradiction that $m \geq 1$. First, we wish to distinguish the prime divisors of π_1 from the prime divisors, so that, when $p \mid \pi_1(n)$, $v_p(\pi_1(n)) = v_p(f(n))$ (which must be even by assumption). By Bézout's lemma, since π_1 and $\pi_2\pi_3 \cdot \ldots \cdot \pi_m$ are coprime, there exist polynomials $u, v \in \mathbb{Z}[X]$ and a non-zero integer N such that

$$u\pi_1 + v\pi_1'\pi_2 \cdot \ldots \cdot \pi_m = N.$$

Now, consider a rational prime $p > a, N$ and a rational integer $n \in \mathbb{Z}$ such that $p \mid \pi_1(n)$; there exists one by Theorem 5.2.1. By assumption, $p \nmid aN$, thus $p \nmid a\pi_2(n) \cdot \ldots \cdot \pi_m(n)$ which implies $v_p(f(n)) = v_p(\pi_1(n))$.

In particular, since $v_p(\pi_1(n))$ and $v_p(\pi_1(n+p))$ are even and positive, we must have

$$p^2 \mid \pi_1(n), \pi_1(n+p).$$

But, by Corollary 5.3.1

$$\pi_1(n+p) \equiv \pi_1(n) + p\pi_1'(n) \equiv p\pi_1'(n) \pmod{p^2}$$

which means p must divide $\pi_1'(n)$.

To conclude, π_1 and π_1' are coprime (since π_1 is irreducible and $\deg \pi_1 > \deg \pi_1'$) so, by Bézout's lemma, there are some $r, s \in \mathbb{Z}[X]$ and a non-zero $M \in \mathbb{Z}$ such that $r\pi_1 + s\pi_1' = M$. Then, for $p > a, M, N$, the previous remark is impossible and we must have $v_p(\pi_1(n)) = 1$ or $v_p(\pi_1(n+p)) = 1$ which is a contradiction. ■

Remark 5.4.1

We could have directly used Bézout on π_1 and $\pi_1'\pi_2 \cdot \ldots \cdot \pi_n$ but we presented it that way to highlight the motivation. In fact, what we have proven wit this is that, if π and $\pi_1, \ldots, \pi_k$ are distinct primitive irreducible polynomials, there exists infinitely many primes p for which there is an n such that $v_p(\pi(n)) = 1$ and $v_p(\pi_i(n)) = 0$ for $i = 1, \ldots, k$.

Remark 5.4.2

In fact, the problem of determining which polynomials reach infinitely many square values has been completely settled with deep arithmetic geometry results. We can also approach this analytically (and elementarily) to get results stronger than what we proved, but worse than the complete characterisation. The idea is that if the leading coefficient of $f \in \mathbb{Z}[X]$ is a square, we can find a polynomial $g \in \mathbb{Z}[X]$ such that

$$g(x)^2 \leq f(x) < (g(x)+1)^2$$

for any sufficiently large $|x|$, which forces $f = g^2$ if f takes infinitely many square values. When the leading coefficient is not a square, we can still transform it into a square in some cases. For instance, if $f(2^n)$ is a square for all n, then the leading coefficient of $f(X)f(2^mX)$ is a square for even m, and this polynomial takes infinitely many square values, so must be a square. It is not hard that this must imply that f is a square of X times a square, which doesn't work (e.g. by looking at the roots: for sufficiently large m, the only possible common root of f and $f(2^mX)$ is 0).

We conclude this chapter with two additional remarks. When dealing with problems about polynomials modulo some prime p, it is very important to keep in mind a polynomial of degree n has at most n roots modulo p (since $\mathbb{F}_p$ is a field). Also, when dealing with exponential functions and polynomials at the same time, say $f(n)$ and a^n, modulo p one can choose the value of a^n and $f(n)$ independently as the first one has period $p-1$ while the latter has period p. We illustrate this by an example.

Problem 5.4.2 (Polish Mathematical Olympiad 2003 Problem 3)

Find all polynomials $f \in \mathbb{Z}[X]$ is a polynomial such that $f(n) \mid 2^n - 1$ for any positive rational integer n.

Solution

Suppose some prime p divides $f(n)$ for some rational integer n. Choose a rational integer n'

satisfying $n' \equiv n \pmod{p}$ and $n' \equiv 0 \pmod{p-1}$ by CRT. Then,

$$p \mid f(n') \mid 2^{n'} - 1 \equiv 1 \pmod{p}$$

which is impossible. Thus, we conclude $f(n) = \pm 1$ for all n which means $f = \pm 1$. These are indeed solutions. ■

5.5 Exercises

Algebraic Results

Exercise 5.5.1†**.** Suppose $f, g \in \mathbb{Z}[X]$ are polynomials such that $f(n) \mid g(n)$ for infinitely many rational integers $n \in \mathbb{Z}$. Prove that $f \mid g$. In addition, generalise the previous statement to $f, g \in \mathbb{Z}[X_1, \ldots, X_m]$ such that $f(x) \mid g(x)$ fo $x \in S_1 \times \ldots \times S_n$, where $S_1, \ldots, S_n \subseteq \mathbb{Z}$ are infinite sets.

Exercise 5.5.2†**.** Let $f \in \mathbb{Q}[X]$ be a polynomial. Suppose that f always takes values which are mth powers in $\mathbb{Q}$. Prove that f is the mth power of a polynomial with rational coefficients. More generally, find all polynomials $f \in \mathbb{Q}[X_1, \ldots, X_m]$ such that $f(x_1, \ldots, x_m)$ is a (non-trivial) perfect power for any $(x_1, \ldots, x_m) \in \mathbb{Z}^m$.

Exercise 5.5.3†**.** Suppose $f, g \in \mathbb{Z}[X]$ are polynomials such that $f(a) - f(b) \mid g(a) - g(b)$ for any rational integers $a, b \in \mathbb{Z}$. Prove that there exists a polynomial $h \in \mathbb{Z}[X]$ such that $g = h \circ f$.

Exercise 5.5.4 (RMM SL 2016)**.** Let p be a prime number. Prove that there are only finitely many primes q such that

$$q \mid \sum_{k=1}^{\lfloor q/p \rfloor} k^{p-1}.$$

Exercise 5.5.5. Let x and y be positive rational integers. Suppose $f, g \in \mathbb{Z}[X]$ are polynomials such that $f(ab) \mid g(a^x + b^y)$ for any $a, b \in \mathbb{Z}$. Prove that f is constant.

Exercise 5.5.6 (ISL 2019)**.** Suppose a and b are positive rational integers such that

$$an + 1 \mid \binom{an}{b} + 1$$

for any rational integer $n \geq b$. Prove that $b + 1$ is prime.

Exercise 5.5.7. Suppose $f \in \mathbb{Z}[X_1, \ldots, X_n]$ is a polynomial such that, for each tuple of rational primes $(p_1, \ldots, p_n)$, there is some i for which $p_i \mid f(p_1, \ldots, p_k)$. Prove that $X_i \mid f$ for some i. (You may assume Dirichlet's theorem.)

Exercise 5.5.8 (Inspired by Iran TST 2019)**.** Suppose $f_1, \ldots, f_k \in \mathbb{Q}[X]$ are polynomials such that, whenever n is a perfect power, one of $f_1, \ldots, f_k$ is too. Prove that one of $f_1, \ldots, f_k$ is a non-trivial power of a polynomial or X.

Polynomials over $\mathbb{F}_p$

Exercise 5.5.9† (Generalised Eisenstein's Criterion)**.** Let $f = a_n X^n + \ldots + a_0 \in \mathbb{Z}[X]$ be a polynomial and let p a rational prime. Suppose that $p \nmid a_n$, $p \mid a_0, \ldots, a_{n-1}$, and $p^2 \nmid a_k$ for some $k < n$. Then any factorisation $f = gh$ in $\mathbb{Q}[X]$ satisfies $\min(\deg g, \deg h) \leq k$.

Exercise 5.5.10† (China TST 2008)**.** Let $f \in \mathbb{Z}[X]$ be a (non-zero) polynomial with coefficients in $\{-1, 1\}$. Suppose that $(X-1)^{2^k}$ divides f and $\deg f \geq 2^k$. Prove that $\deg f \geq 2^{k+1} - 1$.

Exercise 5.5.11† (Romania TST 2002)**.** Let $f, g \in \mathbb{Z}[X]$ be polynomials with coefficients in $\{1, 2002\}$. Prove that $\deg f + 1 \mid \deg g + 1$.

Exercise 5.5.12† (USAMO 2006)**.** Find all polynomials $f \in \mathbb{Z}[X]$ such that the sequence $(P(f(n^2)) - 2n)_{n\geq 0, f(n^2)\neq 0}$ is bounded above, where P is the greatest prime factor function. (In particular, since $P(0) = +\infty$, we have $f(n^2) \neq 0$ for any $n \in \mathbb{Z}$.)

Exercise 5.5.13 (Iran TST 2011)**.** Suppose a polynomial $f \in \mathbb{Z}[X]$ is such that $p^k \mid f(n)$ for all $n \in \mathbb{Z}$, for some $k \leq p$. Prove that there exist polynomials $g_0, \ldots, g_k \in \mathbb{Z}[X]$ such that

$$f = \sum_{i=0}^{k} (X^p - X)^i p^{k-i} g_i.$$

In addition, prove that this becomes false when $k > p$.

Exercise 5.5.14† (China TST 2021)**.** Suppose the polynomials $f, g \in \mathbb{Z}[X]$ are such that, for any sufficiently large rational prime p, there is an element $r_p \in \mathbb{F}_p$ such that $f \equiv g(X + r_p) \pmod{p}$. Prove that there exists a rational number $r \in \mathbb{Q}$ such that $f = g(X + r)$.

Exercise 5.5.15 (IMO 1993)**.** Let $n \geq 2$ be an integer. Prove that the polynomial $X^n + 5X^{n-1} + 3$ is irreducible.

Iterates

Exercise 5.5.16†**.** Let $f \in \mathbb{Z}[X]$ be a polynomial. Show that the sequence $(f^n(0))_{n\geq 0}$ is a *Mersenne sequence*, i.e.

$$\gcd(f^i(0), f^j(0)) = f^{\gcd(i,j)}(0)$$

for any $i, j \geq 0$.

Exercise 5.5.17†**.** Suppose the non-constant polynomial

$$f = a_d X^d + \ldots + a_2 X^2 + a_0 \in \mathbb{Z}[X]$$

has positive coefficients and satisfies $f'(0) = 0$. Prove that the sequence $(f^n(0))_{n\geq 1}$ always has a primitive prime factor.

Exercise 5.5.18† (Tuymaada 2003)**.** Let $f \in \mathbb{Z}[X]$ be a polynomial and $a \in \mathbb{Z}$ a rational integer. Suppose $|f^n(a)| \to \infty$. Prove that there are infinitely many primes p such that $p \mid f^n(a)$ for some $n \geq 0$ unless $f = AX^d$ for some A, d.

Exercise 5.5.19† (USA TST 2020)**.** Find all integers $n \geq 2$ for which there exist a rational integer $m > 1$ and a polynomial $f \in \mathbb{Z}[X]$ such that $\gcd(m, n) = 1$ and $n \mid f^k(0) \iff m \mid k$ for any positive rational integer k.

Exercise 5.5.20†**.** Let $f \in \mathbb{Q}[X]$ be a polynomial of degree k. Prove that there is a constant $h > 0$ such that that the denominator of $f(x)$ is greater than h times the denominator of x^k.

Exercise 5.5.21†**.** Let $f \in \mathbb{Q}[X]$ be a polynomial of degree at least 2. Prove that

$$\bigcap_{k=0}^{\infty} f^k(\mathbb{Q})$$

is finite.

Exercise 5.5.22† (Iran TST 2004)**.** Let $f \in \mathbb{Z}[X]$ be a polynomial such that $f(n) > n$ for any positive rational integer n. Suppose that, for any $N \in \mathbb{Z}$, there is some positive rational integer n such that

$$N \mid f^n(1).$$

Prove that $f = X + 1$.

Divisibility Relations

Exercise 5.5.23†. Find all polynomials $f \in \mathbb{Z}[X]$ such that $f(n) \mid n^{n-1} - 1$ for sufficiently large n.

Exercise 5.5.24. Find all polynomials $f \in \mathbb{Z}[X]$ such that $\gcd(f(a), f(b)) = 1$ whenever $\gcd(a, b) = 1$.

Exercise 5.5.25† (ISL 2012 Generalised)**.** Find all polynomials $f \in \mathbb{Z}[X]$ such that $\operatorname{rad} f(n) \mid \operatorname{rad} f(n^{\operatorname{rad} n})$. (You may assume Dirichlet's theorem.)

Exercise 5.5.26 (ISL 2011)**.** Suppose $f, g \in \mathbb{Z}[X]$ are coprime polynomials such that $f(n)$ and $g(n)$ are positive for any positive rational integer n. Suppose that

$$2^{f(n)} - 1 \mid 3^{g(n)} - 1$$

for any positive rational integer n. Prove that f is constant.

Exercise 5.5.27†. Find all polynomials $f \in \mathbb{Z}[X]$ such that $f(p) \mid 2^p - 2$ for any prime p. (You may assume Dirichlet's theorem.)

Exercise 5.5.28 (Iran Mathematical Olympiad 3rd Round 2016)**.** We say a function $g : \mathbb{N} \to \mathbb{N}$ is *special* if it has the form $g(n) = a^{f(n)}$ where $f \in \mathbb{Z}[X]$ is a polynomial such that $f(n)$ is positive when n is a positive rational integer and a is a rational integer. We also say the sum, difference, and product of two special functions is special. Prove that there does not exist a non-zero special function g and a non-constant polynomial $f \in \mathbb{Z}[X]$ such that

$$f(n) \mid g(n)$$

for any positive rational integer n.

Miscellaneous

Exercise 5.5.29† (Generalised Hensel's Lemma)**.** Let $f \in \mathbb{Z}[X]$ be a polynomial and $a \in \mathbb{Z}$ an integer. Let $m = v_p(f'(a))$. If $p^{2m+1} \mid f(a)$, prove that f has exactly one root b modulo p^k which is congruent to a modulo p^{m+1} for all $k \geq 2m + 1$.

Exercise 5.5.30†. Let $f \in \mathbb{Z}[X]$ be a non-constant polynomial. Is it possible that $f(n)$ is prime for any $n \in \mathbb{Z}$?

Exercise 5.5.31†. Find all polynomials $f \in \mathbb{Q}[X]$ which are surjective onto $\mathbb{Q}$.

Exercise 5.5.32 (Inspired by USA TST 2008)**.** Let n be a positive rational integer. How many sequences of n elements of $\mathbb{Z}/n\mathbb{Z}$ have the form

$$(f(0), \ldots, f(n-1))$$

for some $f \in \mathbb{Z}/n\mathbb{Z}[X]$?

Exercise 5.5.33. We say a subset S of $\mathbb{Z}/n\mathbb{Z}$ is *d-coverable* if there exists a polynomial $f \in \mathbb{Z}/n\mathbb{Z}[X]$ of degree at most d such that

$$S = \{f(0), \ldots, f(n-1)\}.$$

Find all rational integers n such that all subsets of $\mathbb{Z}/n\mathbb{Z}$ are d-coverable for some d, and find the minimum possible d for these n.

Exercise 5.5.34 (Iran TST 2015)**.** Let $(a_n)_{n \geq 0}$ denote the sequence of rational integers which are sums of two squares: $0, 1, 2, 4, 5, 8, \ldots$. Let $m \in \mathbb{Z}$ be a positive rational integer. Prove that there are infinitely many integers n such that $a_{n+1} - a_n = m$.

Exercise 5.5.35† (ISL 2005)**.** Let $f \in \mathbb{Z}[X]$ be a non-constant polynomial with positive leading coefficient. Prove that there are infinitely many positive rational integers n such that $f(n!)$ is composite.

Chapter 6

The Primitive Element Theorem and Galois Theory

Prerequisites for this chapter: Chapters 1, 3 and 4 and Sections A.2 and C.1 for the whole chapter and Chapter 5 for Section 6.4. Chapter 2 is recommended.

6.1 General Definitions

Let's start with some general definitions with which you should be somewhat familiar with by now (from Chapters 2 and 4 and the exercises).

Definition 6.1.1

The smallest ring containing a commutative ring R and elements $\alpha_1, \ldots, \alpha_n$ is denoted

$$R[\alpha_1, \ldots, \alpha_n].$$

It consists of polynomial expressions in $\alpha_1, \ldots, \alpha_n$:

$$R[\alpha_1, \ldots, \alpha_n] = \{f(\alpha_1, \ldots, \alpha_n) \mid f \in R[X_1, \ldots, X_n]\}.$$

Definition 6.1.2

The smallest field containing a commutative field K and elements $\alpha_1, \ldots, \alpha_n$ is denoted

$$K(\alpha_1, \ldots, \alpha_n).$$

It consists of rational expressions in $\alpha_1, \ldots, \alpha_n$:

$$K(\alpha_1, \ldots, \alpha_n) = \{f(\alpha_1, \ldots, \alpha_n) \mid f \in K(X_1, \ldots, X_n)\}.$$

Exercise 6.1.1*. Prove that $R[\alpha_1, \ldots, \alpha_n]$ is indeed the smallest ring containing R and $\alpha_1, \ldots, \alpha_n$, in the sense that any other such ring must contain $R[\alpha_1, \ldots, \alpha_n]$. Similarly, prove that any field containing K and $\alpha_1, \ldots, \alpha_n$ contains $K(\alpha_1, \alpha_n)$.

Exercise 6.1.2*. Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number. Prove that $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.

Remark 6.1.1

Of course, we assumed the multiplication and addition of R and K were compatible with the α_i, and in the second definition, that $K[\alpha_1, \ldots, \alpha_n]$ is an integral domain, otherwise the definitions

do not make sense. Indeed, if $\alpha_1\alpha_2 = 0$ but $\alpha_1, \alpha_2 \neq 0$ then no field can contain α_1 and α_2.

We now generalise the quadratic fields from Chapter 2 to arbitrary fields of the form $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ for some algebraic numbers $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}$. These are called *number fields*. However, to get more number-theoretic information on number fields, we must do algebraic number theory with numbers fields too instead of only $\mathbb{Q}$.

Here is what this means: we defined algebraic numbers as roots of polynomials with rational coefficients. We can then define algebraic numbers *over a number field* K as the roots of polynomials with coefficients in K. These turn out to be the same as the regular algebraic numbers by the fundamental theorem of symmetric polynomials, but what's different is their **minimal polynomial**. Indeed, the minimal polynomial of $\frac{(i+1)\sqrt{2}}{2}$ over $\mathbb{Q}$ is $X^4 + 1$ but over $\mathbb{Q}(i)$ it is just $X^2 - i$.

Exercise 6.1.3*. Prove that the minimal polynomial of $\frac{(i+1)\sqrt{2}}{2}$ over $\mathbb{Q}(i)$ is $X^2 - i$.

We thus make the following definitions. One of the reasons we do it in so much generality is to do number theory with other base fields than $\mathbb{Q}$ (but which are still number fields), but another one is also to revisit the theory of finite fields a bit, since these are also about algebraic elements.

Definition 6.1.3 (Field Extensions)

We say two fields $K \subseteq L$ form a *field extension* denoted L/K (big field over small field).

We will usually only say "extension" for "field extension". We also make analogous definitions for elements algebraic over K, their minimal polynomial, their degree, their conjugates, etc. The field of elements algebraic over L is denoted $\overline{L}$ and called the *algebraic closure* of L (this won't be needed in this book as $\overline{L} = \overline{\mathbb{Q}}$ for any number field L).

Definition 6.1.4 (Degree of a Field Extension)

The *degree* $[L : K]$ of an extension L/K is the dimension of L as a K-vector space.

Exercise 6.1.4*. Check that L is a K-vector space.

What the degree does is that it measures the "size" of the extension. This definition might seem somewhat complicated at first, but it is in fact very simple (in the cases we're interested in): when $L = K(\alpha)$ for some α algebraic over L of degree n, the degree of L/K is also just n! Indeed, by definition the elements $1, \alpha, \dots, \alpha^{n-1}$ are K-linearly independent (otherwise the minimal polynomial of α has degree less than n) while $1, \alpha, \dots, \alpha^n$ aren't (since some polynomial of degree n vanishes at α). For our purposes, all extensions of number fields have the form $L = K(\alpha)$: this is the primitive element theorem 6.2.1. You might thus wonder why we state things with linear algebra terminology: it's simply because linear algebra and bases are convenient to work with, as the following example as well as the tower law 6.1.1 show.

Proof that algebraic numbers are closed under addition and multiplication

Let $\alpha, \beta \in \overline{\mathbb{Q}}$ be algebraic numbers of respective degrees m and n. Then, $\mathbb{Q}(\alpha, \beta)$ is a $\mathbb{Q}$-vector space with dimension at most mn, since its generated by $\alpha^i\beta^j$, $i = 0, \dots, m-1$, $j = 0, \dots, n-1$.

As a consequence, $1, \alpha+\beta, (\alpha+\beta)^2, \dots, (\alpha+\beta)^{mn}$ are linearly dependent which means that there is a polynomial with rational coefficients of degree at most mn vanishing at α_β, in particular it's algebraic.

Similarly, $1, \alpha\beta, (\alpha\beta)^2, \dots, (\alpha\beta)^{mn}$ are linearly dependent so $\alpha\beta$ is algebraic.

■

Note that this proof does not work to show that $\overline{\mathbb{Z}}$ is closed under addition and multiplication, as $\overline{\mathbb{Z}}$ is not a $\mathbb{Q}$-vector space anymore so bases don't work nicely, However, a proof using linear algebra still exists, see Section C.3.

Proposition 6.1.1 (Tower Law)

Suppose $M/L/K$ is a *tower* of extensions (meaning $K \subseteq L \subseteq M$). Then,

$$[M : K] = [M : L][L : K].$$

In other words, the degree is multiplicative in towers of extensions.

Proof

Let $m = [M : L]$ and $n = [L : K]$. Let $u_1, \ldots, u_m$ be a L-basis of M, and $v_1, \ldots, v_n$ be a K-basis of L. Then, $(u_i v_j)_{i\in[m],j\in[n]}$ is a K-basis of M. Since this basis has cardinality mn, $[M : K] = mn$.

■

Exercise 6.1.5*. Prove that $(u_i v_j)_{i\in[m],j\in[n]}$ is a K-basis of M.

Exercise 6.1.6*. Let $M/L/K$ be a tower of extensions and $\alpha \in M$. Prove that the minimal polynomial of α over L divides the minimal polynomial of α over K. In other words, its L-conjugates are among its K-conjugates.

Before we make more definitions, here is an application of why we care about extensions of number fields (where $K \neq \mathbb{Q}$), and why the tower law is useful.

Problem 6.1.1 (IMC 2012 Problem 5)

Let $a \in \mathbb{Q}$ be a rational number, and $n \geq 1$ be an integer. Prove that the polynomial

$$(X^2 + aX)^{2^n} + 1$$

is irreducible in $\mathbb{Q}[X]$.

Before solving this problem, we need a lemma which follows from the tower law.

Lemma 6.1.1

Let $f, g \in \mathbb{Q}[X]$ be polynomials. Then, $f \circ g$ is irreducible in $\mathbb{Q}[X]$ if and only if f is irreducible in $\mathbb{Q}[X]$ and $g - \alpha$ is irreducible in $\mathbb{Q}(\alpha)[X]$, where α is a root of f.

Proof

Let $m = \deg f$ and $n = \deg g$. Consider a root α of f and a root β of $g - \alpha$. Then, β is a root of $f \circ g$ and we have

$$[\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

$f \circ g$ is irreducible if and only if $[\mathbb{Q}(\beta) : \mathbb{Q}] = \deg f \circ g = mn$. Also, $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq m$ since α is a root of f, with equality iff f is irreducible in $\mathbb{Q}[X]$. Similarly, $[\mathbb{Q}(\beta) : \mathbb{Q}(\alpha)] \leq n$ since β is a root

of $g - \alpha$, with equality iff $g - \alpha$ is irreducible in $\mathbb{Q}(\alpha)$. To conclude,

$$[\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq mn$$

with equality if and only if f is irreducible in $\mathbb{Q}[X]$ and $g-\alpha$ is irreducible in $\mathbb{Q}(\alpha)[X]$, as wanted. ■

Solution

Using the lemma, we wish to show that $f = X^{2^n} + 1 = \Phi_{2^{n+1}}$ is irreducible in $\mathbb{Q}[X]$, which is true by Theorem 3.2.1 (or Eisenstein's criterion) and that $g - \omega = X^2 + aX - \omega$ is irreducible in $\mathbb{Q}(\omega)$ where ω is a primitive 2^{n+1}th root of unity. Here is why this is easier to manipulate: a polynomial of degree two is reducible if and only if it has no root. Thus, suppose for the sake of a contradiction that $X^2 + aX - \omega$ has a root in $\mathbb{Q}(\omega)$, i.e. $h(\omega)^2 + ah(\omega) = \omega$ for some $h \in \mathbb{Q}[X]$.

We complete the square and take the norm: $(h(\omega) + b)^2 = \omega + b^2$, where $b = a/2$, and

$$\prod_{k \text{ odd}} (h(\omega^k) + b)^2 = \prod_{k \text{ odd}} \omega^k + b^2.$$

The LHS is a perfect square by the fundamental theorem of symmetric polynomials, while the RHS is

$$\prod_{k \text{ odd}} b^2 - \omega^k = \Phi_{2^{n+1}}(b^2) = b^{2^{n+1}} + 1$$

since $\varphi(2^{n+1}) = 2^n$ is even. Now, we suppose that the diophantine equation $x^4 + y^4 = z^2$ has no solution in non-zero rational integers. This is a classical result which was proven by Fermat. See Exercise 2.6.12† for a proof.

Hence, the diophantine equation $b^{2^{n+1}} + 1 = c^2$ has only the rational solution $b = 0$ which means $a = 0$. But then $(X^2 + 0X)^{2^n} + 1 = \Phi_{2^{n+2}}$ is clearly irreducible so we reach a contradiction in all cases. ■

Finally, we make three more definitions, the last two having been encountered a few times already in special cases.

Definition 6.1.5 (Finite Extension)

We say an extension L/K is *finite* if its degree $[L : K]$ is finite.

Definition 6.1.6 (Number Field)

A finite extension of $\mathbb{Q}$ is called a *number field*.

Exercise 6.1.7*. Prove that finite extensions of K are exactly the fields of the form $K(\alpha_1, \ldots, \alpha_n)$ for $\alpha_1, \ldots, \alpha_n$ algebraic elements over K, using Proposition 6.1.1.

Definition 6.1.7 (Ring of Integers)

Let K be a number field. Its *ring of integer*, $\mathcal{O}_K$, is the ring of algebraic integers of K: $K \cap \overline{\mathbb{Z}}$.

6.2 The Primitive Element Theorem and Field Theory

Our main result is the following: every number field is generated by one element. This is extremely nice, as you will see with all the applications, as all one has to do is to take in account the minimal polynomial of the generator to deduce the structure of the field. For instance, as mentioned before, one can easily compute the degree of $K = \mathbb{Q}(\alpha)$ (if one knows α). Compare this to, say, $\mathbb{Q}(\alpha, \beta)$: you not only have to take in account the contribution of α (its degree over $\mathbb{Q}$), but also what β adds to the contribution of α (its degree over $\mathbb{Q}(\alpha)$)!

Theorem 6.2.1 (Primitive Element Theorem)

Let $K \subseteq \mathbb{C}$ be a field, and $\alpha, \beta \in \overline{K}$ algebraic elements over K. Then, there exists a $\gamma \in K(\alpha, \beta)$ such that

$$K(\alpha, \beta) = K(\gamma).$$

Since, by Exercise 6.1.7*, every number field is finitely generated, repeated applications of the primitive element theorem lead to number fields being generated by one element (by induction).

Proof

We take $\gamma = \alpha + t\beta$, for some $t \in K$ that will be chosen later. We will find two polynomials in $K(\gamma)[X]$ whose gcd is $X - \alpha$: since the gcd can be obtained by the Euclidean algorithm, this means that $\alpha \in K(\gamma)$ and thus also $\beta = (\gamma - \alpha)/t \in K(\gamma)$.

For these polynomials, we choose

$$f = \pi_\alpha = \prod_i X - \alpha_i$$

and

$$g = \prod_j (X - (\gamma - t\beta_j))$$

where α_i and β_j are the conjugates of α and β respectively (over K). By the fundamental theorem of symmetric polynomials, they both have coefficients in $K(\gamma)$. It remains to see that their gcd is $X - \alpha$: since they have distinct roots this is equivalent to α being the only common root. Suppose $\alpha_i = \gamma - t\beta_j = \alpha + t(\beta - \beta_j)$ is another common root: this yields

$$t = \frac{\alpha_i - \alpha}{\beta - \beta_j}$$

($\beta \neq \beta_j$ as $\alpha \neq \alpha_i$). There are clearly a finite number of such values, thus any sufficiently large t works.

■

If you read this proof carefully, you might notice that it almost works for any infinite field K. In fact, it does show that if L/K is finite then L is generated by one element, under the assumption of *separability*. This means that the conjugates of an element are always distinct. Indeed, if this assumption is not satisfied, then the gcd of the two polynomials we constructed could be divisible by $(X - \alpha)^2$ and thus not equal to $X - \alpha$. It seems obvious that irreducible polynomials have no repeated roots, and that's because it is, but only in characteristic zero. In characteristic p, things becomes weird, but one can check that it still holds for finite fields (it can only fail if the derivative of the polynomial is zero). Since these are the cases we are interested in, we will assume that all our extensions are separable, so that we can use the primitive element theorem. See Exercise 6.5.39 for an example of a non-separable extension.

Note also that we also proved the primitive element theorem for finite fields, in Corollary 4.2.1.

Definition 6.2.1 (Separable Extension)

An *algebraic* (i.e. $L \subseteq \overline{K}$) extension L/K is said to be *separable* if the minimal polynomial of any element of L has distinct conjugates.

With this, we can establish a numbers of field theoretic results for number fields. In particular, we shall generalise the norm $N_{\mathbb{Q}(\sqrt{d})}$ of quadratic fields Definition 2.1.4.

Definition 6.2.2 (Embeddings)

Let L/K be a finite extension. The K-embeddings of L are functions $f : L \to \overline{L}$ which additive, multiplicative, and the identity on K. In other words, functions satisfying $f(k) = k$ for $k \in K$, and $f(x + y) = f(x) + f(y)$ as well as $f(xy) = f(x)f(y)$ for $x, y \in L$. The set of K-embeddings of L is denoted $\mathrm{Emb}_K(L)$.

Since we are usually concerned with the case $K = \mathbb{Q}$, we will just say "embedding" for "$\mathbb{Q}$-embedding" as well as write Emb for $\mathrm{Emb}_{\mathbb{Q}}$.

Remark 6.2.1

We say "embedding" because a normal embedding of S into U is an injective morphism $\varphi : S \mapsto U$. Notice that, for $U = \overline{L}$, this corresponds to the $\mathbb{Q}$-embeddings of $\mathbb{Q}/L$, which we just call embeddings. What do we call such a morphism an "embedding"? Because you "embed" S into U by associating it with its isomorphic image $f(S)$: you get a copy of S in U.

Exercise 6.2.1. Let K be a number field. Prove that the embeddings of K are the non-zero functions $f : K \to \mathbb{C}$ which are both multiplicative and additive.

Exercise 6.2.2*. Let L/K be a finite extension and $\varphi \in \mathrm{Emb}_K(L)$ an embedding of L. Prove that $\varphi(f(\alpha)) = f(\varphi(\alpha))$ for any $f \in K[X]$ and $\alpha \in L$.

Exercise 6.2.3*. Let $\alpha \in L$ be an element and $\sigma \in \mathrm{Emb}_K(L)$ be an embedding. Prove that $\sigma(\alpha)$ is a conjugate of α.

Exercise 6.2.4*. Prove that an embedding is injective.

Why do we care about embeddings? Well, because they are precisely the morphisms obtained by conjugation (in the case where L is generated by one element, which can be achieved thanks to the primitive element theorem)!

Proposition 6.2.1 (Embeddings)*

Let $K(\alpha) = L/K$ be a finite separable extension. The K-embeddings of $K(\alpha)$ are precisely the functions $\varphi : f(\alpha) \mapsto f(\beta)$ where β is some conjugate of α and $f \in K(X)$. In particular, there are exactly $[L : K]$ of them.

Let's check that this statement makes sense: φ is clearly additive and multiplicative, and it indeed fixes K since if $f = k$ is a constant polynomial then $k(\alpha) = k = k(\beta)$. Why doesn't it work for any β then? That's because we need to check it's well defined: an element of $K(\alpha)$ has multiple ways of being written (e.g. $0 = \pi_\alpha(\alpha)$) (here π_a means the minimal polynomial with coefficients in K). This is very easy to show: if $f(\alpha) = g(\alpha)$ then

$$f \equiv g \pmod{\pi_\alpha} \iff f \equiv g \pmod{\pi_\beta}$$

so $f(\beta) = g(\beta)$ which shows that it's well defined. In fact, we have already proven the proposition like this, since by Exercise 6.2.3* $\beta = \varphi(\alpha)$ is a conjugate of α and by Exercise 6.2.2* $\varphi : f(\alpha) \mapsto f(\beta)$.

Remark 6.2.2

If L/K is algebraic separable but not finite, there are **many** embeddings and the fundamental theorem of Galois theory Theorem 6.3.1 does not hold anymore (the way it's currently stated). For L/K **not** algebraic, there are even more embeddings! For instance, if $L = K(\alpha)$ with α transcendental over K, then the embeddings of L/K are $\sigma_\beta : f(\alpha) \mapsto f(\beta)$ for **any** transcendental β. (In other words, transcendental elements are all conjugates in some sense.)

Embeddings give us a systematic way to manipulate conjugation. For instance, the embeddings of $\mathbb{C}/\mathbb{R}$ are the identity and complex conjugation, and using the conjugation embedding we proved Proposition A.1.2. We will illustrate this by an application soon, but we need to build up a few results on embeddings first, namely an equivalent version of Exercise 1.5.20†. Here is how to prove it with the formalism of embeddings (note that it's the same proof, but with more comfortable objects). Note that this result is completely obvious: everything is symmetric between conjugates, so of course they are reached the same number of times. We are just expressing this symmetry more formally.

Proposition 6.2.2*

Let $f \in K[X]$. The m conjugates of $f(\alpha)$ are $f(\varphi(\alpha))$, and each is represented n/m times where $n = [K(\alpha) : K]$ is the degree of α.

Proof

Note that conjugates are reached at least once: this follows from the fundamental theorem of symmetric polynomials: $\prod_i X - f(\alpha_i)$ has integer coefficients where α_i are the conjugates of α. Moreover, by Exercise 6.2.3* $f(\alpha_i)$ is always a conjugate of $f(\alpha)$.

It remains to see that they all appear the same number of times. Suppose $f(\varphi_1(\alpha)) = f(\varphi_2(\alpha)) = \ldots = f(\varphi_{k-1}(\alpha))$ is reached exactly k times, where $\varphi_1 = \mathrm{id}$.

Consider one of its conjugate, $f(\psi(\alpha)) = \psi(f(\varphi_1(\alpha)))$. Since ψ is injective by Exercise 6.2.4*, we conclude that $f(\psi(\alpha))$ is also reached exactly k times, for

$$f(\varphi(\alpha)) = \psi(f(\varphi_i(\alpha)) = f(\psi\varphi_i(\alpha)))$$

and if $f(\psi(\alpha)) = f(\psi'(\alpha))$ then $f(\alpha) = f(\psi^{-1}\psi'(\alpha))$ so $\psi^{-1}\psi' \in \{\varphi_1, \ldots, \varphi_k\}$ as wanted.

■

Remark 6.2.3

Here is how this could be proven without field theory. In fact, in this case it is even a lot quicker. However, we have chosen this approach because in general it is nicer to think in terms of embeddings, and this will be particularly important for Section 6.3. Since all roots of $\pi = \prod_i X - f(\alpha_i)$ are roots of π_α, the factorisation in irreducible polynomials must be π_α^k for some k. This means exactly that all conjugates are reached the same amount of times.

This result can be reformulated to show that, if $M/L/K$ is a tower of extensions such that M/K is separable (since we only defined embeddings for separable extensions), every K-embedding of L extends to exactly $[M : K]/[L : K] = [M : L]$ K-embedding of M.

Proposition 6.2.3*

Any K-embedding of L extends to exactly $[M : L]$ K-embedding of M. In particular, every embedding is reached.

Proof

By Exercise 6.2.3*, embeddings of M/K restrict to embeddings of L/K, and by Proposition 6.2.2 each embedding is reached the same number of times, i.e. $[M:K]/[L:K] = [M:L]$.

■

With these result, we can now define the norm for any finite extension! But first, we present an example that shows the conceptual power of embeddings (which, again, only provide a more comfortable to solve the problem, the essence stays the same).

Problem 6.2.1

Suppose $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ are positive real algebraic numbers such that α_i is maximal out of the absolute value of its conjugates for each i. Prove that, if $\sum_{i=1}^n \alpha_i$ is rational, then $\alpha_i \in \mathbb{Q}$ for each i.

Proof

Consider the embeddings of $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. If $\sum_{i=1}^n \alpha_i \in \mathbb{Q}$ is rational, it is fixed by every embedding σ of K. But, the absolute value of

$$\sum_{i=1}^n \alpha_i = \sigma\left(\sum_{i=1}^n \alpha_i\right) = \sum_{i=1}^n \sigma(\alpha_i)$$

is at most $\sum_{i=1}^n |\sigma(\alpha_i)| \leq \sum_{i=1}^n \alpha_i$. Hence, since we have equality in the triangular inequality, we must have $\sigma(\alpha_i) = u\alpha_i$ for some $|u| = 1$. But then,

$$\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \sigma(\alpha_i) = u\sum_{i=1}^n \alpha_i$$

so $u = 1$. Finally, this means that α_i is fixed by any $\sigma \in \mathrm{Emb}(K)$, which means that its fixed by any $\sigma \in \mathrm{Emb}(\mathbb{Q}(\alpha_i))$ by Proposition 6.2.3. We conclude that its only conjugate is itself: $\alpha_i \in \mathbb{Q}$.

■

Exercise 6.2.5. Solve Problem 6.2.1 without field theory, i.e. using only the content of Chapter 1.

As a notable corollary, we get that $\sum_{i=1}^n \sqrt[k_i]{a_i}$ for positive a_i is rational iff a_i is a perfect k_ith power for each i, which was Exercise 1.5.6. To conclude this section, we define the norm in arbitrary finite extensions.

Definition 6.2.3 (Norm)

Let L/K be a finite separable extension. The *norm* $N_{L/K}$ defined as

$$N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Emb}_K(L)} \sigma(\alpha).$$

Notice in particular that the norm is obviously multiplicative because the embeddings are! As an example, the norm in $\mathbb{C}/\mathbb{R}$ is the square of the module: $\mathbb{N}(a+bi) = a^2 + b^2 = |a+bi|^2$. Here is a bad application of the multiplicativity of the norm, which nonetheless appeared in a USA TST.

Problem 6.2.2 (USA TST 2012)

Do there exist abritrarily large rational integers a, b, c such that $a^3 + 2b^3 + 4c^3 = 6abc + 1$?

Solution

One can check that $N_{\mathbb{Q}(\sqrt[3]{2})}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc$. Thus we want to find elements of norm 1 in this field. Notice that $N_{\mathbb{Q}(\sqrt[3]{2})}(1 + \sqrt[3]{2} + \sqrt[3]{4})$ so

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} = (1 + \sqrt[3]{2} + \sqrt[3]{4})^n$$

will also have norm 1 for any n. Pick an n sufficiently large and we are done. ■

Exercise 6.2.6*. Check that $N_{\mathbb{Q}(\sqrt[3]{2})}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc$.

Norms in different extensions are linked by the following proposition. This is left as an exercise in the next section, as we need to define Galois groups to prove it.

Proposition 6.2.4

Let $M/L/K$ be a tower of finite separable field extensions. Then $N_{M/K} = N_{L/K} \circ N_{M/L}$.

6.3 Galois Theory

Galois theory studies *Galois* extensions, i.e. extensions closed under embeddings. An algebraic extension L/K means that every element of L is algebraic over K.

Definition 6.3.1 (Galois Extension)

A *Galois* extension L/K is a separable algebraic extension closed under embeddings, meaning that for any $\alpha \in L$, all the conjugates of α also lie in L.

The simplest case of a Galois extension are the quadratic fields we say in Chapter 2 and the cyclotomic fields $\mathbb{Q}(\omega)$ where ω is a root of unity. Indeed, all its conjugates have the form $\omega^k \in \mathbb{Q}(\omega)$. It is easy to construct Galois extensions: one starts with any extension $K(\alpha)$ and then gets the *galois closure* $L = K(\alpha_1, \ldots, \alpha_n)$ by adding the conjugates $\alpha_1, \ldots, \alpha_n$ of α.

Exercise 6.3.1*. Check that $K(\alpha_1, \ldots, \alpha_n)/K$ is Galois and prove that any Galois extension has this form.

Galois extensions are particularly interesting because $\mathrm{Emb}_K(L)$ becomes a *group*, meaning that the composition of two embeddings is still an embedding since embeddings are now $L \to L$. We thus denote $\mathrm{Emb}_K(L)$ as $\mathrm{Aut}_K(L)$ (also written $\mathrm{Aut}(L/K)$) when L is Galois, because its embeddings are now *automorphisms*.

Definition 6.3.2 (Galois Group)

The *Galois group* $\mathrm{Gal}(L/K)$ of an extension L/K is its group of K-embeddings: $\mathrm{Aut}_K(L)$.

Exercise 6.3.2*. Can you write the Galois group of a quadratic extension L/K in a way that doesn't depend on L or K? (More specifically, show that the Galois groups of quadratic extensions are all isomorphic.)

Exercise 6.3.3*. Check that the Galois group is a group under composition. (You may assume that each element has an inverse, this will be proven later as a corollary of Theorem 2.5.1.)

Exercise 6.3.4. Let L/K be Galois and $K \subseteq M \subseteq L$ be an intermediate field. Prove that $\mathrm{Emb}_K(M)$ is a system of representatives of $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$, where the quotient means $\mathrm{Gal}(L/K)$ modulo $\mathrm{Gal}(L/M)$, i.e. we say $\sigma' \equiv \sigma$ if $\sigma^{-1} \circ \sigma' \in \mathrm{Gal}(L/M)$. (Our quotient A/B is more commonly though of as the set of *right-cosets* of B in A, i.e. the sets Ba for $a \in A$ (which we just wrote as a in our case).) (See also Exercise A.3.14†.)

Exercise 6.3.5. Prove Proposition 6.2.4 using Exercise 6.3.4. (This is a bit technical.)

Again, when $K = \mathbb{Q}$, we may drop the K in the notation. We will also sometimes write $G(L/K)$. Here is the most important Galois group: $\mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q})$ where ω_n is a primitive nth root of unity. By Theorem 3.2.1, this is $\sigma_k : \omega_n \mapsto \omega_n^k$ for $\gcd(n,k) = 1$. Note that $\sigma_i \circ \sigma_j$ maps ω_n to $(\omega^j)^i = \omega^{ij}$. This means that $\sigma_i \circ \sigma_j = \sigma_{ij}$. It is thus *isomorphic* to $(\mathbb{Z}/n\mathbb{Z})^\times$: just label σ_k as $k \pmod n$ and this makes sense by the previous consideration on composition (which becomes multiplication in $(\mathbb{Z}/n\mathbb{Z})^\times$). In particular, it is *abelian*indexgroup!abelian which means that $ab = ba$ (composition commutes).

Another particularly simple Galois group is $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$: by Theorem 4.3.1, its elements are

$$\mathrm{id}, \varphi_p, \varphi_p^2, \dots, \varphi_p^{n-1}.$$

In particular, it is generated by only one element: if we relabel φ_p^k as $k \pmod n$ we get $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$!

Before we state and prove the fundamental theorem of Galois theory, here is a quick application of the Galois group which is a special case of **??**.

Problem 6.3.1

Is $\sqrt[3]{2}$ a sum of roots of unity?

Solution

Suppose that this $\sqrt[3]{2} \in \mathbb{Q}(\omega)$ for some root of unity ω. $X^3 - 2$ is irreducible in $\mathbb{Q}[X]$, so the conjugates of $\sqrt[3]{2}$ are $\zeta^i \sqrt[3]{2}$ where ζ is a primitive third root of unity. Since $\mathbb{Q}(\omega)$ is Galois, $K = \mathbb{Q}(\sqrt[3]{2}, \zeta) \subseteq \mathbb{Q}(\omega)$. By Proposition 6.2.3, $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ restricts to (multiple copies of) $G = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta))$.

The key point is that $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ is abelian (commutes), while G isn't so this is impossible. We have already shown that the former is abelian, so it remains to show that G is not. We claim that the embeddings of K are

$$\sigma_{(a,b)} : \begin{cases} \sqrt[3]{2} \mapsto \zeta^a \sqrt[3]{2} \\ \zeta \mapsto \zeta^b \end{cases}$$

for (independent) $a \in \mathbb{Z}/3\mathbb{Z}$ and $b \in (\mathbb{Z}/3\mathbb{Z})^\times$.

Clearly, these are all the possible embeddings of K, so it remains to check that they are indeed embeddings, i.e. that $[K : \mathbb{Q}] = 3 \cdot 2 = 6$. Since

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\zeta)][\mathbb{Q}(\zeta) : \mathbb{Q}] = 2[K : \mathbb{Q}(\zeta)],$$

it remains to prove that $[K : \mathbb{Q}(\zeta)] = 3$, i.e. that $X^3 - 2$ is irreducible over $\mathbb{Q}(\zeta)$. This is very easy: if it wasn't the case it would have a root in $\mathbb{Q}(\zeta)$, so $\mathbb{Q}(\zeta)$ would contain an element of degree 3 which is impossible as $\mathbb{Q}(\zeta)$ has degree 2.

Finally, one can see that G is not abelian as $\sigma_{(0,-1)} \circ \sigma_{(1,1)} = \sigma_{(-1,-1)}$, but $\sigma_{(1,1)} \circ \sigma_{(0,-1)} = \sigma_{(1,-1)}$. Therefore, $\sqrt[3]{2}$ is not a sum of roots of unity. ■

Remark 6.3.1

In fact, the Kronecker-Weber theorem asserts the converse: if $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, K is contained in a cyclotomic field $\mathbb{Q}(\omega)$ for some root of unity ω.

Exercise 6.3.6*. Compute $\sigma_{(0,-1)} \circ \sigma_{(1,1)}$ and $\sigma_{(1,1)} \circ \sigma_{(0,-1)}$.

Here is the main reason why Galois groups are interesting.

Theorem 6.3.1 (Fundamental Theorem of Galois Theory)

Let L/K be a finite Galois extension. There is a one-to-one correspondence – called the *Galois correspondence* – between *subgroups* H of $\mathrm{Gal}(L/K)$ (subsets closed under composition and inversion) and the intermediate fields $L/M/K$. This correspondence is given by

$$H \mapsto L^H,$$

where L^H is the fixed field of H, i.e. the elements of L which are fixed by all of H. The reverse direction is given by

$$M \mapsto \mathrm{Gal}(L/M).$$

Proof

Note that $\mathrm{Gal}(L/M) = \mathrm{Emb}_M(L)$. In particular, the elements fixed by $\mathrm{Gal}(L/M)$ are those which have only one M-conjugate: they are thus in M. This shows that $L^{\mathrm{Gal}(L/M)} = M$.

It remains to prove that $\mathrm{Gal}(L/L^H) = H$. Clearly, $H \subseteq \mathrm{Gal}(L/L^H)$ since H fixes L^H by definition. Write $L = L^H(\alpha)$: the cardinality of $\mathrm{Gal}(L/L^H)$ is the degree of α (over L^H). However, note that

$$e_i(\sigma_1(\alpha), \dots, \sigma_k(\alpha))$$

is fixed by H for any i, where $\sigma_1, \dots, \sigma_k$ are the elements of H (this is because $\sigma H = H$ for any $\sigma \in H$). Thus, α has at most k conjugates. To conclude, we have $H \subseteq \mathrm{Gal}(L/L^H)$ and $|\mathrm{Gal}(L/L^H)| \leq |H|$ which implies $H = \mathrm{Gal}(L/L^H)$.

■

Remark 6.3.2

There is an explicit way of choosing a primitive element of L^H from a primitive element of L. If $L = K(\alpha)$, set $f_H(X) = \prod_{\sigma \in H} X - \sigma(\alpha)$. For sufficiently large $n \in \mathbb{Z}$, $f_H(n)$ is fixed only by H: since σf_H and f_H are distinct polynomials for $\sigma \notin H$, they have a finite number of common roots. Finally, if β is fixed only by H, then $\mathrm{Gal}(L/K(\beta)) = H$ by definition, which means $K(\beta) = L^H$.

Exercise 6.3.7*. Prove that $e_i(\sigma_1(\alpha), \dots, \sigma_k(\alpha))$ is fixed by H for any i.

For $L/K = \mathbb{F}_{p^n}/\mathbb{F}_p$ for instance, this is Corollary 4.3.1. Indeed, the (additive, so closed under addition) subgroups of $\mathbb{Z}/n\mathbb{Z}$ are simply $\mathbb{Z}/d\mathbb{Z}$ for $d \mid n$ and the fixed field $\mathbb{F}_{p^n}^{\mathbb{Z}/d\mathbb{Z}}$ is $\mathbb{F}_{p^{n/d}}$, the fixed field of $\varphi_p^{n/d}$ (as $\mathbb{Z}/d\mathbb{Z}$ is generated by $\varphi_p^{n/d}$). We now present a quick application of the fundamental theorem of Galois theory in the case of cyclotomic fields.

Problem 6.3.2

Let ω_m be a primitive mth root of unity, and ω_n a primitive nth root of unity. What are $\mathbb{Q}(\omega_m, \omega_n)$ and $\mathbb{Q}(\omega_m) \cap \mathbb{Q}(\omega_n)$?

Solution

Let ω be a primitive mnth root of unity and σ_k be the embedding $\omega \mapsto \omega^k$.

Let ω_d be a primitive dth root of unity where $d \mid mn$. Notice that $\mathbb{Q}(\omega_d)$ is the fixed field of

$$H_d = \{\sigma_k \mid kmn/d \equiv_{mn} mn/d \iff k \equiv_d 1\}$$

since these are exactly the automorphisms such that $\sigma_k(\omega_d) = \omega_d$, as $\omega_d = \omega^{mn/d}$. In particular,

$$H_m \cap H_n = \{\sigma_k \mid k \equiv_m 1, k \equiv_n 1\} = \{\sigma_k \mid k \equiv_{\mathrm{lcm}(m,n)} 1\} = H_{\mathrm{lcm}(m,n)}.$$

This means that $\mathbb{Q}(\omega_m, \omega_n)$ is $\mathbb{Q}(\omega_{\mathrm{lcm}(m,n)})$ by Exercise 6.3.8*. Similarly, the group generated by H_m and H_n is

$$\langle H_m, H_n \rangle = \{ab \mid a \equiv_m 1, b \equiv_n 1\} = H_{\gcd(m,n)}$$

since $(1+am)(1+bn) \equiv_{mn} 1+(am+bn)$ goes through every residue which is 1 modulo $\gcd(m,n)$ by Bézout's lemma. Thus, $\mathbb{Q}(\omega_m) \cap \mathbb{Q}(\omega_n)$ is $\mathbb{Q}(\omega_{\gcd(m,n)})$. ■

Remark 6.3.3

In fact, a very direct proof could be given for $\mathbb{Q}(\omega_m, \omega_n) = \mathbb{Q}(\omega_{\mathrm{lcm}(m,n)})$: one inclusion is trivial, and for the other we have

$$\exp\left(\frac{2i\pi}{m}\right)^b \exp\left(\frac{2i\pi}{n}\right)^a = \exp\left(\frac{2i\pi}{\mathrm{lcm}(m,n)}\right)$$

where $am + bn = \gcd(m,n)$. However, such a proof does not work anymore for $\mathbb{Q}(\omega_m) \cap \mathbb{Q}(\omega_n)$ because we do not have access directly to this field. For instance, $K(\omega_m, \omega_n) = K(\omega_{\mathrm{lcm}(m,n)})$ is always true, but $K(\omega_m) \cap K(\omega_n) = K(\omega_{\gcd(m,n)})$ isn't always! As an example, if $K = \mathbb{Q}(\sqrt{3})$, then $K(i) = \mathbb{Q}(i, \sqrt{3}) = K(j)$ where j is a primitive cube root of unity. Thus, $K(i) \cap K(j) \neq K$.

Exercise 6.3.8*. Given two subfields A and B of a field L, define their *compositum* or *composite field* AB as the smallest subfield of L containing both A and B (in other words, the field generated by A and B). Let L/K be a finite Galois extension and A, B be intermediate fields. Prove that $\mathrm{Gal}(L/AB) = \mathrm{Gal}(L/A) \cap \mathrm{Gal}(L/B)$.

Exercise 6.3.9*. Given two subgroups H_1, H_2 of a group H, define the subgroup they generate, $\langle H_1, H_2 \rangle$, as the smallest subgroup containing both H_1 and H_2. Let L/K be a finite Galois extension and A, B be intermediate fields. Prove that $\mathrm{Gal}(L/A \cap B) = \langle \mathrm{Gal}(L/A), \mathrm{Gal}(L/B) \rangle$.

Here are a few additional properties of the Galois correspondence.

Proposition 6.3.1

We have $[L^H : K] = |G|/|H|$ where $G = \mathrm{Gal}(L/K)$.

Proof

$|H| = |\mathrm{Aut}(L/L^H)| = [L : L^H]$ and $|G| = [L : K]$ so

$$[L^H : K] = \frac{[L:K]}{[L:L^H]} = \frac{|G|}{|H|}.$$

■

Proposition 6.3.2

The Galois correspondence is *inclusion reversing*: $H_1 \subseteq H_2 \iff L^{H_1} \supseteq L^{H_2}$.

Exercise 6.3.10*. Prove Proposition 6.3.2.

Here is another application of the fundamental theorem of Galois theory, generalising Problem 6.3.1.

Problem 6.3.3

When is $\sqrt[n]{2}$ a sum of roots of unity?

Solution

Suppose that $\mathbb{Q}(\sqrt[n]{2}) \subseteq \mathbb{Q}(\omega)$ for some root of unity ω. By Exercise 6.3.11*, any subfield of $\mathbb{Q}(\omega)$ is Galois over $\mathbb{Q}$, so $\mathbb{Q}(\sqrt[n]{2})$ also is. Note that, since $X^n - 2$ is irreducible by Eisenstein's criterion, the conjugates of $\sqrt[n]{2}$ are $\zeta^k \sqrt[n]{2}$ where ζ is a primitive nth root of unity. In particular, we must have $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\sqrt[n]{2}) \subseteq \mathbb{R}$, which implies $n = 1$ or $n = 2$. Conversely, these works: $2 = 1 + 1$ and $\sqrt[n]{2} = \pm(\omega + 1/\omega)$ for any primitive eight root of unity ω. Indeed,

$$\left(\omega + \frac{1}{\omega}\right)^2 = \omega^2 + \frac{1}{\omega^2} + 2 = 2$$

as $\omega^4 = -1$ (this is a Gauss sum). ■

Exercise 6.3.11*. Let L/K be a finite Galois extension and let M be an intermediate field. Prove that, for any $\sigma \in \mathrm{Gal}(L/K)$, $\mathrm{Gal}(L/\sigma M) = \sigma \,\mathrm{Gal}(L/M)\sigma^{-1}$. Deduce that the intermediate fields which are also Galois (over K) are $M = L^H$ where H is a *normal* subgroup of $G = \mathrm{Gal}(L/K)$, meaning that $\sigma H \sigma^{-1} = H$ for any $\sigma \in G$. In particular, if L/K is *abelian*, meaning that its Galois group is, any intermediate field is Galois over K.

This fundamental theorem of Galois theory lets us get deeper insight on the Gauss sums of Section 4.5. Indeed, the Galois group of $\mathbb{Q}(\omega)$ where ω is a primitive qth root of unity is (isomorphic to) $(\mathbb{Z}/q\mathbb{Z})^\times$. By Galois theory (and a bit of group theory), we already know that this field contains a unique field of degree 2: indeed, by Proposition 6.3.1, it's L^H where $|G|/|H| = 2$. It can be seen easily that the unique such subgroup is the subgroup of quadratic residues. Let σ_k denote the embedding $\omega \mapsto \omega^k$. Hence, we get

$$\sum_{\left(\frac{k}{q}\right)=1} \omega^k \in L^H$$

and

$$\sum_{\left(\frac{k}{q}\right)=-1} \omega^k \in L^H$$

(they are fixed by the embeddings of H) and then it's just a matter of computing the value of these sums to deduce what the quadratic field is. To simplify things a bit we can consider our Gauss sum since when we square it it's fixed by all automorphisms which means it's rational.

Once we know that this quadratic field is $\mathbb{Q}(\sqrt{q^*})$ where $q^* = (-1)^{\frac{q-1}{2}} 1$, we directly[1] get the law of quadratic reciprocity (without using the Gauss sum): if $\sqrt{q^*} = f(\omega) \in L^H$ for some $f \in \mathbb{Z}[X]$, then

$$(\sqrt{q^*})^p \equiv \sigma_p(q^*) \pmod{p}$$

by Frobenius and this is equal to q^* iff $\sigma_p \in H$, i.e. p is a quadratic residue modulo q. Otherwise, it's its other conjugate $-\sqrt{q^*}$. The rest of the proof is the same as before.

[1] Actually, we need to know that the denominator of the coefficients of f are not divisible by p, so that f makes sense over $\mathbb{F}_p$ and we can use the Frobenius morphism. This follows for instance from Exercise 3.5.26†.

To finish with the quadratic reciprocity law, we said that we didn't need to use Gauss sums, but then how do we show that $\sqrt{q^*} \in \mathbb{Q}(\omega)$ without computing them? One way of doing this is to notice that, on the one hand,

$$\prod_{k=1}^{q-1} 1-\omega^k = \Phi_q(1) = q.$$

On the other hand,

$$\prod_{k=1}^{q-1} 1-\omega^k = \prod_{k=1}^{\frac{q-1}{2}} (1-\omega^k)(1-\omega^{-k}) = \prod_{k=1}^{q-1} 1-\omega^k = \prod_{k=1}^{\frac{q-1}{2}} \omega^{-k}(1-\omega^k)^2 = (-1)^{\frac{q-1}{2}}\omega^\ell \left(\prod_{k=1}^{\frac{q-1}{2}}(1-\omega^k)\right)^2$$

so $(-1)^{\frac{q-1}{2}}q$ is a square (ω^ℓ is a square: just choose $\ell' \equiv \ell/2 \pmod q$ to get $\omega^\ell = (\omega^{\ell'})^2$) thus concluding our new proof of the quadratic reciprocity law.

Exercise 6.3.12*. Fill in the details of this proof of the quadratic reciprocity law.

We worked hard to get all of this, so here is a concrete application of the fundamental theorem of Galois theory, which generalises Proposition 4.4.2.

Problem 6.3.4 (Schur)

Let H be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ (i.e. a subset closed under multiplication and inversion, or equivalently just closed under multiplication by little Fermat). Prove that there exists a polynomial $f \in \mathbb{Z}[X]$ such that, for any rational prime $p \nmid n$, $f \pmod p$ has all its roots in $\mathbb{F}_p$ when $p \pmod n \in H$, and no roots in $\mathbb{F}_p$ otherwise, up to a finite number of exceptions.

Proof

If one tries to copy the construction of Ψ in Proposition 4.4.2, one might choose f to be the minimal polynomial polynomial of $\sum_{h\in H}\omega^h$ where ω is a complex primitive nth root of unity. However, when we need to show that

$$\left(\sum_{h\in H}\zeta^h\right)^p = \sum_{h\in H}\zeta^{ph}$$

is equal to $\sum_{h\in H}\zeta^h$ (where ζ is now a primitive nth root of unity in $\overline{\mathbb{F}}_p$) iff $p \pmod n \in H$ we run into trouble. First, notice that this is equivalent to

$$\sum_{h\in H}\omega^{ph} = \sum_{h\in H}\omega^h$$

for sufficiently large p by the fundamental theorem of symmetric polynomials. Indeed, suppose there are infinitely many primes $p \equiv k \pmod n$ such that f has a root in $\mathbb{F}_p$. Consider the (absolute) norm of $\sum_{h\in H}\omega^{hk} - \sum_{h\in H}\omega^h$: if $\sum_{h\in H}\zeta^{hk} = \sum_{h\in H}\zeta^h$ this norm is divisible by p so if it's true infinitely many times it must be zero (which we want to show is false if $k \notin H$). Conversely, clearly if $p \pmod n \in H$, f has all its roots ζ^h in $\mathbb{F}_p$.

Unfortunately, it is not always true that $\sum_{h\in H}\omega^h$ is distinct from its conjugates $\sum_{h\in H}\omega^{kh}$ for $k \notin H$. Indeed, let $n = 12$ and $H = \{1, 7\}$: we get $\omega + \omega^7 = \omega(1+\omega^6) = 0$ which is absolutely not what we want.

However, if we think a bit about what we want, we realise that we wish that $\sigma_k(r) = r$ if and only if $k \in H$ where $r \in \mathbb{Q}(\omega)$ is a root of f (since $\varphi_p(r) = \sigma_p(r)$). This is exactly what it means for r to be in $\mathbb{Q}(\omega)^H$! Thus, we are done: just choose r to be a generator of $\mathbb{Q}(\omega)^H$.

■

Exercise 6.3.13*. Convince yourself of this solution.

Since Galois theory is very much related to group theory (via the Galois group), we finish the section with two fundamental group theory results: the Lagrange and Cauchy theorems. The former generalises Fermat's little theorem. It shows that a subgroup of a finite group is just a subset closed under multiplication (or addition depending on what your operation is), without needing the assumption that it's closed under inversion too. Keep in mind that a group is not necessary abelian, so our proof of Theorem 4.2.1 does not work for this. Also, remember that the identity e of a group G is an element such that $ge = eg = g$ for any $g \in G$. The latter constitutes a converse of Lagrange's theorem when the order is prime: it shows that, as long as p divides $|G|$, there is an element of order p.

Exercise 6.3.14*. Prove that the identity of a group is unique.

Theorem 6.3.2 (Lagrange's Theorem)

Let G be a group of cardinality n (we also say G has order n) with the operation $\cdot$. Then, for any $g \in G$, the order of g, meaning the smallest $k > 0$ such that $g^k = e$, divides n.

Proof

The proof will be combinatorial. Let m be the order of G. Partition G into orbits of the form $O_h = \{h, hg, hg^2, \ldots\}$. We claim that this is indeed a partition: if $O_h \cap O_{h'} \neq \emptyset$ then $O_h = O_{h'}$.

Indeed, if $hg^i = h'g^j$ for some i, j then $hg^k = h'g^{j-i+k}$ for any k so $O_h = O_{h'}$. Since each orbit has cardinality m, we conclude that $m \mid n$.

■

Exercise 6.3.15*. Prove the following refinement of Theorem 2.5.1: if G is a finite group and H a subgroup of G, $|H|$ divides $|G|$. Why does it imply Theorem 2.5.1?

Theorem 6.3.3 (Cauchy's Theorem)

Let G be a finite group. If $p \mid |G|$ is a rational prime, then, G has an element of order p.

Proof

The proof is again combinatorial (group theory is very combinatorial). Consider the set S of $(g_1, \ldots, g_p) \in G$ such that $g_1 \cdot \ldots \cdot g_p = e$, the identity of G. There are $p \mid |G|^{p-1}$ such tuples. Now group them by circular permutations: consider the orbits

$$\{(g_1, \ldots, g_p), (g_2, \ldots, g_1), \ldots, (g_p, \ldots, g_{p-1})\}.$$

The size of each orbit has size 1 or p: indeed, if σ denotes the circular permutation $(x_1, \ldots, x_p) \mapsto (x_2, \ldots, x_1)$, we have $\sigma^p = \mathrm{id}$ so the order of σ divides p by Lagrange's theorem (in the group of permutations of $(x_1, \ldots, x_p)$, which might not be $\mathfrak{S}_n$ for fixed x_i). (This can also be seen directly: if $\sigma^k(g_1, \ldots, g_p) = (g_1, \ldots, g_p)$, then $g_{i+kn} = g_i$ so if k is invertible modulo p, $g_i = g_j$ for any $i \neq j$ which means the orbit has size 1, and otherwise the orbit has size p.)

Thus, modulo p, the cardinality of S is congruent to the number of orbits of size 1. However, $(g, \ldots, g)$ is in S iff $g^p = e$, i.e. g has order 1 or p. Thus, if we let n_p denote the number of elements of order p, we get

$$1 + n_p \equiv |S| \equiv 0 \pmod{p}$$

since $p \mid |S| = |G|^{p-1}$, which implies that n_p is non-zero as wanted.

■

6.4 Splitting of Polynomials

We shall now discuss an application of the primitive element theorem, other than that it lets us build Galois theory quickly. We have already seen in Section 5.2 that, when $f \in \mathbb{Z}[X]$ is non-constant, the set $\mathcal{P}(f)$ of rational primes p such that $f \pmod p$ has a root in $\mathbb{F}_p$ is infinite. Here, we show a stronger result, namely that $\mathcal{P}_{\text{split}}(f)$, the set of rational primes which don't divide the leading coefficient of f such that f is split modulo p, meaning that f has as many roots in $\mathbb{F}_p$ as its degree, is infinite.

Theorem 6.4.1

For any non-constant polynomial $f \in \mathbb{Z}[X]$ of leading coefficient a, there are infinitely many rational primes $p \nmid a$ such that $f \pmod p$ is split in $\mathbb{F}_p$, meaning that its root in $\overline{\mathbb{F}}_p$ are all in $\mathbb{F}_p$.

Proof

Without loss of generality, we can assume $f \in \mathbb{Q}[X]$ is monic; the condiiton $p \nmid a$ becomes that p doesn't divide the denominators of the coefficients. Let $\alpha_1, \dots, \alpha_n$ be the roots of f, and $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$. By the primitive element theorem, there is a β such that $K = \mathbb{Q}(\beta)$. Consider the minimal polynomial π of β: we show that whenever $\pi \pmod p$ has a root in $\mathbb{F}_p$ and p is sufficiently large, $f \pmod p$ is split in $\mathbb{F}_p$. By Theorem 5.2.1, there are infinitely many such primes.

Indeed, we know that β generates the roots α_i of f in $\overline{\mathbb{Q}}$, so we might expect the same to hold in $\mathbb{F}_p$. It is in fact quite easy to show that this intuition holds true. Let $g_1, \dots, g_n \in \mathbb{Q}[X]$ be such that $f_i(\beta) = \alpha_i$.

Let p be greater than the denominators of the g_i so that $g_i \pmod p$ makes sense and suppose $\beta_p \in \mathbb{F}_p$ is a root of $\pi \pmod p$. We shall show that

$$f \equiv \prod_{k=1}^{n} X - g_k(\beta_p).$$

Consider the coefficient in front of X^i: $\pm e_i(g_1, \dots, g_n)$ evaluated at β_p. By assumption,

$$e_i(g_1, \dots, g_n)(\beta) = a_i \in \mathbb{Q}$$

so that $\pi \mid e_i(g_1, \dots, g_n) - a_i$. Using Gauss's lemma, this divisibility becomes a divisibility in $\mathbb{F}_{[}X]]$ (as p doesn't divide the denominators of g_i) which means that we also have

$$e_i(g_1, \dots, g_n)(\beta_p) \equiv a_i.$$

This concludes the proof.

■

As an important corollary, we get that any set of non-constant polynomials have infinitely many common prime divisors.

Corollary 6.4.1

For any non-constant polynomials $f_1, \dots, f_n \in \mathbb{Z}[X]$, $\mathcal{P}_{\text{split}}(f_1) \cap \dots \cap \mathcal{P}_{\text{split}}(f_n)$ is infinite.

Proof

Apply Theorem 6.4.1 to $f = f_1 \cdot \ldots \cdot f_n$.

■

From this, we can deduce the following very non-trivial result.

Corollary 6.4.2

Let $n \geq 1$ be a rational integer. Any non-constant polynomial $f \in \mathbb{Z}[X]$ has infinitely many prime factors $p \equiv 1 \pmod{n}$.

Proof

Apply Corollary 6.4.1 to f and Φ_n.

■

Exercise 6.4.1. Does there exist an $a \not\equiv 1 \pmod{n}$ such that any non-constant $f \in \mathbb{Z}[X]$ has infinitely many prime factors congruent to a modulo n?

6.5 Exercises

Field and Galois Theory

Exercise 6.5.1†**.** Let L/K be a finite separable extension of prime degree p. If $f \in K[X]$ has prime degree q and is irreducible over K but reducible over L, then $p = q$.

Exercise 6.5.2†**.** Let L/K be a finite Galois extension and M/K be a finite extension. Prove that $\mathrm{Gal}(LM : M) \simeq \mathrm{Gal}(L : L \cap M)$. In particular, $[LM : L] = [L : L \cap M]$. Conclude that, if L/K and M/K are Galois, we have

$$[LM : K][L \cap M : K] = [L : K][M : K].$$

Exercise 6.5.3†**.** Prove that, for any n, there is a finite Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/n\mathbb{Z}$.

Exercise 6.5.4† (Cayley's Theorem)**.** Let G be a finite group. Prove that it is a subgroup of $\mathfrak{S}_n$ for some n. Conclude that there is a finite Galois extension L/K of number fields such that $G \simeq \mathrm{Gal}(L/K)$. (This is part of the *inverse Galois problem*. So far, it has only been conjectured that we can choose $K = \mathbb{Q}$.)

Exercise 6.5.5† (Dedekind's Lemma)**.** Let L/K be a finite separable extension in characteristic 0. Prove that the K-embeddings of L are linearly independent.

Exercise 6.5.6† (Hilbert's Theorem 90)**.** Suppose L/K is a *cyclic* extension in characteristic 0, meaning its Galois group $\mathrm{Gal}(L/K) \simeq (\mathbb{Z}/n\mathbb{Z}, +)$ for some n (like $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$) or $\mathrm{Gal}(\mathbb{Q}(\exp(2i\pi/p))/\mathbb{Q})$). Prove that $\alpha \in L$ has norm 1 if and only if it can be written as $\beta/\sigma(\beta)$ for some $\beta \in L$, where σ is a generator of the Galois group (element of order n).

Exercise 6.5.7. When are two number fields isomorphic?

Exercise 6.5.8† (Lüroth's Theorem)**.** Let K be a field and L a field between K and $K(T)$. Prove that there exists a rational functions $f \in K(T)$ such that $L = K(f)$.

nth Roots

Exercise 6.5.9†. Let K be a field, p a prime number, and α an element of K. Prove that $X^p - \alpha$ is irreducible over K if and only if it has no root.

Exercise 6.5.10†. Let $f \in K[X]$ be a monic irreducible polynomial and p a rational prime. Suppose that $(-1)^{\deg f} f(0)$ is not a pth power in K. Prove that $f(X^p)$ is also irreducible.

Exercise 6.5.11† (Vahlen, Capelli, Redei)**.** Let K be a field and $\alpha \in K$. When is $X^n - \alpha$ irreducible over K?

Exercise 6.5.12†. Let $n \geq 1$ be an integer and ζ a primitive nth root of unity. What is the Galois group of $\mathbb{Q}(\sqrt[n]{2}, \zeta)$ over $\mathbb{Q}$?

Exercise 6.5.13†. Let $n \geq 1$ be an integer and $p_1, \ldots, p_m$ rational primes. Prove that

$$[\mathbb{Q}(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m}) : \mathbb{Q}] = n^m.$$

(This is a generalisation of Exercise 4.6.24†.)

Exercise 6.5.14† (Kummer Theory)**.** Let L/K be a finite Galois extension in characteristic 0. Suppose that $\mathrm{Gal}(L/K) \sim \mathbb{Z}/n\mathbb{Z}$. If K contains a primitive nth root of unity, prove that $L = K(\alpha)$ for some $\alpha^n \in K$.

Exercise 6.5.15† (Artin-Schreier Theorem)**.** Let L/K be a finite extension such that L is algebraically closed. Prove that $[L : K] \leq 2$.

Constructibility and Solvability

Exercise 6.5.16†. Given two points, you are allowed to draw the line between them, as well as the circle of center one of the points going through the other. Initially, you may start with the points $(0, 0)$ and $(0, 1)$ and define additional points that way. We say a real number r is *constructible* if the point $(0, r)$ is constructible. Prove that, if x and y are constructible, so are $x + y$, xy, $-x$, $\sqrt{|x|}$, and $\frac{1}{x}$ if $x \neq 0$.

Exercise 6.5.17†. Prove that a real number is constructible if and only if it is algebraic and the degree of its splitting field, meaning the field generated by its conjugates, is a power of 2. Deduce that, using only a (non-graded) ruler and a compass,

1. A regular n-gon is constructible if and only if $\varphi(n)$ is a power of 2.
2. It is not always possible to trisect an angle.
3. Given a square with area A, it is not possible to construct a square with area $2A$.

Exercise 6.5.18†. We say a finite Galois extension L/K in characteristic 0 is *solvable by radicals* if there is a tower of extensions

$$K = K_0 \subset K_1 \subset \ldots \subset K_m \supseteq L$$

such that K_{i+1} is obtained from K_i by adjoining an nth root of some element of K_i to K_i, for some n. We also say a group G is *solvable* if there is a chain $0 = G_0 \subset G_1 \subset \ldots \subset G_m = G$ such that G_i is normal in G_{i+1} (see Exercise 6.3.11*) and G_{i+1}/G_i is cyclic. Prove that L/K is solvable by radicals if and only if its Galois group is. (When L is the field generated by the roots of a polynomial $f \in K[X]$, L/K being solvable by radicals means that the roots of f can be written with radicals, which explains the name.)

Exercise 6.5.19†. Let $n \geq 1$ be an integer. Prove that $\mathfrak{S}_n$ is not solvable for $n \geq 5$. Conclude from Exercise 6.5.21† that some polynomial equations are not solvable by radicals.[2] (This is quite technical.)

[2] If one only wants to show that there is no general formula, one doesn't need to do the first part since the general polynomial $\prod_{i=1}^{n} X - A_i \in \mathbb{Q}(A_1, \ldots, A_n)[X]$ already has Galois group $\mathfrak{S}_n$ (where $A_1, \ldots, A_n$ are formal variables).

Exercise 6.5.20†. We say a finite Galois extension L/K of real fields, i.e. $L \subseteq \mathbb{R}$, is *solvable by real radicals* if there is a tower of extensions

$$K = K_0 \subset K_1 \subset \ldots \subset K_m \supseteq L$$

such that K_{i+1} is obtained from K_i by adjoining the nth root of some positive element of K_i to K_i. Prove that L/K is solvable by real radicals if and only if $[L : K]$ is a power of 2.

Exercise 6.5.21†. Let p be a prime number and $G \subseteq \mathfrak{S}_p$ a subgroup containing a transposition τ (see the paragraph after Definition C.3.2) and an element γ of order p. Prove that $G = \mathfrak{S}_p$. Deduce that, if $f \in \mathbb{Q}[X]$ is an irreducible polynomial of degree p with precisely two non-real complex roots, then the Galois group of the field generated by its roots (called its *splitting field*, because it is a field where it splits) over $\mathbb{Q}$ is $\mathfrak{S}_p$.

Exercise 6.5.22†. Let n be a positive integer. Prove that there is a number field K, Galois over $\mathbb{Q}$, such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathfrak{S}_n$. (You may assume the following result of Dedekind: if $f \in \mathbb{Z}[X]$ is a polynomial, for any prime number p not dividing the discriminant Δ of f, the Galois group of f over $\mathbb{F}_p$ is a subgroup of the Galois group of f over $\mathbb{Q}$.[3])

Cyclotomic Fields

Exercise 6.5.23†. Let ω be a primitive nth root of unity. When is Φ_m irreducible over $\mathbb{Q}(\omega)$?

Exercise 6.5.24. Prove that $\mathbb{Q}(\omega_m, \omega_n) = \mathbb{Q}(\omega_m + \omega_n)$, where ω_m and ω_n are primitive mth and nth roots of unity respectively.

Exercise 6.5.25†. Let n be an integer and $m \in \mathbb{Z}/n\mathbb{Z}$ be such that $m^2 \equiv 1 \pmod{n}$. Prove that there exist infinitely many primes congruent to m modulo n, provided that there exists at least one which is greater than n^2. (It is also true that our Euclidean approach to special cases of Dirichlet's theorem only works for $m^2 \equiv 1 \pmod{n}$, see **??**.)

Exercise 6.5.26† (Mann)**.** Suppose that $\omega_1, \ldots, \omega_n$ are roots of unity such that $\sum_{i=1}^{n} a_i\omega_i = 0$ for some $a_i \in \mathbb{Q}$ and $\sum_{i\in I} a_i\omega_i \neq 0$ for any non-empty strict subset $I \subseteq [n]$. Prove that $\omega_i^m = \omega_j^m$ for any $i, j \in [n]$ where m is the product of primes at most n.

Exercise 6.5.27. Which quadratic subfields does a cyclotomic field contain?

Exercise 6.5.28†. Prove the Gauss and Lucas formulas: given an odd squarefree integer $n > 1$, there exist polynomials $A_n, B_n, C_n, D_n \in \mathbb{Z}[X]$ such that

$$4\Phi_n = A_n^2 - (-1)^{\frac{n-1}{2}} nB_n^2 = C_n^2 - (-1)^{\frac{n-1}{2}} nXD_n^2.$$

Deduce that, given any non-zero rational number r, there are infinitely many pairs of distinct rational prime (p, q) such that r has the same order modulo p and modulo q.

Exercise 6.5.29 (Inspired by USAMO 2007)**.** Let p be an odd prime and $n \geq 1$ an integer. Prove that the number

$$p^{2p^n} - 1$$

has at least $3n$ prime factors (counted with multiplicity).

Miscellaneous

Exercise 6.5.30†. Let $f \in \mathbb{Q}[X]$ be an irreducible polynomial with exactly one real root of degree at least 2. Prove that the real parts of its non-real roots are all irrational.

[3]The Galois group of a polynomial f over a field F is defined as the Galois group of its splitting field over F, i.e. as $\mathrm{Gal}(F(\alpha_1, \ldots, \alpha_k)/F)$, where $\alpha_1, \ldots, \alpha_k$ are the roots of f.

Exercise 6.5.31†. Let K be a number field of degree n. Prove that there are elements $\alpha_1, \ldots, \alpha_n$ of K such that

$$\mathcal{O}_K \subseteq \alpha_1\mathbb{Z} + \ldots + \alpha_n\mathbb{Z}.$$

By showing that any submodule of a $\mathbb{Z}$-module generated by n elements is also generated by n elements, deduce that $\mathcal{O}_K$ has an *integral basis*, i.e. elements $\beta_1, \ldots, \beta_n$ such that

$$\mathcal{O}_K = \beta_1\mathbb{Z} + \ldots + \beta_n\mathbb{Z}.$$

Exercise 6.5.32†. Let $f \in \mathbb{Q}[X]$ be an irreducible polynomial of prime degree p and denote its roots by $\alpha_0, \ldots, \alpha_{p-1}$. Suppose that

$$\lambda_0\alpha_0 + \ldots + \lambda_{p-1}\alpha_{p-1} \in \mathbb{Q}$$

for some rational λ_i. Prove that $\lambda_0 = \ldots = \lambda_{p-1}$.

Exercise 6.5.33† (TFJM 2019)**.** Let N be an odd integer. Prove that there exist infinitely many rational primes $p \equiv 1 \pmod{N}$ such that $x \mapsto x^{n+1} + x$ is a bijection of $\mathbb{F}_p$, where $n = \frac{p-1}{N}$.

Exercise 6.5.34†. Let $f \in \mathbb{C}(X)$ be a rational function, and suppose f sends rational integers algebraic integers to algebraic integers. Prove that f is a polynomial.

Exercise 6.5.35. Let $\alpha \in \overline{\mathbb{Z}}$ be an algebraic integer with minimal polynomial f. Prove that a rational prime p not dividing the discriminant Δ of f stays prime in $\mathcal{O}_{\mathbb{Q}(\alpha)}$ if and only if f stays irreducible in $\mathbb{F}_p[X]$.

Exercise 6.5.36. Suppose $f \in \mathbb{R}[X]$ is positive on $\mathbb{R}$. Prove that there exist polynomials $g, h \in \mathbb{R}[X]$ such that $f = g(X)^2 + h(X)^2$.

Exercise 6.5.37. Suppose $f \in \mathbb{R}[X]$ is positive on $\mathbb{R}_{>0}$. Prove that there exist polynomials $g, h \in \mathbb{R}[X]$ such that $f = g(X)^2 + Xh(X)^2$.

Exercise 6.5.38 (Inspired by ISL 2020)**.** Let p be a prime and $f \in \mathbb{Z}[X]$ a polynomial. Alice and Bob play a game: Bob chooses two initial element $\alpha, \beta \in \mathbb{F}_p$ and Alice iteratively replace α by $f(\alpha)$ or α' such that $\alpha = f(\alpha')$. She wins if she can reach β, otherwise Bob wins. Prove that there exists infinitely many primes p such that Bob is able to win.

Exercise 6.5.39. Prove that $\mathbb{F}_p(U,T)/\mathbb{F}_p(U^p, T^p)$ has no primitive element.

Chapter 7

Units in Quadratic Fields and Pell's Equation

Prerequisites for this chapter: Chapter 2 for the whole chapter and Chapter 6 for Section 7.4.

7.1 Fundamental Unit

Recall that a unit $\alpha \in \mathcal{O}_K$ is an invertible element (in $\mathcal{O}_K$), i.e. an element of norm ± 1. By abuse of terminology, we shall also call α a unit of K, even though all non-zero elements are units in K since it's a field.

Exercise 7.1.1*. Prove that α is invertible if and only if its norm is ± 1.

We are interested in characterising units in quadratic fields. Notice that $a + b\sqrt{d} \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a unit if and only if $\pm 1 = N(a + b\sqrt{d}) = a^2 - bd^2$ so units in quadratic fields are deeply linked with the so-called *Pell equation*.

Note also that units are closed under multiplications since the norm is multiplicative. In particular, if K has a unit which is not a root of unity, it has infinitely many units.

We shall prove that there always exists such a unit, but first we turn ourselves over to the *complex* case, i.e. $\mathbb{Q}(\sqrt{d})$ for $d < 0$ (such a field is called a *complex quadratic field*), for which the situation is a lot simpler. Indeed, the norm of $a + b\sqrt{d}$ is a $a - db^2 \geq a^2 + b^2$ since $d < 0$. We thus get the following characterisation of units in complex quadratic fields.

Proposition 7.1.1

Let $d < 0$ be a squarefree rational integer. The units of $\mathbb{Q}(\sqrt{d})$ are $\{1, -1, i, -i\}$ for $d = -1$, $\{1, -1, j, j^2\}$ for $d = 3$, and $\{1, -1\}$ for other d.

Exercise 7.1.2*. Prove Proposition 7.1.1.

In the real case, however, the situation is completely different ($\mathbb{Q}(\sqrt{d})$ for $d > 0$ is called a *real quadratic field*). Indeed, there always exists infinitely many units. Before we prove this, let us talk about *fundamental units*. Notice that since $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R}$, the only roots of unity it has are ± 1.

Definition 7.1.1 (Fundamental Unit)

Let K be a real quadratic field. A unit θ of K is said to be a *fundamental unit* if it generates all other units of K, i.e. any unit has the form $\pm\theta^n$ for some $n \in \mathbb{Z}$.

We now show that, if there is a non-trivial unit, there always exists a fundamental unit greater than 1. We will refer to this unit when we say "**the** fundamental unit".

Proposition 7.1.2

Any real quadratic field has a fundamental unit θ (unique with the additional condition $\theta > 1$).

Proof of Proposition 7.1.2 assuming there is a non-trivial unit

The uniqueness is obvious: if $\alpha = \pm\beta^u$ and $\beta = \pm\alpha^v$, then $\alpha = \pm(\pm\alpha^v)^u$ so either $u = v = \pm 1$ and $\alpha = \pm\beta^{\pm 1}$ as wanted, or α is a root of unity (which means the only units are ± 1 but we assumed there was a non-trivial unit).

Notice that, if K has a unit $\alpha = a + b\sqrt{d} \neq \pm 1$, then it has a unit $\beta = |a| + |b|\sqrt{d} > 1$. Let θ be the smallest unit which is greater than 1; there exists one since there are only finitely many units in any interval $[a, b]$ for positive a, b.

Indeed, if $\theta \in [a, b]$ then $\overline{\theta} = 1/\theta \in [1/b, 1/a]$ so the minimal polynomial of θ has bounded coefficients which shows that there are a finite number of such θ.

Now, we prove that all units are generate by θ. Suppose for the sake of a contradiction that $\varepsilon > 1$ is the smallest unit which is not a power of θ (we can do that for the same reasons as before). Since θ is the minimal unit greater than 1, we must have $\varepsilon > 1$; but then $1 < \varepsilon/\theta < \varepsilon$ is a smaller unit which is not a power of θ and that is a contradiction.

■

It remains to prove that the units of a real quadratic field are not all trivial. We follow the proof of Lagrange. First, we need a lemma.

Lemma 7.1.1 (Dirichlet's Approximation Theorem)

Let $\alpha \in \mathbb{R}$ be a real number. For any rational integer $N > 0$, there are rational integers p, q such that $0 < q \leq N$ and

$$|q\alpha - p| < \frac{1}{N}.$$

In particular, there are infinitely many pairs of rational integers (p, q) such that $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$. This will prove to be very useful for finding units.

Proof

Consider the fractional parts of the numbers $0, \alpha, 2\alpha, \ldots, N\alpha$. They all lie in the intervals

$$\left[0, \frac{1}{N}\right], \left[\frac{1}{N}, \frac{2}{N}\right], \ldots, \left[\frac{N-1}{N}, 1\right]$$

so, by the pigeonhole principle, two of them must lie in the same interval. Thus, their difference has absolute value less than $\frac{1}{N}$, which is exactly what we were looking for:

$$|\alpha q - p| = |(\alpha q_1 - p_1) - (\alpha q_2 - p_2)| < \frac{1}{N}$$

where $q = |q_1 - q_2|$, $p = \pm(p_1 - p_2)$ and $p_1 = \lfloor \alpha q_1 \rfloor$, $p_2 = \lfloor \alpha q_2 \rfloor$.

■

Finally, we prove the existence of a non-trivial unit.

Proof of the existence of a non-trivial unit

Take $\alpha - \sqrt{d}$ in the Dirichlet approximation theorem. Suppose $|a - b\sqrt{d}| < \frac{1}{b}$. Then,

$$|a^2 - db^2| < \frac{a + b\sqrt{d}}{b} \leq \frac{2b\sqrt{d} + 1}{b}$$

as $a \leq b\sqrt{d} + \frac{1}{b}$.

In particular, some value M must be reached infinitely many times by $a^2 - db^2$. Moreover, again by the pigeonhole principle, some pair $(a, b) \pmod M$ must be repeated infinitely many times. If $(a, b) \equiv (a', b') \pmod M$ and $a^2 - db^2 = M = a'^2 - db'^2$ then

$$\frac{a + b\sqrt{d}}{a' + b'\sqrt{d}} = \frac{(a + b\sqrt{d})(a' - b'\sqrt{d})}{M}$$

is an algebraic integer as $(a+b\sqrt{d})(a'-b'\sqrt{d}) \equiv (a+b\sqrt{d})(a-b\sqrt{d}) \equiv 0 \pmod M$ and has norm 1. We have found a non-trivial unit.

■

Here is a table of the fundamental units for small d.

- $\theta_2 = 1 + \sqrt{2}$ (norm -1).
- $\theta_3 = 2 + \sqrt{3}$ (norm 1).
- $\theta_5 = \frac{1+\sqrt{5}}{2}$ (norm -1).
- $\theta_6 = 5 + 2\sqrt{6}$ (norm 1).
- $\theta_7 = 8 + 3\sqrt{7}$ (norm 1).
- $\theta_{10} = 3 + \sqrt{10}$ (norm -1).

7.2 Pell-Type Equations

Notice that the fundamental unit may have norm 1 or norm -1. To have norm -1, a necessary condition is that -1 is a quadratic residue modulo d. However, as Exercise 7.5.13† shows, it is not sufficient and one cannot really predict which sign the norm of the fundamental unit will have. That said, this condition is sufficient when d is a prime number.

Proposition 7.2.1

Let p be a rational prime. The fundamental unit of $\mathbb{Q}(\sqrt{p})$ has norm -1 if and only if $\left(\frac{-1}{p}\right) = 1$, i.e. $p \equiv 1 \pmod 4$ or $p = 2$.

Proof

If the fundamental unit has norm -1, then $\left(\frac{-1}{p}\right) = 1$ so it suffices to prove that the converse also holds. When $p = 2$, the fundamental unit indeed has norm -1. Now suppose $p \equiv 1 \pmod 4$, and let $a + b\sqrt{p} > 1$ be the minimal unit of $\mathbb{Q}(\sqrt{p})$ with $a, b \in \mathbb{Z}$ (so not necessarily the fundamental

unit). We have $a^2 - pb^2 = 1$ so, modulo 4 we get that a is even (otherwise $a^2 - pb^2 \equiv -1$). Since

$$(a-1)(a+1) = pb^2,$$

we must have $a \pm 1 = 2x^2$ and $a \mp 1 = 2py^2$ for some $x, y \in \mathbb{Z}$. If $a + 1 = 2x^2$, we get

$$2x^2 - 2py^2 = (a+1) - (a-1) = 2$$

which is impossible as $a + b\sqrt{d}$ was already the smallest unit with norm 1. Thus,

$$2x^2 - 2py^2 = (a-1) - (a+1) = -2$$

as wanted.

■

Note that when we proved the existence of a unit, we did not use the fact that d was squarefree anywhere. Thus, we in fact get that the Pell equation $x^2 - dy^2 = 1$ has integral solutions for any positive squarefree d, and that all solutions are generated by the minimal one. However, we will also prove this from the existence of a fundamental unit.

Write $d = uv^2$ where u is the squarefree part of d, and let α be the fundamental unit of $\mathbb{Q}(\sqrt{u})$. Then, the (positive) solutions of $x^2 - uy^2 = 1$ have the form

$$x + y\sqrt{u} = \alpha^n.$$

Thus, we get

$$y = \frac{\alpha^n - \overline{\alpha}^n}{2\sqrt{u}}.$$

We want to know when y is divisible by v, i.e. when

$$2v \mid \alpha^n - \overline{\alpha}^n = \alpha^n - \alpha^{-n}$$

which is equivalent to $2v\sqrt{u} \mid \alpha^{2n} - 1$ as α is a unit.

In fact, we can find when any non-zero $\beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ divides $\alpha^{2n} - 1$ exactly like we would in $\mathbb{Z}$. Indeed, $\mathcal{O}_{\mathbb{Q}(\sqrt{u})}$ modulo β has a finite number of elements (in fact $|N(\beta)|$ by **??**) so α^{2n} cycles modulo k:

$$\alpha^{2i} \equiv \alpha^{2j} \iff k \mid \alpha^{2(i-j)} - 1$$

(α is a unit so we can divide by it). Then, we can define the order of α^2 modulo β to be the smallest m such that $\alpha^{2m} \equiv 1$ to get that $\alpha^{2n} \equiv 1 \iff m \mid n$ which means that the solutions to $k \mid \alpha^{2n}$ are generated by α^m, the minimal solution, as wanted.

Exercise 7.2.1*. Prove that $\mathcal{O}_{\mathbb{Q}(\sqrt{u})}/\beta\mathcal{O}_{\mathbb{Q}(\sqrt{u})}$ is finite if $\beta \neq 0$.

Here is how our previous discussion translates. Actually, our statement is a bit more general because we also allow rings of the form $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ when $d \equiv 1 \pmod 4$, but these still have a non-trivial unit since we have shown that $\mathbb{Z}[\sqrt{d}]$ do (and the same proof as Proposition 7.1.2 shows that the minimal unit greater than 1 is fundamental).

Definition 7.2.1 (Fundamental Unit)

Let δ be a quadratic integer. A unit θ of $\mathbb{Z}[\delta]$ is said to be a *fundamental unit* if it generates all other units of K, i.e. any unit has the form $\pm\theta^n$ for some $n \in \mathbb{Z}$.

Proposition 7.2.2

For any quadratic integer δ, $\mathbb{Z}[\delta]$ always has a unique fundamental unit greater than 1.

Note that this differs from our previous definition (although the proof is the same as before) because $\mathbb{Z}[\delta]$ may not be $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. We will also call (x, y) the fundamental solution of $x^2 - dy^2 = 1$ if $x + y\sqrt{d}$ is the fundamental unit of $\mathbb{Z}[\delta]$, where $\mathbb{Z}[\delta] = \mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ (d is not necessarily squarefree anymore).

We now discuss equations of the form $x^2 - dy^2 = k$ for some fixed k. As we have seen earlier with $k = -1$, it is very hard to determine when this equation has a solution, so we will instead show that all solutions are generated by the fundamental solution of $x^2 - dy^2 = 1$ and a finite number of pairs (x_i, y_i) such that $x_i^2 - dy_i^2 = k$.

Proposition 7.2.3

Let $k \in \mathbb{Z}$ be a non-zero rational integer which is not a perfect square and θ the fundamental unit of $\mathbb{Z}[\delta]$. There exists elements $\alpha_1, \dots \alpha_n \in \mathbb{Z}[\delta]$ of norm k such that the elements of $\mathbb{Z}[\delta]$ of norm k are exactly those of the form $\pm\theta^i\alpha_j$.

Proof

The proof is the same as before. For each $(a, b) \in (\mathbb{Z}/2k\mathbb{Z})^2$, pick an element $\alpha_{(a,b)} = \frac{a'+b'\sqrt{d}}{2} \in \mathbb{Z}[\delta]$ with $(a', b') \equiv (a, b) \pmod{k}$ of norm k if there exists one. Then, if $\alpha = \frac{a+b\sqrt{d}}{2}$ has norm k,

$$\frac{\alpha}{\alpha_{(a,b)} \pmod{k}}$$

is a unit of $\mathbb{Z}[\delta]$ so has the form θ^i for some i.

■

Remark 7.2.1

Note that we can solve this equation in finite time, since it suffices to find elements of norm k between 1 and the fundamental unit θ, as any solution greater than θ reduces to one smaller after a division by a suitable power of θ.

To conclude this section, we consider the equation $ax^2 - by^2 = k$. Again, we will not determine when this has non-trivial solutions since the case $b = -1$ reduces to $y^2 - ax^2 = -1$. We shall get a characterisation of the solutions to these equations, albeit non-explicit and slightly cumbersome. Nevertheless, for any given values of a, b, k one can compute all solutions explicitly with this.

Proposition 7.2.4

Let a and b be non-zero rational numbers of same sign such that ab is not a square and let θ be the fundamental unit of $\mathbb{Z}[\sqrt{ab}]$. Further, let $k \neq 0$ be a rational integer. Then, there exists elements $\alpha_1, \dots \alpha_n \in \mathbb{Z}[\sqrt{ab}]$ of norm k and rational integers $u_1, \dots, u_n, m_1, \dots, m_n$ such that the integral solutions of $ax^2 - by^2 = k$ are exactly the x, y for which

$$x + y\sqrt{ab} \in \{\pm\theta^{u_i+jn_i}\alpha_i \mid i \in [n], j \in \mathbb{Z}\}.$$

Proof

Solving $ax^2 - by^2 = k$ is equivalent to solving $(ax)^2 - aby^2 = ak$. We already know that the solutions of $x^2 - aby^2 = ak$ have the form $x + y\sqrt{d} = \pm\alpha_i\theta^n$. We wish to know when a divides

$$x = \frac{\alpha_i\theta^n + \overline{\alpha_i}\overline{\theta}^n}{2},$$

i.e. when $2a$ divides $\alpha_i\theta^{2n} + \overline{\alpha_i}$. Let $m_i > 0$ be the smallest integer such that $\alpha_i(\theta^{2m_i} - 1) \equiv 0$.

Either there is no solution to $\alpha_i\theta^{2n} \equiv -\overline{\alpha_i}$ or u_i is a solution and all solutions are given by $n \equiv u_i \pmod{m_i}$. Indeed, $\alpha_i\theta^{2n} \equiv -\overline{\alpha_i}$ is then equivalent to

$$\alpha_i\theta^{2n} \equiv \alpha_i\theta^{2u_i} \iff \alpha(\theta^{2(n-u_i)-1}) \equiv 0$$

since θ is a unit. Thus, it remains to prove that $\alpha_i\theta^{2m} \equiv \alpha_i$ if and only if $m_i \mid m$.

We proceed like we would when $\alpha_i = 1$. Suppose, for the sake of a contradiction, that $\alpha_i\theta^{2m} \equiv \alpha$ and $m_i \nmid m$. Write the Euclidean division $m = qm_i + r$ with $0 < r < m_i$. Then,

$$\alpha_i \equiv \alpha_i\theta^{2m} = \alpha_i\theta^{2qm_i}\theta^{2r} \equiv \alpha_i\theta^{2r}$$

which is a contradiction since m_i was assumed to be minimal.

■

Remark 7.2.2

It is no coincidence that proving that

$$\alpha_i\theta^{2m} \equiv \alpha_i \pmod{2a}$$

iff $m_i \mid m$ was so similar to proving that $\theta^{2m} \equiv 1$ iff the order of θ^2 divides m. This is because it is in fact the same result, but modulo $2a/\gcd(2a, \alpha_i)$. Since we have not defined the gcd in non-Bézout domains, we could not use this approach (the gcd is usually not a number but an ideal!).

7.3 Størmer's Theorem

In this section, we focus on a very nice application of Pell equations, regarding consecutive S-units.

Definition 7.3.1 (S-Units)

Let S be a finite set of rational primes. A rational number $r \in \mathbb{Q}$ is said to be a *S-unit* if the prime factors of its numerator and denominator are in S. Given a non-zero rational integer $s \in \mathbb{Z}$, We also say r is a *s-unit* if all prime factors of the numerator and denominator of r are prime factors of s.

Theorem 7.3.1 (Størmer's Theorem)

For any set of rational primes S of cardinality n, the equation $u - v = 1$ has at most 3^n solutions in positive integral S-units.

Here is how we will approach this theorem: if v and $u = v + 1$ are S-units, then one of them is even so $2 \in S$. Thus, $4v(v + 1) = (2v + 1)^2 - 1$ is also an S-unit. Let $x = 2v + 1$. Write

$$x^2 - 1 = \prod_{p \in S} p^{k_p},$$

and for each $k_p \neq 0$, choose $d_p \in \{1, 2\}$ such that $d_p \equiv k_p \pmod 2$ (otherwise set $d_p = 0$). Then, $\prod_{p \in S} p^{k_p - d_p}$ is a perfect square, say y^2. Letting $d = \prod_{p \in S} p^{d_p}$ we get the Pell equation

$$x^2 - dy^2 = 1.$$

Also – and this is the key point – note that y is a d-unit by construction. We shall prove that the only possible solution to the Pell equation $x^2 - dy^2 = 1$ where y is a d-unit is the fundamental solution. Thus, for each such Pell equation there is at most one corresponding pair of consecutive S-units. Since $d_p \in \{0, 1, 2\}$ for each p, there are 3^n equations to consider which yields the result.

Hence, we just need to prove the following proposition.

Proposition 7.3.1

For any positive rational integer d which is not a perfect square, the only possible positive solution to the Pell equation $x^2 - dy^2 = 1$ where y is a d-unit is the fundamental solution.

Proof

Let $x + y\sqrt{d}$ be the fundamental unit of $\mathbb{Z}[\sqrt{d}]$. Since we are interested in positive solutions of the Pell equation, by Proposition 7.2.2, we want to show that if

$$y_n = \frac{(x + y\sqrt{d})^n - (x - y\sqrt{d})^n}{2\sqrt{d}}$$

is a d-unit, then $n = 1$. Suppose there is a solution where $n \neq 1$. Since $y_m \mid y_n$ when $m \mid n$, we may assume $n = p$ is prime.

We have

$$y_p = \binom{p}{1} x^{p-1} + \binom{p}{3} x^{p-3} y^2 d + \binom{p}{5} x^{p-5} y^4 d^2 + \dots \qquad (*)$$

Let q be a prime factor of y_p; by assumption $q \mid d$. Every term of this sum except the first one is divisible by d, thus

$$q \mid \binom{p}{1} x^{p-1} = p x^{p-1}.$$

Since $x^2 - dy^2 = 1$, x is coprime with d so $q \mid p$ which means $q = p$. Thus, y_p is a power of p and in particular divisible by p^2 unless $p = 2$.

However, as $p \mid \binom{p}{k}$ for $0 < k < p$, if $p > 3$, every term of $(*)$ is divisble by p^2 except the first one which is px^{p-1}. This is a contradiction.

It remains to settle the cases $p = 2$ and $p = 3$. The first one is trivial: we have $y_2 = 2x$ so $x = 1$ as it's coprime with d which is impossible since $x + y\sqrt{d}$ was a non-trivial unit.

Finally, in the case $p = 3$ we get $y_3 = 3x^2 + dy^2$, and since $x^2 - dy^2 = 1$ this means

$$y_3 = 3x^2 + (x^2 - 1) = (2x - 1)(2x + 1).$$

This is a product of two numbers which differ by 2, thus it can only be a power of 3 if $x = 1$ since the only powers of 3 which differ by 2 are 1 and 3. This is again impossible as $x + y\sqrt{d}$ is a non-trivial unit.

■

Exercise 7.3.1*. Prove that $y_m \mid y_n$ iff $m \mid n$.

7.4 Units in Complex Cubic Fields, Thue's Equation and Kobayashi's Theorem

In this section, we will prove that, for any finite set of rational primes S and any fixed integer $k \neq 0$, the equation $u - v = k$ has finitely many solutions in integral S-units. We will, however, not find an explicit bound like we did in the last section for $k = 1$. In fact, our method **can not** give bounds; and it does not let us compute *effectively* all solutions for a fixed k and S.

Exercise 7.4.1. Why does looking at the $(2^k)^2$ Pell-type equations $ax^2 - by^2 = k$ for squarefree integral S-units a, b not prove that $u - v = k$ has finitely many integral S-units solutions?

Thus, instead of considering Pell-type equations $ax^2 - by^2 = k$ that usually have infinitely many solutions, we shall consider equations of the form $ax^3 - by^3 = k$. Indeed, if $u = \prod_{p\in S} p^{r_p}$ and $v = \prod_{p\in S} p^{s_p}$ then, by choosing $a_p, b_p \in \{1, 2, 3\}$ such that $a_p \equiv r_p \pmod 3$ and $b_p \equiv s_p \pmod 3$ and defining $a = \prod_{p\in S} p^{a_p}$ and $b = \prod_{p\in S} p^{b_p}$, we get that $(\sqrt[3]{u/a}, \sqrt[3]{v/b})$ is a solution of one of the 3^k Thue equations

$$ax^3 - by^3 = k.$$

Indeed, it is a theorem of Thue that such an equation has only finitely many solutions for $k \neq 0$. This is what we'll prove in this section.

The theorem that $u-v = k$ has finitely many integral S-units solutions is also known as Kobayashi's theorem. It is usually written as such:

Theorem 7.4.1 (Kobayashi's Theorem)

Let M be a set of rational integers with finitely many prime divisors, meaning that there are finitely many rational primes which divide at least one element of M. Then, the translate $k + M$ has infinitely many prime divisors for any rational integer $k \neq 0$.

Note that this is indeed equivalent to our result on the finiteness of integral S-units equations: M has finitely many prime divisors if and only if all its elements are S-units for some finite S, and the same holds for $k + M$. So if they're both sets of S-units for some finite S, we can assume it's the same S for both of them but then the equation $u - v = k$ has infinitely many solutions in integral S-units.

Thus, we need to prove the following special case of Thue's theorem.

Theorem 7.4.2 (Thue)

For any non-zero rational integers a, b and k, the equation $ax^3 + by^3 = k$ has finitely many solutions in rational integers.

The equation $ax^2 - bx^2 = k$ was linked to units in $\mathbb{Q}(\sqrt{b/a})$, thus, for $ax^3 + by^3$ we will consider units in $\mathbb{Q}(\sqrt[3]{b/a})$. When a/b is perfect cube this problem is more or less trivial so we can assume that it isn't the case, i.e. that $\mathbb{Q}(\sqrt[3]{b/a})$ is a field of degree 3.

Exercise 7.4.2*. Prove Theorem 7.4.2 in the case where a/b is a rational cube.

As before, we first consider the case where $a = 1$ and $k = 1$ since it corresponds to units of $\mathbb{Q}(\sqrt[3]{b})$. Indeed, if $x^3 + by^3 = 1$, then $N(x + y\sqrt[3]{b}) = 1$. Why should we expect $\mathbb{Q}(\sqrt[3]{b})$ to have finitely many such units when there are infinitely many of them for $K = \mathbb{Q}(\sqrt{d})$? It's because this unit does not have a term in $\sqrt[3]{b^2}$, so for instance units of that form are absolutely not closed under multiplication, contrary to the quadratic case.

We shall find a characterisation of the units of $\mathbb{Q}(\sqrt[3]{b})$. This relies on the fact that $\mathbb{Q}(\sqrt[3]{b})$ is a *complex cubic field*, not because it's not real but because some of its conjugates fields $\mathbb{Q}(j\sqrt[3]{b})$ for some primitive third root of unity j aren't.

We also say a number field K is *totally real* if all its conjugate fields are real. Also, we say an embedding σ is *real* if σK is real, and *complex* otherwise. Complex embeddings come into pair $\sigma, \overline{\sigma}$: this will be quite useful for us as we only need to deduce information on an element of $\mathbb{Q}(\sqrt[3]{b})$ and one its conjugate to have information on all its conjugates.

We define fundamental units almost as before, but this time we don't require θ to be non-trivial if there are no non-trivial units (i.e. we allow $\theta = 1$). There always exists a non-trivial unit, but since it's non-trivial to show and we do not need it (it's better for us if there are less units) we do not do it. Again, we say "unit of K" to mean "unit of $\mathcal{O}_K$".

Definition 7.4.1 (Fundamental Unit For Complex Cubic Fields)

Let $K \subseteq \mathbb{R}$ be a complex cubic field. A unit $\theta \geq 1$ of K is said to be a *fundamental* unit if it generates all others: any unit can be written as $\pm\theta^n$.

Proposition 7.4.1

Let $K \subseteq \mathbb{R}$ be a complex cubic field. If K has a non-trivial unit, then K has a (unique) fundamental unit.

Proof

Again, uniqueness is obvious from existence. Suppose K has a unit greater than 1, otherwise all its units are ± 1 so we can take $\theta = 1$ (this is in fact impossible and even if it were possible we wouldn't call it a fundamental unit because the units are generated by **no** element).

We imitate the proof of Proposition 7.1.2. The key step is the existence of a **minimal** unit $\theta > 1$. Such a unit exists, because if $\varepsilon \neq \pm 1$ is a unit then $|\varepsilon|^{\pm 1}$ is a unit greater than 1 for some choice of ± 1.

Now, let's prove that a minimal one exists. As before, we prove that there are finitely many units in any interval $[a, b]$ for positive a, b. Suppose $\varepsilon \in [a, b]$ is a unit. Let $\sigma, \overline{\sigma}$ be the complex embeddings of K. Then,

$$1 = |\varepsilon\sigma(\varepsilon)\overline{\sigma}(\varepsilon)| = \varepsilon|\sigma\varepsilon|^2.$$

Thus, the absolute values of the conjugates of ε are all bounded, which means that the minimal polynomial of ε has bounded coefficients: there exists finitely many such ε.

Finally, we again proceed as in the quadratic case. Let θ be the minimal unit greater than 1 Suppose $\varepsilon > 1$ is the minimal unit which is not a power of θ. Then, $\varepsilon > \theta$ by minimality of θ, which means $1 < \varepsilon/\theta < \varepsilon$, contradicting the minimality of ε.

■

Now that we have characterised units of $\mathbb{Q}(\sqrt[3]{b/a})$, we characterise elements of $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{b/a})}$ of norm k for a fixed k. This is related to our equation $ax^3 + by^3 = k$: indeed, if x, y is an integral solution of this equation, then $N(ax + y\sqrt[3]{a^2 b}) = a^2 k$.

Proposition 7.4.2

Let $k \in \mathbb{Z}$ be a non-zero rational integer and θ the fundamental unit of $\mathbb{Q}(\sqrt[3]{d})$. There exists elements $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}[\sqrt[3]{d}]$ of norm k such that the elements of $\mathcal{O}_K$ of norm k all have the form $\pm\theta^i\alpha_j$.

Proof

The proof is again the same as before. For each $(a,b,c) \in (\mathbb{Z}/k\mathbb{Z})^3$, pick an element of norm k

$$\alpha_{(a,b,c)} = a' + b'\sqrt[3]{d} + c'\sqrt[3]{d^2}$$

with $(a',b',c') \equiv (a,b,c) \pmod{k}$ if there exists one. Then, if $\alpha = a + b\sqrt[3]{d} + c\sqrt[3]{d^2}$ has norm k,

$$\frac{\alpha}{\alpha_{(a,b,c)} \pmod{k}}$$

is a unit of $\mathcal{O}_K$ so has the form θ^i.

■

Remark 7.4.1

We did not consider the equation $N(\alpha) = k$ in $\mathcal{O}_K$ because that would require to find the structure of $\mathcal{O}_K$ which is slightly cumbersome. This is left as Exercise 7.5.27 and we let the reader adapt the proof for $\mathcal{O}_K$ (the conclusion is that the elements of norm k are exactly those of the form $\pm\theta_j^{\alpha}$.)

Finally, we prove Theorem 7.4.2.

Proof of Theorem 7.4.2

Let $K = \mathbb{Q}(\sqrt[3]{b/a}) = \mathbb{Q}(\sqrt[3]{d})$ where $d = a^2b$, and denote its fundamental unit by θ.

From the previous consideration and Proposition 7.4.2, it suffices to show that, for any non-zero element $\alpha \in \mathcal{O}_K$, there are finitely many rational integers n such that $\alpha\theta^n$ has the form $x + y\sqrt[3]{d}$. If $\theta = \pm 1$ is trivial, the claim is obvious, thus suppose $\theta > 1$ is non-trivial.

Let j be a primitive third root of unity and σ be the complex embedding of K sending $\sqrt[3]{d}$ to $j\sqrt[3]{d}$. Since $j^2 + j + 1 = 0$, $\alpha\theta^n$ has the form $x + y\sqrt[3]{d}$ if and only if

$$\alpha\theta^n + j\sigma(\alpha)\sigma(\theta)^n + j^2\overline{\sigma}(\alpha)\overline{\sigma}(\theta)^n = 0.$$

Indeed, if $\beta = r + s\sqrt[3]{d} + t\sqrt[3]{d^2}$, we have

$$3t\sqrt[3]{d^2} = (r + s\sqrt[3]{d} + t\sqrt[3]{d^2}) + (jr + j^2 s\sqrt[3]{d} + t\sqrt[3]{d^2}) + (j^2 r + js\sqrt[3]{d} + t\sqrt[3]{d^2}) = \beta + \sigma\beta + \overline{\sigma}\beta.$$

Thus, we wish to show that the linear recurrence of algebraic numbers

$$\alpha\theta^n + j\sigma(\alpha)\sigma(\theta)^n + j^2\overline{\sigma}(\alpha)\overline{\sigma}(\theta)^n$$

has finitely many zeros. By Corollary 8.5.2 of the Skolem-Mahler-Lech theorem 8.5.1 which will be proven in Chapter 8, there exists two embeddings σ_1 and σ_2 such that

$$\frac{\sigma_1(\theta)}{\sigma_2(\theta)}$$

is a root of unity. By composing with another embedding, we may assume $\sigma_1 = \mathrm{id}$, and by symmetry between j and j^2 we may assume $\sigma_2 = \sigma$.

By an argument similar to Problem 6.3.1, we can show that the only roots of unity in $\mathbb{Q}(\sqrt[3]{d}, j)$ are ± 1, $\pm j$ and $\pm j^2$. Hence, we must have $\theta/\sigma(\theta) \in \{\pm 1, \pm j, \pm j^2\}$. Write $\theta = x + y\sqrt[3]{d} + z\sqrt[3]{d^2}$. Suppose $\theta/\sigma(\theta) = \pm 1$. We get

$$x + y\sqrt[3]{d} + z\sqrt[3]{d^2} = \pm(x + yj\sqrt[3]{d} + zj^2\sqrt[3]{d^2})$$

which means $y = z = 0$ as j has degree two over $\mathbb{Q}(\sqrt[3]{d})$ (since it's not in $\mathbb{Q}(\sqrt[3]{d}) \subseteq \mathbb{R}$) so $1, \sqrt[3]{d}, \sqrt[3]{d^2}, j, j\sqrt[3]{d}, j^2\sqrt[3]{d^2}$ are $\mathbb{Q}$-linearly independent. This is impossible since θ is non-trivial by assumption. The other cases yield similar contradictions, which finishes the proof.

■

Exercise 7.4.3*. Prove that the only roots of unity of $\mathbb{Q}(\sqrt[3]{d}, j)$ are ± 1, $\pm j$ and $\pm j^2$.

Exercise 7.4.4*. Prove that $\theta/\sigma(\theta) \in \{\pm j, \pm j^2\}$ is also impossible.

Remark 7.4.2

In fact, if K is a number field of degree n with real embeddings $\tau_1, \ldots, \tau_r$ and complex embeddings $\sigma_1, \overline{\sigma}_1, \ldots, \sigma_s, \overline{\sigma}_s$, the Dirichlet unit theorem states that the units of K have the form

$$\zeta \varepsilon_1^{n_1} \cdot \ldots \cdot \varepsilon_{r+s-1}^{n_{r+s-1}}$$

where ζ is a root of unity and $\varepsilon_1, \ldots, \varepsilon_{r+s-1} \in K$ are multiplicatively independent units. The case we treated corresponded to $(r, s) = (2, 0)$ and $(r, s) = (1, 1)$ (although we didn't prove they were multiplicatively independent for complex cubic fields, i.e. that the units are not all roots of unity).

Remark 7.4.3

Thue in fact proved more generally that if $f \in \mathbb{Z}[X, Y]$ is an irreducible homogeneous polynomial of degree $n \geq 3$, i.e. f is homogeneous and $f(X, 1)$ is irreducible in $\mathbb{Z}[X]$, the equation

$$f(x, y) = k$$

has a finite number of integral solutions $x, y \in \mathbb{Z}$ for any fixed $k \in \mathbb{Z}$. In fact, this is deeply linked with the *irrationality measure* of algebraic numbers (it can also be proven with p-adic methods like the Skolem-Mahler-Lech theorem (see [6]) but Thue proved it that way).

The equality $f(x, y) = k$ yields $f(x/y, 1) = k/y^n$ which means that x/y is very close to a root of f. In fact, it is equivalent to the finiteness of pairs of rational integers (p, q) with $q \neq 0$ such that

$$\left| \alpha - \frac{p}{q} \right| < \frac{C}{q^n}$$

for any $C > 0$. Thue proved that there were finitely many pairs (p, q) such that

$$\left(\alpha - \frac{p}{q} \right) < \frac{1}{q^{n/2+\varepsilon}}$$

for any $\varepsilon > 0$, thus establishing his theorem. See Silverman-Tate, chapter 5, section 3 [26].

We say a real number $\alpha \in \mathbb{R}$ has irrationality measure μ if μ is the largest real number such that, for any $\varepsilon > 0$, there are finitely many pairs of rational integers (p, q) with $q \neq 0$ such that

$$\left(\alpha - \frac{p}{q} \right) < \frac{1}{q^{\mu+\varepsilon}}.$$

Dirichlet's approximation theorem Lemma 7.1.1 shows that any real number has irrationality measure at least 2. Conversely, the very deep Thue-Siegel-Roth theorem states that any real algebraic number has irrationality measure exactly 2 (Siegel proved you could take $\mu = 2\sqrt{n}$ and Roth $\mu = 2$).

Remark 7.4.4

In fact, the S-unit equation $u - v = 1$ also has a finite number of **rational** solutions. This is considerably harder than Kobayashi's theorem.

7.5 Exercises

Diophantine Equations

Exercise 7.5.1† (ISL 1990)**.** Find all positive rational integers n such that $\frac{1^2+\ldots+n^2}{n}$ is a perfect square.

Exercise 7.5.2† (BMO 1 2006)**.** Let n be a rational integer. Prove that, if $2+2\sqrt{1+12n^2}$ is a rational integer, then it is a perfect square.

Exercise 7.5.3. Find all rational integers n such that $2n+1$ and $3n+1$ are both perfect squares.

Exercise 7.5.4† (RMM 2011)**.** Let $\Omega(\cdot)$ denote the number of prime factors counted with multiplicity of a rational integer, and define $\lambda(\cdot) = (-1)^{\Omega(\cdot)}$. Prove that there are infinitely many rational integers n such that $\lambda(n) = \lambda(n+1) = 1$ and infinitely many rational integers n such that $\lambda(n) = \lambda(n+1) = -1$.

Exercise 7.5.5†**.** Let k be a rational integer. Prove that there are infinitely positive integers n such that $n^2 + k \mid n!$.

Exercise 7.5.6 (BAMO 2011)**.** Does there exist a row of the Pascal triangle with four distinct numbers a, b, c, d satisfying $a = 2b$ and $c = 2d$?

Exercise 7.5.7 (Bulgaria National Olympiad 1999)**.** Prove that there are infinitely many rational integers x, y, z, t such that $x^3 + y^3 + z^3 + t^3 = 1999$.

Exercise 7.5.8. Let n be a positive rational integer which is not a perfect square. Prove that there are infinitely many rational integers a, b, c, d such that

$$(a^2 + nd^2)(b^2 + nd^2)(c^2 + nd^2)$$

is a perfect square.

Exercise 7.5.9 (ISL 1999)**.** Find two infinite increasing sequences of rational integers $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ such that $a_n(a_n+1) \mid b_n^2 + 1$ for any n.

Exercise 7.5.10 (EGMO 2016)**.** (EGMO 2016). Let S be the set of all positive integers n such that n^4 has a divisor in the range $[n^2+1, n^2+2n]$. Prove that there are infinitely many elements of S congruent to $0, 1, 2, 5, 6$ modulo 7 and no element congruent to 3 or 4.

Pell-Type Equations

Exercise 7.5.11†**.** Let d be a rational integer. Solve the equation $x^2 - dy^2 = 1$ over $\mathbb{Q}$.

Exercise 7.5.12. Let $p \equiv -1 \pmod 4$ be a rational prime. Prove that the equation $x^2 - py^2 = 2\left(\frac{2}{p}\right)$ has a non-trivial solution over $\mathbb{Z}$.

Exercise 7.5.13†**.** Prove that the equation $x^2 - 34y^2 = -1$ has no non-trivial solution in $\mathbb{Z}$ despite -1 being a square modulo 34.

Exercise 7.5.14. Solve the equation $3x^2 - 2y^2 = 10$ over $\mathbb{Z}$.

Fundamental Units

Exercise 7.5.15†**.** Let $d \equiv 1 \pmod 4$ be a squarefree integer, and suppose $\eta = \frac{a+b\sqrt{d}}{2} \notin \mathbb{Z}[\sqrt{d}]$ is the fundamental unit of $\mathbb{Q}(\sqrt{d})$. Prove that $\eta^n \in \mathbb{Z}[\sqrt{d}]$ if and only if $3 \mid n$.

Exercise 7.5.16†**.** Let $d \neq 1$ be a squarefree rational integer, and suppose that $2^{2n} + 1 = dm^2$ for some integers $n, m \geq 0$. Show that $2^n + m\sqrt{d}$ is the fundamental unit of $\mathbb{Q}(\sqrt{d})$, provided that $d \neq 5$.

Exercise 7.5.17†**.** Suppose that $d = a^2 \pm 1$ is squarefree, where $a \geq 1$ is some rational integer and let $k \geq 0$ be a rational integer. Suppose that the equation $x^2 - dy^2 = m$ has a solution in $\mathbb{Z}$ for some $|m| < ka$. For sufficiently large d, prove that $|m|$, $d+m$ or $d-m$ is a square.

Exercise 7.5.18†. Solve completely the equation $x^3 + 2y^3 + 4z^3 = 6xyz + 1$ which was seen in Problem 6.2.2.

Exercise 7.5.19† (Weak Dirichlet's Unit Theorem)**.** Let K be a number field with r real embeddings and s pairs of complex embeddings. Prove that there exist units $\varepsilon_1, \ldots, \varepsilon_k$ with $k \leq r + s - 1$ such that any unit of K can be written uniquely in the form

$$\zeta \varepsilon_1^{n_1} \cdot \ldots \cdot \varepsilon_k^{n_k}$$

for some integers n_i and a root of unity ζ.

Exercise 7.5.20† (Gabriel Dospinescu)**.** Find all monic polynomials $f \in \mathbb{Q}[X]$ such that $f(X^n)$ is reducible in $\mathbb{Q}[X]$ for all $n \geq 2$ but f is irreducible.

Miscellaneous

Exercise 7.5.21† (Liouville's Theorem)**.** Let α be an algebraic number of degree n. Prove that there exists a constant $C > 0$ such that

$$\left| \alpha - \frac{p}{q} \right| > \frac{C}{q^n}$$

for any $p, q \in \mathbb{Z}$ (with $q > 0$).

Exercise 7.5.22†. Prove that $5n^2 \pm 4$ is a perfect square for some choice of $\pm$ if and only if n is a Fibonacci number.

Exercise 7.5.23† (ELMO 2020)**.** Suppose n is a Fibonacci number modulo every rational prime. Must it follow that n is a Fibonacci number?

Exercise 7.5.24† (Nagell, Ko-Chao, Chein)**.** Let p be an odd rational prime. Suppose that $x, y \in \mathbb{Z}$ are rational integers such that $x^2 - y^p = 1$. Prove that $2 \mid y$ and $p \mid x$. Deduce that this equation has no solution for $p \geq 5$. (The case $p = 3$ is Exercise 8.7.19†.)

Exercise 7.5.25†. Prove that there are at most $3^{|S|}$ pairs of S-units distant by 2.

Exercise 7.5.26†. Assuming the finiteness of rational solutions to the S-unit equation $u + v = 1$ for any finite S, determine all functions $f : \mathbb{Z} \to \mathbb{Z}$ such that $m - n \mid f(m) - f(n)$ for any m, n and f is a bijection modulo sufficiently large primes.

Exercise 7.5.27. Let m be a rational integer. What are the integers of $\mathbb{Q}(\sqrt[3]{m})$?

Chapter 8

p-adic Analysis

Prerequisites for this chapter: Section A.1 for the whole chapter, Sections 6.2 and 6.4 for Section 8.5 and Chapter 2 for Section 8.6. Chapter 6 is recommended.

p-adic numbers have many applications and are absolutely fundamental in number theory nowadays. That said, this chapter will be almost exclusively dedicated to proving the Skolem-Mahler-Lech theorem 8.5.1 and related results. We refer the reader to the Addendum 3A of [2] for more applications of p-adic numbers.

8.1 p-adic Integers and Numbers

Again, this section will be a bit abstract. If you have trouble, following, skip to Problem 8.3.1 for motivation. In elementary number theory, when working with diophantine equations, it is often useful to reduce the equation modulo a rational prime p. If that is not sufficient, one might look modulo p^2, then modulo p^3, etc. p-adic numbers are what you get when you consider something modulo p^n for **all** n. More precisely, a p-adic integer is the data of an element of $\mathbb{Z}/p\mathbb{Z}$, of an element of $\mathbb{Z}/p^2\mathbb{Z}$, of an element of $\mathbb{Z}/p^3\mathbb{Z}$, ..., such that these elements are compatible between them (the element of $\mathbb{Z}/p^2\mathbb{Z}$ is congruent to the element of $\mathbb{Z}/p\mathbb{Z}$ modulo p.)

Definition 8.1.1 (p-adic Integers)

A *p-adic integer* a is a tuple

$$(a_1, a_2, a_3 \ldots) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^3\mathbb{Z} \times \ldots$$

such that $a_i \equiv a_j \pmod{p^{\min(i,j)}}$ for any i, j. The set of p-adic integers is denoted $\mathbb{Z}_p$.

The p-adic integers $\mathbb{Z}_p$[1] form an integral domain under component-wise addition and multiplication, meaning that

$$(a_1, a_2, a_3, \ldots)(b_1, b_2, b_3, \ldots) := (a_1 b_1, a_2 b_2, a_3 b_3, \ldots)$$

and

$$(a_1, a_2, a_3, \ldots) + (b_1, b_2, b_3, \ldots) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots).$$

Exercise 8.1.1*. Check that $\mathbb{Z}_p$ is an integral domain. What is its characteristic?

Since p-adic integers are supposed to represent a tuple of local data modulo powers of p, it makes sense to associate the rational integer $a \in \mathbb{Z}$ with the p-adic integer $(a \pmod{p}, a \pmod{p^2}, a$

[1] Now you know why you shouldn't use $\mathbb{Z}_n$ for $\mathbb{Z}/n\mathbb{Z}$! If you want a shorter notation you can use $\mathbb{Z}/n$.

$(\text{mod } p^3), \ldots)$. Thus, by abuse of notation, we say $\mathbb{Z} \subseteq \mathbb{Z}_p$ because of this embedding.[2] In fact, since $a \pmod{p^n}$ makes sense when a is a rational number with denominator coprime with p, we even get

$$\mathbb{Z}_{(p)} \subseteq \mathbb{Z}_p$$

where $\mathbb{Z}_{(p)}$ denotes the rational numbers with denominator coprime with p.

Exercise 8.1.2*. Check that $a \mapsto (a \pmod{p}, a \pmod{p^2}, a \pmod{p^3}, \ldots)$ is indeed an embedding of $\mathbb{Z}_{(p)}$ into $\mathbb{Z}_p$, i.e. that it's injective.

Remark 8.1.1

We use the notation $\mathbb{Z}_{(p)}$ because it is the *localisation* of $\mathbb{Z}$ away from the prime ideal (p).

Now, suppose we want to make sense of $1/p$ p-adically. This can't be a p-adic integer because $1/p$ makes no sense modulo p. Thus, we define *p-adic numbers* by allowing a formal (subject to some relations) division of p-adic integers by powers of p.

Definition 8.1.2 (p-adic numbers)

A *p-adic number* is an element of the form $p^k a$ for some $k \in \mathbb{Z}$ and $a \in \mathbb{Z}_p$. The set of p-adic numbers is denoted $\mathbb{Q}_p$.

With this, we can now say (somewhat abusively) that $\mathbb{Q} \subseteq \mathbb{Q}_p$ by associating the rational number $r = p^k a$ with $a \in \mathbb{Z}_{(p)}$ to $p^k(a \pmod{p}, a \pmod{p^2}, a \pmod{p^3}, \ldots)$. For instance, $1/p = p^{-1}(1, 1, 1, \ldots)$.

p-adic numbers now form a *field*, and as we have seen numerous times, working in a field is always great. Here is how multiplication and addition are defined: let $x = p^k a$ and $y = p^m b$ be p-adic numbers. Suppose without loss of generality that $m, k < 0$ otherwise they are p-adic integers. Multiplication is defined as $(p^k a)(p^m b) = p^{k+m} ab$, and addition by

$$p^k a + p^m b = p^{k+m}(p^{-k} a + p^{-m} b) = p^{k+m}(p^{-k} a_1 + p^{-m} b_1, p^{-k} a_2 + p^{-m} b_2, \ldots)$$

as $p^{-k} a$ and $p^{-m} b$ are p-adic integers by assumption.[3]

It remains to prove that every element of $\mathbb{Q}_p$ has a multiplicative inverse, so far we have only shown that it is a ring. This is easy, but before we do it let us define the *p-adic valuation* of p-adic numbers.

Proposition 8.1.1 (Units of $\mathbb{Z}_p$)

The units in $\mathbb{Z}_p$ (we will also call them "units of $\mathbb{Q}_p$" abusively), $\mathbb{Z}_p^\times$, are the p-adic integer with non-zero first coordinate: $a = (a_0, \ldots)$ and $a_0 \not\equiv 0 \pmod{p}$.

Proof

This is obvious: if $a_0 \equiv 0$ then $a_0 b_0 \equiv 0$ for any b_0 so ab can never be $1 = (1, 1, 1, \ldots)$. Conversely,

[2] $\mathbb{Z}$ is isomorphic to the subset of p-adic integers of the previous form; in general, when $f : S \to U$ is an injective morphism, we call f an *embedding* of S into U. Notice that the regular embeddings of a number fields are embeddings into $\mathbb{C}$. See also Remark 6.2.1.

[3] Technically, as we have defined p-adic numbers, $p^k(a_1, a_2, a_3, \ldots)$ and $(p^k a_1, p^k a_2, p^k a_3, \ldots)$ are distinct for positive k. Indeed, we said our division by p was *formal*, which means a p-adic number is a tuple $(k, a) \in \mathbb{Z} \times \mathbb{Z}_p$ which we write as $p^k a$. This is however very easy to fix: just identify these two p-adic numbers to be the same.

if $a_0 \not\equiv 0$, the components of a are all invertible since they are coprime with p^n for any n, so

$$a^{-1} = (a_0^{-1}, a_1^{-1}, a_2^{-1}, \ldots).$$

■

Definition 8.1.3 (p-adic valuation)

Let $z \in \mathbb{Q}_p$ be a non-zero p-adic number. Write $z = p^k a$ where $a \in \mathbb{Z}_p^\times$ is a unit. The *p-adic valuation* of z, $v_p(z)$ is the integer k. We also define $v_p(0) = +\infty$.

Of course, the p-adic valuation of rational integers is the same as the regular p-adic valuation. Now it is follows directly that $\mathbb{Q}_p$ is a field: if $z = p^{v_p(z)}a$, $z^{-1} = p^{-v_p(z)}a^{-1}$.

To finish this section, we mention one nice property of p-adic numbers. Even if this proposition does not convince you of the use of $\mathbb{Q}_p$, it should at least convince you that it is a very nice object.

Theorem 8.1.1 (Hensel's Lemma)

Let $f \in \mathbb{Z}_p[X]$ be a polynomial. If, for some $a \in \mathbb{Z}_p$, $|f(a)|_p < 1$ and $|f'(a)| = 1$, then f has a unique root $\alpha \equiv a \pmod{p}$ in $\mathbb{Z}_p$.

Proof

This is almost exactly the regular Hensel lemma 5.3.1: if f has a root a modulo p, i.e. $|f(a)|_p < 1$, such that $p \nmid f'(a)$, i.e. $|f'(a)|_p = 1$, then f has a unique root r_k in $\mathbb{Z}/p^k\mathbb{Z}$ congruent to a modulo p. The number $\alpha = (\alpha_1, \alpha_2, \alpha_3, \ldots)$ is then the unique root of f in $\mathbb{Q}_p$ congruent to a modulo p. The only difference is that, in our previous version of Hensel's lemma, f had coefficients in $\mathbb{Z}$ and not in $\mathbb{Z}_p$. However, it is easy to check that this does note change anything to the proof.

■

This usually reduces the problem of finding roots of polynomials in $\mathbb{Q}_p$ to finding roots in $\mathbb{F}_p$. For instance, there is a square root of -1 in $\mathbb{Q}_5$.

8.2 p-adic Absolute Value

This p-adic valuation lets us define an *absolute value* on $\mathbb{Q}_p$: $|z|_p = p^{-v_p(z_p)}$ (and $|0|_p = 0$).

Definition 8.2.1 (p-adic Absolute Value)

The p-adic absolute of $\mathbb{Q}_p$ is defined as $|\cdot|_p = p^{-v_p(\cdot)}$ (in particular $|p|_p = 1/p$). The regular absolute value on $\mathbb{R}$ (or $\mathbb{C}$) will be denoted $|\cdot|_\infty$.

By an absolute value, we mean a function $|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}_{>0}$ which is multiplicative, zero only at zero, and which satisfies the triangular inequality. The first two properties are obvious, and the last one follows from the following stronger inequality.

Proposition 8.2.1 (Strong Triangle Inequality)*

For any p-adic numbers $x, y \in \mathbb{Q}_p$, we have $|x + y|_p \leq \max(|x|_p, |y|_p)$ with equality if $|x_p| \neq |y|_p$.

Proof

This is equivalent to $v_p(x+y) \geq \min(v_p(x), v_p(y))$ with equality if $v_p(x) \neq v_p(y)$ which is obvious.

■

Notice that with this absolute value, the p-adic integers are now a *ball*: $\mathbb{Z}_p = \{|z|_p \leq 1 \mid z \in \mathbb{Q}_p\}$ since p-adic integers are the p-adic numbers with non-negative p-adic valuation.

With this norm we can now define a *distance* on $\mathbb{Q}_p$: $d(x, y) = |x-y|_p$. This is completely analogous to $\mathbb{R}$ and $\mathbb{C}$, but now two numbers are very close if they are divisible by a large power of p. With this distance, we can define convergence: a sequence $(a_n)_{n\geq 0}$ of p-adic numbers converges to $a \in \mathbb{Q}_p$ if $d(a, a_n) \to 0$, i.e. $|a - a_n|_p \to 0$. This is also equivalent to $v_p(a - a_n) \to +\infty$. For instance, the sequence $(p^n)_{n\geq 0}$ converges to 0 p-adically.

Remark 8.2.1

We will usually use $x_n \to 0$ to mean that x_n goes to 0 p-adically, but sometimes it will also mean that $x_n \to 0$ over $\mathbb{R}$. We hope that the distinction will be made clear from context; the latter will normally be used when x_n is a sequence of norms of p-adic numbers.

Similarly, we can define convergence of series $\sum_i a_i$: we say the series converges if its partial sums $b_n = \sum_{i=0}^{n} a_i$ converge. Here is a fundamental proposition, that show that the situation is very different in the p-adic case compared to the real or complex case.

Proposition 8.2.2 (p-adic Convergence of Series)*

The series $\sum_i a_i$ converges if and only if $a_n \to 0$.

Proof

It is clear that if it converges, $a_n = \sum_{i=0}^{n} a_i - \sum_{i=0}^{n-1} a_i$ converges. The surprising part is that the converse also holds. If $a_n \to 0$, we can assume they are all p-adic integers since there will only be a finite number of non-integral a_i ($a_n \in \mathbb{Z}_p$ iff $|a_n|_p \leq 1$).

Consider the kth component of the series $\sum_i a_i$: it is the sum of the kth components of a_i. But since $a_m \to 0$, the kth component of a_i is zero for sufficiently large i. Thus, the kth component of $\sum_i a_i$ is a sum of a finite number of terms for each k, which mean that they are all well-defined and thus $\sum_i a_i$ is too. (Looking at the kth component is equivalent to reducing modulo p^k: there are a finite number of a_i not divisible by p^k so the partial sums eventually stabil modulo p^k, which means that it converges p-adically since it is true for all k.)

■

Exercise 8.2.1*. Convince yourself of this proof.

Over $\mathbb{R}$ this is very wrong: the harmonic series $\sum_{i\geq 1} \frac{1}{i}$ diverges but $\frac{1}{i} \to 0$. As a corollary, we get a very simple criterion for the convergence of a sequnce $(a_n)_{n\geq 0}$.

Corollary 8.2.1*

A sequence $(a_n)_{n\geq 0}$ of p-adic numbers converges if and only if $a_{n+1} - a_n \to 0$.

Proof

Apply Proposition 8.2.2 to the series $\sum_i a_{i+1} - a_i$ (the nth partial sum is $a_n - a_0$).

■

Exercise 8.2.2*. Prove that the strong triangle inequality also holds for series: if $a_i \to 0$ then $\left|\sum_i a_i\right|_p \leq \max_i |a_i|_p$ with equality if the maximum is achieved only once.

Let us talk a bit more about the p-adic absolute value. Recall that real numbers are constructed from rational numbers by *adding the limits of sequences which should converge but do not in* $\mathbb{Q}$. Here is an example. If you write down the decimal digits of $\sqrt{2}$, you get a sequence of rational numbers converging (in $\mathbb{R}$) to $\sqrt{2}$. But in $\mathbb{Q}$, this sequence does not have a limit (so does not converge) as $\sqrt{2} \notin \mathbb{Q}$. You might ask "how do we determine which sequences *should* converge without having defined $\mathbb{R}$ first?". This is achieved by the notion of a *Cauchy sequence*: a sequence $(a_n)_{n\geq 0}$ such that, for any $\varepsilon > 0$, $|a_m - a_n| \leq \varepsilon$ for sufficiently large m and n ($m, n \geq N$ for some N).

This process is called *completing* $\mathbb{Q}$ *with respect to* $|\cdot|_\infty$, and $\mathbb{R}$ is said to be the *completion of* $\mathbb{Q}$ *with respect to* $|\cdot|_\infty$. For this reason we shall also denote $\mathbb{R}$ by $\mathbb{Q}_\infty$.[4] We do not discuss the technical details here, but it turns out the p-adic fields we constructed are the completions of $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot|_p$ (the fact that Cauchy sequences converges follows from the stronger Corollary 8.2.1).[5] In fact, the only fields you can get by completing $\mathbb{Q}$ with respect to some absolute value are $\mathbb{R}$ and the p-adic fields $\mathbb{Q}_p$ (thus called the completions of $\mathbb{Q}$) by Exercise 8.7.9†[6]

The completions of $\mathbb{Q}$ (and their finite extensions) are called *local* fields (because they have local data) while $\mathbb{Q}$ and its finite extensions are called *global* fields.[7] In **??** we will see one instance of how you can piece local data together to get global data (the Hasse-Minkowski principle **??**). More simply, though, we have the following proposition.

Proposition 8.2.3 (Product Formula)

For any non-zero $x \in \mathbb{Q}$, we have

$$|x|_\infty \cdot \prod_p |x|_p = 1.$$

Exercise 8.2.3*. Prove the product formula.

8.3 Binomial Series

This section will be a bit more concrete. We wish to make sense of a^b for p-adic numbers a and b. Actually, already over $\mathbb{Q}$, a^b doesn't always make sense in $\mathbb{Q}$ for instance $2^{1/2} \notin \mathbb{Q}$ (and if we consider $\mathbb{Q}(\sqrt{2})$, then $2^{\sqrt{2}}$ is not even algebraic by a deep result of Gelfond-Schneider). Thus we will only try to make sense of a^b for $b \in \mathbb{Z}_p$, although even there it won't be defined canonically for all $a \in \mathbb{Q}_p$: we will define a^b only when $a \equiv 1 \pmod{p}$ and $b \in \mathbb{Z}_p$.

Write $a = 1 + u$, with $p \mid u$. Over $\mathbb{Z}$, we can define $(1+u)^b$ for positive $b \in \mathbb{Z}$ as

$$\sum_k \binom{b}{k} u^k.$$

In fact, the same formula works for any $b \in \mathbb{Z}_p$ because $u^k \to 0$ so the series will converge. Let us explain a bit more. We need the fundamental fact that $\mathbb{Z}$ and even $\mathbb{N}$ are dense in $\mathbb{Z}_p$.

[4] $\mathbb{Z}_\infty$ is sometimes thought of as $[-1, 1]$ since for $p \neq \infty$ we have $\mathbb{Z}_p = \{|x| \leq 1 \mid x \in \mathbb{Q}_p\}$, but it doesn't have properties as nice as the other $\mathbb{Z}_p$.

[5] The fact that its elements have such an explicit form in terms of $\mathbb{Q}$ is because $|\cdot|_p$ is *non-Archimedean*, i.e. satisfies the strong triangle inequality Proposition 8.2.1.

[6] There are absolute values different from $|\cdot|_\infty$ and $|\cdot|_p$ like $|\cdot|_\infty^2$, but completing $\mathbb{Q}$ with respect to $|\cdot|_\infty^2$ gives (a field isomorphic to) $\mathbb{R}$.

[7] Technically, there are other local or global fields as well, but these are the only ones in characteristic 0.

Proposition 8.3.1

$\mathbb{N}$ is *dense* in $\mathbb{Z}_p$, meaning that for any $a = (a_1, \ldots) \in \mathbb{Z}_p$ and any $\varepsilon > 0$, there is a $b \in \mathbb{N}$ such that $|a - b| < \varepsilon$. Similarly, $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

Proof

Simply pick $b \equiv a_n \pmod{p^n}$ for some large n: we get $|a-b|_p \leq p^{-n}$. For $\mathbb{Q}_p$ it's Exercise 8.3.1*. ■

Exercise 8.3.1*. Prove that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

Here is what this implies. For a fixed k, denote by $\binom{\cdot}{k} : \mathbb{Z}_p \to \mathbb{Q}_p$ the function

$$\binom{n}{k} = \frac{n(n-1)\cdot\ldots\cdot(n-(k-1))}{k!}.$$

This is a continuous function (Exercise 8.3.2*) which satisfies $\left|\binom{n}{k}\right|_p \leq 1$ on $\mathbb{N}$. Since $\mathbb{N}$ is dense in $\mathbb{Z}_p$, we in fact have $\left|\binom{n}{k}\right|_p \leq 1$ on $\mathbb{Z}_p$ so $\binom{\cdot}{k} : \mathbb{Z}_p \to \mathbb{Z}_p$ (Exercise 8.3.3*). Finally, this means that, for $|u|_p < 1$, the function

$$(1+u)^n = \sum_{k=0}^{\infty} \binom{n}{k} u^k$$

converges for any n in $\mathbb{Z}_p$ by Proposition 8.2.2 as $\left|\binom{n}{k}u^k\right|_p \leq |u|_p^k \to 0$. In fact, this is the unique extension of $n \mapsto (1+u)^n$ from $\mathbb{N}$ to $\mathbb{Z}_p$ as $\mathbb{N}$ is dense in $\mathbb{Z}_p$.

Exercise 8.3.2*. Let $f \in \mathbb{Q}_p[X]$ be a polynomial. Prove that f is continuous on $\mathbb{Q}_p$.

Exercise 8.3.3*. Let $f : \mathbb{Z}_p \to \mathbb{Q}_p$ be a continuous function. If $|f(x)|_p \leq 1$ for any n in a dense subset (in $\mathbb{Z}_p$), prove that $|f(x)|_p \leq 1$ for any $x \in \mathbb{Z}_p$.

Finally, we get the following proposition.

Proposition 8.3.2*

Let $|u|_p < 1$ be a p-adic number. The function

$$z \mapsto (1+u)^z := \sum_{k=0}^{\infty} \binom{z}{k} u^k$$

is a continuous multiplicative function $\mathbb{Z}_p \to \mathbb{Z}_p$, i.e. for any $x, y \in \mathbb{Z}_p$ we have

$$(1+u)^x (1+u)^y = (1+u)^{x+y}.$$

Proof

It sufices to note that $(1+u)^x(1+u)^y = (1+u)^{x+y}$ for any $x, y \in \mathbb{N}$ thus for any $x, y \in \mathbb{Z}_p$ by density. ■

Before presenting an application, let us present a philosophical remark about p-adic numbers taken from Evan Chen [9]. Imagine you are given the following problem: estimate $\frac{1}{1^2} + \ldots + \frac{1}{10000^2}$ to within 0.001. This is a statement solely about rational numbers, but it is considerably easier to solve if one knows about real numbers:

$$\frac{1}{1^2} + \ldots + \frac{1}{10000^2} = \frac{\pi^2}{6} - \sum_{k=10001}^{\infty} \frac{1}{k^2}$$

and it is now very easy to estimate $\frac{\pi^2}{6}$ and $\sum_{k=10001}^{\infty} \frac{1}{k^2}$. Similarly, suppose you are given the following problem.

Problem 8.3.1 (USA TST 2002 Problem 2)

Let $p > 5$ be a rational prime. Prove that the sum

$$f_p(x) = \sum_{k=1}^{p-1} \frac{1}{(px+k)^2}$$

does not depend on $x \in \mathbb{Z}$ modulo p^3.

We wish to compute this sum modulo p^3, that is, estimate this p-adic sum S to a value $s \in \mathbb{Q}$ such that $|S - s|_p \leq p^{-3}$. This is a statement about rational numbers, but it really helps to use p-adic numbers to estimate it p-adically.

Solution

We work in $\mathbb{Q}_p$. We have

$$\begin{aligned}
\sum_{k=1}^{p-1} \frac{1}{(px+k)^2} &= \sum_{k=1}^{p-1} \frac{1}{k^2} \left(1 + \frac{px}{k}\right)^{-2} \\
&= \sum_{k=1}^{p-1} \frac{1}{k^2} \sum_{i=0}^{\infty} \binom{-2}{i} \left(\frac{px}{k}\right)^i \\
&\equiv \sum_{k=1}^{p-1} \frac{1}{k^2} \left(\binom{-2}{0} + \binom{-2}{1} \frac{px}{k} + \binom{-2}{2} \frac{p^2x^2}{k^2} \right) \pmod{p^3} \\
&= \sum_{k=1}^{p-1} \frac{1}{k^2} - 2xp \sum_{k=1}^{p-1} \frac{1}{k^3} + 3x^2p^2 \sum_{k=1}^{p-1} p - 1 \frac{1}{k^4}.
\end{aligned}$$

By Exercise 8.3.4*, this is congruent to $\sum_{k=1}^{p-1} \frac{1}{k^2}$ modulo p^3, which proves the result. ■

Exercise 8.3.4*. Prove that, if $p > 5$ is a rational prime, $p^2 \mid \sum_{k=1}^{p-1} \frac{1}{k^3}$ and $p \mid \sum_{k=1}^{p-1} \frac{1}{k^4}$.

Finally, we prove that $x \mapsto (1+u)^x$ can be expanded as a power series in x. This will be useful for proving the Skolem-Mahler-Lech theorem in Section 8.5. In fact we prove the following more general result.

Proposition 8.3.3

Let $(a_n)_{n \geq 0}$ be a sequence of p-adic numbers such that $a_n \to 0$. If $a_k/k! \to 0$, the function

$$f(x) = \sum_{k=0}^{\infty} a_k \binom{x}{k}$$

defines a convergent power series on $\mathbb{Z}_p$.

We shall simply expand the binomial coefficients in terms of x and switch the double sums to get a power series. For this, we need a lemma to switch double sums (of infinitely many terms), similar to Proposition 8.2.2. Over $\mathbb{R}$ and $\mathbb{C}$ it's usually tricky and not always true, but over $\mathbb{Q}_p$ it's very simple like for Proposition 8.2.2.

Proposition 8.3.4 (Switching Double Sums)

Let $(a_{i,j})_{(i,j)\in\mathbb{N}^2}$ be a family of p-adic numbers. Suppose $a_{i,j} \to 0$ when $i+j \to \infty$ (meaning that, for any $\varepsilon > 0$, there are finitely many pairs (i,j) such that $|a_{i,j}|_p > \varepsilon$). Then,

$$\sum_{i=0}^{\infty}\sum_{j=0}^{\infty} a_{i,j} = \sum_{j=0}^{\infty}\sum_{i=0}^{\infty} a_{i,j}$$

(in particular, both series converge).

Exercise 8.3.5*. Prove Proposition 8.3.4.

Proof of Proposition 8.3.3

Expand $k!\binom{x}{k} = x(x-1)\cdot\ldots\cdot(x-(k-1))$ as $\sum_i c_{i,k}x^i$, where $|c_{i,k}|_p \leq 1$ as $c_{i,k} \in \mathbb{Z}$. By Proposition 8.3.4, we get

$$\sum_{k=0}^{\infty} a_k \binom{x}{k} = \sum_{i=0}^{\infty} x^i \sum_{k=0}^{\infty} c_{i,k}\frac{a_k}{k!}$$

as $|c_{i,k}a_k/k!|_p \leq |a_k/k!|_p \underset{i+k}{\longrightarrow} 0$.

■

Finally, to conclude that $x \mapsto (1+u)^x$ is a power series, by Proposition 8.3.3, we need to estimate $|k!|_p$ to prove that we indeed have $u^k/k! \to 0$. This follows from the following proposition.

Proposition 8.3.5 (Legendre's Formula)*

Let $n \in \mathbb{N}$. We have

$$v_p(n!) = \sum_{k=1}^{\infty}\left\lfloor\frac{n}{p^k}\right\rfloor = \frac{n - s_p(n)}{p-1}.$$

In particular, $v_p(n!) = \frac{n}{p-1} + o(n)$ and $|n!|_p = p^{-n/(p-1)+o(n)}$, where $o(n) = -\frac{s_p(n)}{p-1}$ is a quantity such that $o(n)/n \to 0$.

Remark 8.3.1

One might notice that for $u \in \mathbb{Q}_p$, $|u|_p < p^{-1/(p-1)}$ is equivalent to $|u|_p < 1$ because the only values $|u|_p \leq 1$ can take are $1, 1/p, 1/p^2, \ldots$. There is however a reason why we stated it that way: it's because we can do algebraic number theory over $\mathbb{Q}_p$, and over extensions of $\mathbb{Q}_p$ we might have $p^{-1/(p-1)} < |u|_p < 1$. (See **??**.)

Proof

The first equality is left as Exercise 8.3.6*. For the second one, write $n = n_m p^m + \ldots + n_1 p + n_0$

the base p expansion of n. Then,

$$\left\lfloor \frac{n}{p^k} \right\rfloor = n_m p^{m-k} + \ldots + n_{k+1} p + n_k.$$

Thus,

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \\ &= \sum_{k=1}^{m} \sum_{i=k}^{m} n_i p^{i-k} \\ &= \sum_{i=0}^{m} n_i \sum_{k=1}^{i} p^{i-k} \\ &= \sum_{i=0}^{m} n_i \cdot \frac{p^i - 1}{p-1} \\ &= \frac{n - s_p(n)}{p-1}. \end{aligned}$$

■

Exercise 8.3.6*. Let $n \in \mathbb{N}$ be a positive rational integer and p be a prime number. Prove that

$$v_p(n)! = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Corollary 8.3.1*

For any $|u|_p < p^{-1/(p-1)}$, the function $x \mapsto (1+u)^x$ is a convergent power series on $\mathbb{Z}_p$.

Exercise 8.3.7*. Prove Corollary 8.3.1.

8.4 Analytic Functions

In this section, we discuss (p-adic) (locally and globally)*analytic* functions, i.e. functions given (locally or globally) by power series.

Definition 8.4.1 (Local Analyticity)

Let $f : \mathbb{Z}_p \to \mathbb{Q}_p$ be a function. We say f is *locally analytic* at α if $f(x)$ is a given by a power series in $x-\alpha$ around α, i.e. there is an $\varepsilon > 0$ and numbers $a_n \to 0$ such that, for any $|x-\alpha|_p \leq \varepsilon$,

$$f(x) = \sum_{i=0}^{\infty} a_i (x-\alpha)^i.$$

If f is locally analytic everywhere (on $\mathbb{Z}_p$), we say it's simply locally analytic (on $\mathbb{Z}_p$).

Remark 8.4.1

Locally analytic functions are commonly referred to as just analytic functions.

Exercise 8.4.1*. Prove that locally analytic functions are continuous.

Exercise 8.4.2*. Prove that the sum and product of two locally analytic functions is again a locally analytic function.

Exercise 8.4.3*. Prove that polynomials are locally analytic (everywhere).

It turns out that there is an extremely simple class of p-adic analytic functions: globally analytic functions, i.e. functions given by a convergent power series $f(x) = \sum_{i=0}^{\infty} a_i x^i$ for some $a_i \to 0$. This lets us prove that a function is locally analytic in a very simple way. Why do we care about analytic functions? Let us explain a bit what we are trying to do.

Our goal is to prove the Skolem-Mahler-Lech theorem 8.5.1, which says that the zeros of a linear recurrence $(a_n)_{n\in\mathbb{Z}}$ of algebraic numbers[8] are a union of a finite set and some arithmetic progressions; this was used in Section 7.4 for instance. How are we going to approach this theorem? There are two main steps. For the sake of simplicity, we suppose $a_n = \sum_i f_i(n)\alpha_i^n$ where $f_i \in \mathbb{Z}[X]$ and $\alpha_i \in \mathbb{Z}$.

1. Transform $(a_n)_{n\in\mathbb{Z}}$ into (the restriction of) multiple p-adic analytic functions. $n \mapsto \alpha_i^n$ might not define directly a p-adic analytic function with Corollary 8.3.1, but $n \mapsto \alpha_i^{(p-1)n}$ does since, by little Fermat's theorem, $\alpha_i^{p-1} \equiv 1 \pmod p$. Hence $s_k = (a_{(p-1)m+k})_{m\in\mathbb{Z}}$ define $p-1$ analytic functions on $\mathbb{Z}_p$.

2. Show that a locally analytic function is either identically zero on $\mathbb{Z}_p$, or has finitely many zeros in $\mathbb{Z}_p$ (and thus in $\mathbb{Z}$ too). This means that each s_k is either always zero or has finitely many zeros which was what we wanted to show (the zeros of $(a_n)_{n\in\mathbb{Z}}$ are a union of a finite set and arithmetic progressions of the form $((p-1)m+k)_m$).

Thus, our goal in this section is to prove that $x \mapsto (1+u)^x$ defines a locally analytic function, as well as the second step: that a locally analytic funtion has finitely many zeros in $\mathbb{Z}_p$. This is in fact not so surprising in hindsight: $\mathbb{Z}_p$ consists of those elements of $\mathbb{Q}_p$ which are "small" (have absolute value at most 1). In fact, for small elements, the same results hold over $\mathbb{R}$ and $\mathbb{C}$: a locally analytic function in $\mathbb{R}$ is either identically zero in $[-1,1]$ or has finitely many zeros there, and the same goes for $\mathbb{C}$ and the unit disk. What changes is that rational integers are small in $\mathbb{Q}_p$ but big in $\mathbb{R}$ and $\mathbb{C}$.

We now come back to what we first stated in this section: the fact that globally analytic functions are locally analytic. We shall prove that any power series is locally analytic: this will imply that $x \mapsto (1+u)^x$ is locally analytic for $|u|_p < p^{-1/(p-1)}$, by Proposition 8.3.3. This means that, although analycity was defined as being a *local* property, it also follows from a *global* one (but the converse is not true[9]).

Definition 8.4.2 (Globally Analytic Function)

A globally analytic function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is a function given everywhere (on $\mathbb{Z}_p$) by a convergent power series around some $\alpha \in \mathbb{Z}_p$, i.e., there are numbers $a_n \to 0$ such that, for any $x \in \mathbb{Z}_p$,

$$f(x) = \sum_{i=0}^{\infty} a_i (x-\alpha)^i.$$

[8] Actually, it is also true for sequences in any field of characteristic zero, but we only prove it for sequences of algebraic numbers. The general case is Exercise 8.7.29†.

[9] For instance, if $p^{-1/(p-1)} < |u|_p < 1$, $(1+u)^x$ is locally analytic since we can show that $(1+u)^{p^n} \equiv 1 \pmod p$ for some n, but not globally analytic. As we mentioned in Remark 8.3.1, to find such an u requires knowledge of algebraic extensions of $\mathbb{Q}_p$, see Exercise 8.7.13†.

Proposition 8.4.1

Let f be a globally analytic on $\mathbb{Z}_p$. Then, f is also locally analytic.

We will in fact prove that, for any $\alpha \in \mathbb{Z}_p$, f is equal around α to its Taylor series at α ($f^{(n)}$ is the nth (formal) derivative of f: $\left(\sum_{i=0}^{\infty} a_i x^i\right)' = \sum_{i=0}^{\infty} i a_i x^{i-1}$):

Proposition 8.4.2 (Taylor Series)

Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$ which converges everywhere for $\mathbb{Z}_p$. Then, for any $\alpha \in \mathbb{Z}_p$,

$$f(x) = \sum_{n=0}^{\infty} (x-\alpha)^n \frac{f^{(n)}(\alpha)}{n!}$$

for any $x \in \mathbb{Z}_p$ (in particular this series converges for such x).

As a corollary, the globally analytic functions are exactly the convergent power series. Actually, the proof of this proposition is almost identical to the one of Proposition 5.3.1, using Proposition 8.3.4.

Exercise 8.4.4*. Prove Proposition 8.4.2.

To conclude this section, we prove that a locally analytic function has finitely many zeros on $\mathbb{Z}_p$ or is identically zero. For this, we need to prove that $\mathbb{Z}_p$ is *sequentially compact*, meaning that any $(a_n)_{n\geq 0}$ sequence of p-adic integers has a convergent subsequence $(a_{\varphi(n)})_{n\geq 0}$ (over $\mathbb{R}$ or $\mathbb{C}$ this is known as the Bolzano-Weierstrass theorem, see Exercise 8.7.10†).

Definition 8.4.3 (Sequential Compactness)

We say a set S of p-adic numbers is *sequentially compact* if any sequence $(s_n)_{n\geq 0}$ of elements of S has a subsequence $s_{\varphi(n)} \to s \in S$ converging to an element of S.

Proposition 8.4.3 ($\mathbb{Z}_p$ is Sequentially Compact)

$\mathbb{Z}_p$ is sequentially compact.

Proof

Let $(a_n)_{n\geq 0}$ be a sequence of p-adic integers. By the pigeonhole principle, $(a_n)_n =: (a_{n,0})_n$ has an infinite subsequence $(a_{n,1})_n$ which is constant modulo p. Now $(a_{n,1})_n$ has an infinite subsequence constant modulo p^2, $(a_{n,2})_n$. Repeating this process, we get an chain of sequences

$$(a_{n,0})_n \subseteq (a_{n,1})_n \subseteq \dots$$

such that $(a_{n,k})_n$ is constant modulo p^k. Thus, the subsequence

$$(a_{0,0}, a_{0,1}, a_{0,2}, \dots)$$

converges as $a_{0,k+1} \equiv a_{0,k} \pmod{p^k}$ so $|a_{0,k+1} - a_{0,k}|_p \leq p^{-k}$.

■

Proposition 8.4.4 (Principle of Isolated Zeros)

Let f be a non-zero locally analytic function. The zeros of f are *isolated*, meaning that there is no sequence of distinct zeros of f which converges to another zero.

Proof

Let α be a zero of f, if there exists one. Write

$$f(x) = \sum_{k=0} a_k (x-\alpha)^k$$

(using Proposition 8.4.2 we get that this converges for all $|x|_p < r$). Let m be the smallest integer such that $a_m \neq 0$; there exists one otherwise f is identically zero. Define

$$g(x) = \sum_{k=m}^{\infty} b_k (x-\alpha)^{k-m}$$

so that $f(x) = (x-\alpha)^m g(x)$. Since $g(\alpha) = b_m$ is non-zero, by continuity there is some ε such that $g(x)$ is non-zero when $|x-\alpha|_p < \varepsilon$. Thus, $f(x) = g(x)(x-\alpha)^m$ is also non-zero there, which shows that α is isolated.

■

Corollary 8.4.1*

A non-zero locally analytic function on a sequential compact has finitely many zeros.

Proof

Suppose a locally analytic function f had infinitely many zeros there would be a sequence of zeros converging by Proposition 8.4.3. By continuity, it converges to another zero z. This contradicts the fact that z is isolated.

■

Note that the only property we have used here is the sequential compactness, so in particular this result also holds over $\mathbb{R}$ and $\mathbb{C}$.

8.5 The Skolem-Mahler-Lech Theorem

With all the hard work we did in the previous section, it is now straightforward to deduce the Skolem-Mahler-Lech theorem.

Theorem 8.5.1 (Skolem-Mahler-Lech Theorem)

Let $(u_n)_{n\in\mathbb{Z}}$ be a linear recurrence of algebraic numbers. The zeros $\mathcal{Z}((u_n)_n)$ of $(a_n)_n$, i.e. the set of n such that $a_n = 0$, is a union of a finite set and a finite number of arithmetic progressions:

$$\mathcal{Z}((u_n)_n) = S \cup \bigcup_{i=0}^{k} (a_i + b_i\mathbb{Z})$$

where S is a finite set and $a_i, b_i \in \mathbb{Z}$.

Remark 8.5.1

The Skolem-Mahler-Lech theorem is also valid for sequences in aribtrary fields of characteristic zero. Skolem proved it for sequences of rational numbers, Mahler for algebraic numbers and Lech for sequences in any field of characteristic zero. Thus, the above theorem could perhaps be called the "Skolem-Mahler theorem".

Notice that this theorem is optimal: the sequence

$$a_n = (n - s_1) \cdot \ldots \cdot (n - s_m) \cdot (\omega_1^{n-b_1} - 1) \cdot \ldots \cdot (\omega_k^{n-b_k} - 1)$$

where ω_i is a primitive a_ith root of unity vanishes exactly on $\{s_1, \ldots, s_m\} \bigcup_{i=0}^{k} (a_i + b_i\mathbb{Z})$.

Proof

Write $u_n = \sum_i f_i(n)\alpha_i^n$ where $f_i \in \overline{\mathbb{Q}}[X]$ and $\alpha_i \in \overline{\mathbb{Q}}$ by Theorem C.4.1. Note that we can suppose without loss of generality that $(u_n)_{n\geq 0}$ takes rational values. Indeed, if K is the fields generated by the α_i and the coefficients of the f_i as well as all their conjugates, then, for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, u_n is zero iff

$$\sigma(u_n) = \sum_i \sigma f_i(n)\sigma(\alpha_i)^n$$

is, so we can consider the norm $\prod_\sigma \sum_i \sigma f_i(n)\sigma(\alpha_i)^n$.

Choose a rational prime such that α_i and the coefficients of f_i make sense in $\mathbb{F}_p$ for all i. This can be done as follows: pick a non-zero $N \in \mathbb{Z}$ such that $Nf_i \in \overline{\mathbb{Z}}[X]$ and $N\alpha_i \in \overline{\mathbb{Z}}$ and then define h as the lcm of the minimal polynomials of $N\alpha_i$ and the minimal polynomials of the (non-zero) coefficients of Nf_i. Then, choose a rational prime $p \nmid N$ such that h splits in $\mathbb{F}_p$; there exists such a prime by Theorem 6.4.1.

In addition, choose p sufficiently large so that if $p \nmid h(a)$ then $p \nmid h'(a)$; this can be done using Bézout's lemma 5.4.1 as g is squarefree so coprime with its derivative. Finally, we also want the roots of h in $\mathbb{F}_p$ to be non-zero, this is again true for sufficiently large p as $h(0) \neq 0$ (since $\alpha_i \neq 0$).

Thus, write $a_n = \sum_i g_i\beta_i^n$ where $g_i \in \mathbb{Q}_p[X]$ and $\beta_i \in \mathbb{Q}_p$ by Theorem 8.1.1. Since $|\beta_i|_p = 1$ by construction, we have $|\beta_i^{p-1} - 1|_p \leq 1/p$ by Fermat's little theorem.

Thus, the function $n \mapsto \beta_i^{(p-1)n} = (1 + (\beta_i^{p-1} - 1))^n$ is analytic by Corollary 8.3.1 and Proposition 8.4.1. To conclude, for a fixed $r \in \mathbb{Z}/p\mathbb{Z}$, the function

$$n \mapsto \sum_i g_i((p-1)n + b)\beta_i^{(p-1)n+r} = u_{(p-1)n+r}$$

is analytic on $\mathbb{Z}_p$, so is either identically zero or has finitely many zeros in $\mathbb{Z}_p$ and thus in $\mathbb{Z}$ by Corollary 8.4.1.

Finally, put the zeros in the finite set when they are a finite number of them, and as an arithmetic progression when it is identically zero and we are done.

■

Remark 8.5.2

One could wonder why the fact that $s \mapsto (\alpha^N)^s$ is analytic doesn't imply that $s \mapsto \alpha^s$ is as well, by replacing s by s/N. The problems is that this only gives us an analytic function f which is equal to α^n **when** n **is a rational integer divisible by** N. More precisely, since $f(x+y) = f(x)f(y)$ for all $x, y \in \mathbb{Z}_p$, we know $f(1)$ is an Nth root of $f(N) = \alpha^N$, but we don't know which one. As

well we shall see very shortly, roots of unity are exactly the reason why some linear recurrences can be zero infinitely many times without being identically zero.

Exercise 8.5.1*. Convince yourself of this proof.

Exercise 8.5.2*. Do you think this proof could be formulated without appealing to p-adic analysis?

Corollary 8.5.1

For any linear recurrence $(u_n)_{n\in\mathbb{Z}}$ of algebraic numbers, there are finitely many $\alpha \in \overline{\mathbb{Q}}$ such that $(u_n)_n$ reaches α infinitely many times.

Proof

Write $u_n = \sum_i f_i(n)\alpha_i^n$. Our proof of Theorem 8.5.1 shows that the common difference depends only on the number field K generated by the coefficients of f_i as well as the α_i. Clearly, if $(u_n)_n$ reaches α then $\alpha \in K$.

This means that the common difference d is the same for $(a_n)_n$ as well as the linear recurrence $(u_n - \alpha)_n$, so if the latter vanishes infinitely many times then it vanishes on $d\mathbb{Z} + c$ for some c. Thus, $(u_n)_n$ can take a value α infinitely many times only for at most d values of α, otherwise, $(u_n - \alpha)_n$ and $(u_n - \beta)_n$ will vanish on the same $d\mathbb{Z} + c$ which is impossible for $\alpha \neq \beta$.

■

Here is a very nice corollary of the Skolem-Mahler-Lech theorem.

Corollary 8.5.2

Suppose $a_n = \sum_i f_i(n)\alpha_i^n$ is a linear recurrence of algebraic numbers which is zero infinitely many times but not identically zero. Then, α_i/α_j is root of unity for some $i \neq j$.

Note that this is not a weak result at all: if the field K generated by the α_i has exactly N roots of unity, then, for any fixed m, the sequence $(u_{Nn+m})_{n\in\mathbb{Z}}$ is a linear recurrence such that the quotient

$$\alpha_i^N/\alpha_j^N = (\alpha_i/\alpha_j)^N$$

of two distinct roots of its characteristic polynomial is never a root of unity since $\omega^N = 1$ for any root of unity $\omega \in K$. Thus, we can partition $(u_n)_{n\in\mathbb{Z}}$ into subsequences of the form $(u_{Nn+m})_{n\in\mathbb{Z}}$, and each of these subsequence must either be always zero or finitely many times zero. If we are dealing with sequences of integers, we can even combine this with Corollary 8.5.1 to get that each subsequence must be constant of tend to infinity in absolute value.

Exercise 8.5.3*. Prove that any number field has a finite number N of roots of unity, and that $\omega^N = 1$ for any root of unity ω of K. (In other words, the roots of unity of K are exactly the Nth roots of unity.)

We need a lemma to prove this corollary, which was already used in the proof of Theorem C.4.1.

Lemma 8.5.1

Let K be a field of characteristic zero. If

$$u_n = \sum_{i=1}^{k} g_i(n)\beta_i^n = 0$$

for any $n \in \mathbb{Z}$, where $g_i \in K[X]$ and $\beta_i \in K$ are both non-zero for all i, then $\beta_i = \beta_j$ for some $i \neq j$.

Proof of Corollary 8.5.2 using the Lemma

If $u_n = \sum_i f_i(n)\alpha_i^n$ is infinitely many times zero for some non-zero $f_i \in \overline{\mathbb{Q}}[X]$ and non-zero $r_i \in \overline{\mathbb{Q}}$, then

$$u_{r+sn} = \sum_i \alpha_i^v f_i(r+sn)\alpha_i^{un}$$

is identically zero for some $u \neq 0, v$ by Theorem 8.5.1. Thus, by the lemma, we must have $\alpha_i^s = \alpha_j^s$ for some $i \neq j$, which implies that α_i/α_j is a root of unity as wanted.

■

Proof of the Lemma

We prove the contrapositive: if $\beta_1, \ldots, \beta_k$ are all distinct then $g_i = 0$ for all i. We proceed by induction on $\sum_i \deg g_i$, the base case follows from the Vandermonde determinant C.3.2. For the induction step, suppose $\deg g_1 \geq 1$ without loss of generality. Consider the sequence

$$v_n = u_{n+1} - \beta_1 u_n = \sum_i (\beta_i g_i(n+1) - \beta_1 g_i(n))\beta_i^n.$$

Since $\deg(\beta_i g_i(X+1) - \beta_1 g_i) \leq \deg f_i$ for $i \geq 1$ and $\deg(\beta_1(g_i(X+1) - g_i)) \leq \deg f_i - 1$, by the induction hypothesis we have $\beta_i g_i(X+1) - \beta_1 g_i = 0$ for all i. This means that they are constant, but we have already treated this case so we are done.

■

Alternative Proof of the Lemma for $K = \overline{\mathbb{Q}}$, using Algebraic Number Theory

Here is an alternative proof, which in this case is less efficient than the first one but that we still present because it is neat. Using an argument similar to Exercise 8.7.29†, one can also adapt it to work over any characteristic zero field. Consider an N such that $g_1(N), \ldots, g_k(N) \neq 0$. Pick a large prime p such that g_i and β_i make sense modulo p, using Theorem 6.4.1 and write $u_n \equiv \sum_i g_i'(n)\beta_i^{n\prime}$ where $g_i' \in \overline{\mathbb{F}}_p[X]$ and $\beta_i' \in \overline{\mathbb{F}}_p$. By picking p sufficiently large, suppose also that $p \nmid g_i'(N), \beta_i'$ for each i.

Since the order of β_i' is coprime with p (it divides $p^m - 1$ for some m), using CRT we can choose an M such that $\beta_i^{M\prime} = 1$ for each i and $g_i'(M) = g_i'(N)$. Thus we have $\sum_i g_i'(N)\beta_i^{n\prime} = 0$ for all n. By Vandermonde C.3.2 this implies

$$\prod_{i \neq j} \beta_i - \beta_j \equiv \prod_{i \neq j} \beta_i' - \beta_j' = 0.$$

Since this is true for infinitely many primes, the LHS is zero too, i.e. $\beta_i = \beta_j$ for some $i \neq j$.

■

Remark 8.5.3

Note that we again proved a global statement in a local way, although we only used finite fields instead of p-adic numbers here. Results like Exercise 8.7.29† prove that we can even prove results about $\mathbb{C}$ that seem analytic or algebraic in nature with number theory. In fact, the only known proofs of Skolem-Mahler-Lech are p-adic in essence.

Remark 8.5.4

It is interesting to note that our proof of the Skolem-Mahler-Lech is *non-effective*. We can find the common difference of the arithmetic progressions if the sequence has infinitely many zeros,

although our proof is not excellent for this because we chose to work $\mathbb{Q}_p$ instead of finite extensions of $\mathbb{Q}_p$, and we can also bound the size of the additional finite set with Theorem 8.6.1, but we cannot decide if a linear recurrence has a zero or not. This defect is shared by all known proofs.

Remark 8.5.5

Our bound on the common difference of the arithmetic progressions is very weak because we do not know how big the least prime such that every exists in $\mathbb{F}_p$ is. Using finite extensions of $\mathbb{Q}_p$ and the theory of finite fields, one can get a way better bound, as we can now choose the smallest p such that the algebraic numbers are non-zero in $\overline{\mathbb{F}}_p$ (see **??** for how to extend the p-adic absolute value to finite extensions).

8.6 Strassmann's Theorem

Our previous method of showing an analytic function had finitely many zeros on $\mathbb{Z}_p$ did not proving any actual bound, so we will fix that here. With the bounds we get, in some situations we will be able to determine all zeros of certain linear recurrences, and solve certain diophantine equations thanks to them.

Theorem 8.6.1 (Strassmann's Theorem)

Let $f(x) = \sum_{k=0}^{\infty} a_k x^k$ be a non-zero power series convergent on $\mathbb{Z}_p$, i.e. $a_k \to 0$. Suppose N is maximal such that $|a_N|_p := \max(|a_n|_p)$, i.e. $|a_N|_p > |a_n|_p$ for $n > N$, and $|a_N|_p \geq |a_n|_p$ for $n \leq N$. Then f has at most N zeros.

Notice that such an N always exists, for otherwise $a_k \not\to 0$.

Proof

We proceed by induction on N. When $N = 0$,

$$|f(x)|_p \leq \max(|a_i x^i|_p) = |a_0|_p$$

by the strong triangle inequality 8.2.1 since $|a_0|_p > |a_i|_p \geq |a_i x^i|_p$ for any $i > 0$. Moreover, the maximum is achieved only once so we have $|f(x)|_p = |a_0|_p$ for all $x \in \mathbb{Z}_p$ so f never vanishes (if $a_0 = 0$ then $f = 0$ since it's the maximum coefficient, which is impossible).

Now, suppose $N \geq 1$ is maximal such that $|a_N|_p = \max(|a_n|_p)$. Suppose $\alpha \in \mathbb{Z}_p$ is a zero of f, if there is none we are already done. Write

$$\begin{aligned} f(x) &= f(x) - f(\alpha) \\ &= \sum_{i=0}^{\infty} a_i x^i - \sum_{i=0}^{\infty} a_i \alpha^i \\ &= \sum_{i=0}^{\infty} a_i (x^i - \alpha^i) \\ &= (x-\alpha)^i \sum_{i=0}^{\infty} \sum_{j=0}^{i-1} a_i x^j \alpha^{i-j-1} \\ &= (x-\alpha)^i \sum_{j=0}^{\infty} x^j \sum_{i=j+1}^{\infty} a_i \alpha^{i-j-1}. \end{aligned}$$

using Proposition 8.3.4. Let

$$b_j = \sum_{i=j+1}^{\infty} a_i \alpha^{i-j-1}$$

and define

$$g(x) = \sum_{k=0}^{\infty} b_k x^k$$

so that $f(x) = (x-\alpha)g(x)$ for $x \in \mathbb{Z}_p$.

We shall prove that $|b_{N-1}|_p > |b_n|_p$ for $n > N-1$, and $|b_{N-1}|_p \geq |b_n|$ for $n \leq N$, that way g will have at most $N-1$ zeros by the induction hypothesis so f at most N. Note that

$$b_{N-1} = a_N + \alpha a_{N+1} + \alpha^2 a_{N+2} + \dots$$

so that $|b_{N-1}|_p = |a_N|_p$ by the strong triangle inequality. For $n \neq N-1$, we have

$$|b_n|_p = |a_{n+1} + \alpha a_{n+2} + \alpha^2 a_{n+3} + \dots|_p \leq \max_{i>n}(|a_i \alpha^i|_p) \leq \max_{i>n}(|a_i|_p) \leq |a_N|_- = |b_{N-1}|_p$$

and this inequality is strict for $n > N-1$ since we then have $|a_i|_p < |a_N|_p$ for $i \geq n+1 > N$.

■

Here is an application from [7], very hard to solve by elementary means (which would be in essence p-adic anyway).

Proposition 8.6.1 (Ramanujan, Nagell)

The positive integers n such that

$$x^2 + 7 = 2^n$$

has a solution in $\mathbb{Z}$ are $n \in \{3, 4, 5, 7, 15\}$.

Proof

First, let's analyse this equation in $\mathbb{Q}(\sqrt{-7})$. By Exercise 8.6.1, it is Euclidean so a UFD. Suppose (x, n) is a solution; clearly x is odd. We get

$$\frac{x+\sqrt{-7}}{2} \cdot \frac{x-\sqrt{-7}}{2} = 2^{n-2}$$

and the prime factorisation of 2 is $\frac{1+\sqrt{-7}}{2} \cdot \frac{1-\sqrt{-7}}{2}$. Let $\alpha = \frac{1+\sqrt{-7}}{2}$ and $\beta = \frac{1-\sqrt{-7}}{2}$. Since $\frac{1\pm\sqrt{-7}}{2}$ isn't divisible by 2, we must have (Exercise 8.6.2)

$$\frac{x \pm \sqrt{-7}}{2} = \alpha^{n-2}.$$

This has a solution if and only if

$$\frac{\alpha^{n-2} - \beta^{n-2}}{\alpha - \beta} = \pm 1.$$

The LHS is a linear recurrence which we will denote by $(u_{n-2})_{n \geq 0}$.

Now, let's try to find a p-adic field where $\sqrt{-7}$ exists. Since $-7 \equiv 2^2 \pmod{11}$ we can work in $\mathbb{Q}_{11}$. By Hensel's lemma, there are two roots of $X^2 - X + 2$ (this is the characteristic polynomial of the sequence) which we will abusively call α and β again. One of the roots is congruent to 16 modulo 11^2, say α, and the other one is $\beta = 1 - \alpha \equiv 106 \pmod{11^2}$.

Let $r \in \{0, 1, \ldots, 9\}$ be an integer. Since $a = \alpha^{10} - 1 \equiv 99 \pmod{11^2}$ and $b = \beta^{10} - 1 \equiv 77 \pmod{11^2}$ are divisible by 11, the functions $s \mapsto u_{r+10s}$ are analytic. Let's find out how many times they can be ± 1. Expand $(\alpha - \beta)(u_{r+10s} \pm 1)$ as a power series in s:

$$\begin{aligned}(\alpha - \beta)(u_{r+10s} \pm 1) &= \alpha^r(1+a)^s - \beta^r(1+b)^s \pm (\alpha - \beta) \\ &= \alpha^r \sum_k \binom{s}{k} a^s - \beta^r \sum_k \binom{s}{k} b^s \pm (\alpha - \beta) \\ &\equiv \alpha^r(1+as) - \beta^r(1+bs) \pm (\alpha - \beta) \pmod{11^2}.\end{aligned}$$

An easy computation shows that the Strassmann bounds are $N = 1$ for $r \in \{1, 2, 5\}$ and $N = 0$ for $r \in \{0, 4, 6, 7, 8, 9\}$. For $r = 3$, by expanding one more term, we find that the Strassmann bound is $N = 2$. Since we have exactly this many solutions ($r + 10s \in \{1, 2, 3, 5, 13\}$), we are done as they correspond to $n \in \{3, 4, 5, 7, 15\}$. (Technically we have to consider 20 functions because of the ± 1 sign, but it is easy to see that only the $+$ sign works for $r \in \{1, 2\}$, only the $-$ sign works for $r \in \{3, 5\}$, and none of them do for other r.)

■

Exercise 8.6.1. Prove that $\mathbb{Q}(\sqrt{-7})$ is norm-Euclidean. (This is also Exercise 2.6.4†.)

Exercise 8.6.2. Prove that, if $x^2 + 7 = 2^n$, then $\frac{x \pm \sqrt{-7}}{2} = \left(\frac{1+\sqrt{-7}}{2}\right)^{n-2}$ for some choice of $\pm$.

Exercise 8.6.3*. Compute the Strassmann bounds for the function $s \mapsto (\alpha - \beta)(u_{s+10r} \pm 1)$, for each $r \in \{0, 1, \ldots, 9\}$. (If you do not want to do it all by hand, you may use a computer. In any case, it is better to do it to have a feel for why it works because it's very cool.)

Exercise 8.6.4. Prove that $3, 4, 5, 7, 15$ are indeed solutions to the given equation. (You may use a computer for $n = 15$.)

8.7 Exercises

Analysis

Exercise 8.7.1† (Vandermonde's Identity)**.** Let x and y be p-adic integers. Prove that

$$\binom{x+y}{k} = \sum_{i+j=k, i,j \geq 0} \binom{x}{i}\binom{y}{j}$$

for any k.

Exercise 8.7.2† (Mahler's Theorem)**.** Prove that a function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is continuous if and only if there exist $a_i \to 0$ such that

$$f(x) = \sum_{i=0}^{\infty} a_i \binom{x}{i}$$

for all $x \in \mathbb{Z}_p$. These a_i are called the *Mahler coefficients* of f. Moreover, show that $\max(|f(x)|_p) = \max(|a_i|_p)$.

Exercise 8.7.3 (USA TST 2011)**.** We say a sequence $(z_n)_{n \geq 0}$ is a *p-pod* if

$$v_p\left(\sum_{k=0}^{m} (-1)^k \binom{m}{k} z_k\right) \to \infty.$$

Prove that if $(a_n)_{n \geq 0}$ and $(b_n)_{n \geq 0}$ are p-pods then $(a_n b_n)_{n \geq 0}$ is too.

Exercise 8.7.4†. Prove that the following power series converge if and only if for $|x|_p < 1$ and $|x|_p < p^{-1/(p-1)}$ respctively:

$$\log_p(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}x^k}{k}, \ \exp_p(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!}.$$

In addition, prove that

1. $\exp_p(x+y) = \exp_p(x)\exp_p(y)$ for $|x|_p, |y|_p < p^{-1/(p-1)}$.
2. $\log_p(xy) = \log_p(x) + \log_p(y)$ for $|x|_p, |y|_p < 1$
3. $\exp_p(\log(1+x)) = 1+x$ for $|x|_p < p^{-1/(p-1)}$.
4. $\log_p(\exp(x)) = x$ for $|x|_p < p^{-1/(p-1)}$.

Exercise 8.7.5†. Prove that

$$v_2\left(\sum_{k=1}^{n} \frac{2^k}{k}\right) \to \infty.$$

Exercise 8.7.6† (Mean Value Theorem)**.** Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$ be a p-adic power series converging for $|x|_p \leq 1$, i.e. $a_i \to 0$. Prove that

$$|f(t+h) - f(t)|_p \leq |h|_p \max_i(|a_i|_p)$$

for any $|t|_p \leq 1$ and $|h|_p \leq p^{-1/(p-1)}$.

Absolute Values

Exercise 8.7.7†. We say an absolute value $|\cdot|$ over a field K, i.e. a function $|\cdot| \to \mathbb{R}_{\geq 0}$ such that

- $|x| = 0 \iff x = 0$
- $|x+y| \leq |x| + |y|$
- $|xy| = |x| \cdot |y|$

is *non-Archimedean* if the sequence $|m| \leq 1$ for all $m \in \mathbb{Z}$ and *Archimedean* otherwise. Prove that m is non-Archimedean if and only if it satisfies the strong triangular inequality $|x+y| \leq \max(|x|, |y|)$ for all $x, y \in K$. In addition, prove that, if $|\cdot|$ is non-Archimedean, we have $|x+y| = \max(|x|, |y|)$ whenever $|x| \neq |y|$.

Exercise 8.7.8†. Let K be a field and let $|\cdot| : K \to \mathbb{R}_{\geq 0}$ be a multiplicative function which is an absolute value on $\mathbb{Q}$. Suppose that $|\cdot|$ satisfies the modified triangular inequality $|x+y| \leq c(|x| + |y|)$ for all $x, y \in K$, where $c > 0$ is some constant. Prove that it satisfies the triangular inequality.

Exercise 8.7.9† (Ostrowski's Theorem)**.** Let $|\cdot|$ be an absolute value of $\mathbb{Q}$. Prove that $|\cdot|$ is equal to $|\cdot|_p^r$ for some prime p and some $r \geq 1$, or to $|\cdot|_\infty^r$ for some $0 < r \leq 1$ or is the trivial absolute value $|\cdot|_0$ which is 0 at 0 and 1 everywhere else.

Exercise 8.7.10† (Bolzano-Weierstrass Theorem)**.** Prove that a set $S \subseteq \mathbb{R}^n$ is sequentially compact if and only if it closed, meaning that any sequence of elements of S converging in $\mathbb{R}^n$ (for the Euclidean distance) converges in S, and bounded.

Exercise 8.7.11† (Extremal Value Theorem)**.** Let M be a *metric space*, i.e. a set with a distance $d : M \to \mathbb{R}_{\geq 0}$ such that $d(x,y) = 0$ iff $x = y$, $d(x,y) = d(y,x)$ (commutativity) and $d(x,y) \leq d(x,z) + d(z,y)$ (triangle inequality) for any $x, y, z \in M$ and let S be a sequentially compact subset of M. Suppose $f : S \to \mathbb{R}$ is a continuous function. Prove that f has a maximum and a minimum.

Exercise 8.7.12† (Equivalence of Norms)**.** Let $(K, |\cdot|)$ be a complete valued field in characteristic 0, i.e. a field with an absolute value $|\cdot|$ which is complete[10] for the distance induced by this absolute value. A *norm* on a vector space V over K is a function $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ such that

- $\|x\| = 0 \iff x = 0$
- $\|x + y\| \leq \|x\| + \|y\|$
- $\|ax\| = |a|\|x\|$

for all $x, y \in V$ and $a \in K$. We say two norms $\|\cdot\|_2$ and $\|\cdot\|_2$ are *equivalence of norms* if there are two positive real numbers c_1 and c_2 such that $\|x\|_1 \leq c_1\|x\|_2$ and $\|x\|_2 \leq c_2\|x\|_1$ for all $x \in V$.[11] Prove that any two norms are equivalent over a finite-dimensional K-vector space V. In addition, prove that V is complete under the induced distance of any norm $\|\cdot\|$.

Exercise 8.7.13†**.** Let $K = \mathbb{Q}_p$ be a local field[12], where p be a prime number or ∞ and let L be a finite extension of K. Prove that there is only one absolute value of L extending $|\cdot|_p$ on K, and that it's given by $|\cdot|_p = \left|N_{L/K}(\cdot)\right|_p^{1/[L/K]}$.[13][14][15]

Exercise 8.7.14†**.** Let $(K, \cdot)$ be a complete valued field in characteristic 0 and let $f \in K[X]$ be a polynomial. Prove that f either has a root in K, or there is a real number $c > 0$ such that $|f(x)| \geq c$ for all $x \in K$.

Exercise 8.7.15† (Ostrowski)**.** Let $(K, \cdot)$ be a complete valued Archimedean field in characteristic 0[16]. Prove that it is isomorphic to to $(\mathbb{R}, |\cdot|_\infty)$ or $(\mathbb{C}, |\cdot|_\infty)$.

Diophantine Equations

Exercise 8.7.16† (Brazilian Mathematical Olympiad 2010)**.** Find all positive rational integers n and x such that $3^n = 2x^2 + 1$.

Exercise 8.7.17 (Taiwan TST 2021)**.** Find all triples of positive rational integers (x, y, z) such that

$$x^2 + 4^y = 5^z.$$

Exercise 8.7.18. Prove that the equation $x^3 + 11y^3 = 1$ has no non-trivial rational integer solutions.

Exercise 8.7.19†**.** Solve the diophantine equation $x^2 - y^3 = 1$ over $\mathbb{Z}$.

Exercise 8.7.20† (Lebesgue)**.** Solve the equation $x^2 + 1 = y^n$ over $\mathbb{Z}$, where $n \geq 3$ is an odd integer.

Exercise 8.7.21†**.** Solve the equation $x^2 + 1 = 2y^n$ over $\mathbb{Z}$, where $n \geq 3$ is an odd integer.

[10] Recall that completeness means that all Cauchy sequences converge. A Cauchy sequence $(u_n)_{n\geq 0}$ is a sequence such that, for any $\varepsilon > 0$, there is an N such that $|u_m - u_n| \leq \varepsilon$ for all $m, n \geq N$.

[11] This means that they induce the same topology on V.

[12] This result is true for any complete valued field $(K, |\cdot|)$, but it is harder to prove.

[13] In particular, this absolute value is still non-Archimedean if it initially was. For instance, by Exercise 8.7.7†, if p is prime, the extension of $|\cdot|_p$ still satisfies the strong triangle inequality. In fact, this is the only interesting case since it's too hard to treat the case $K = \mathbb{R}$ separately.

[14] Here is why this absolute value is intuitive: by symmetry between the conjugates, we should have $|\alpha|_p = |\beta|_p$ if α and β are conjugates. Taking the norm yields $|N_{K/\mathbb{Q}_p}(\alpha)|_p = |\alpha|_p^{[K:\mathbb{Q}_p]}$ as indicated.

[15] One might be tempted to also define a p-adic valuation for elements of K as $v_p(\cdot) = -\log(|\cdot|_p)/\log(p)$, and this is also what we will do in some of the exercises. However, we warn the reader that, if $\alpha \in \overline{\mathbb{Z}}$ is an algebraic integer and α_p is a root of its minimal polynomial in $\overline{\mathbb{Q}_p}$, $v_p(\alpha_p) \geq 1$ does not mean anymore that p divides α in $\overline{\mathbb{Z}}$, it only means that p divides α_p in $\overline{\mathbb{Z}_p} := \{x \in \overline{\mathbb{Q}_p} \mid |x|_{\leq} 1\}$.

[16] In fact it is quite easy to show that $\operatorname{char} K = 0$ follows from the assumption that $|\cdot|$ is Archimedean, but we add this assumption for the convenience of the reader.

Linear Recurrences

Exercise 8.7.22†. Let $(u_n)_{n\geq 0}$ be a linear recurrence of rational integers given by $\sum_i f_i(n)\alpha_i^n$ such that α_i/α_j is not a root of unity for $i \neq j$. If u_n is not of the form $a\alpha^n$ for some $a, \alpha \in \mathbb{Z}$, prove that there are infinitely many prime numbers p such that $p \mid u_n$ for some integer $n \geq 0$.

Exercise 8.7.23†. Does there exists an unbounded linear recurrence $(u_n)_{n\geq 0}$ such that u_n is prime for all n?

Miscellaneous

Exercise 8.7.24†. Which roots of unity are in $\mathbb{Q}_p$?

Exercise 8.7.25. Any p-adic number can be written uniquely in the following way: $a = \sum_{k>N} a_k p^k$ for some $N \in \mathbb{Z}$ and $a_k \in [p]$ (this amounts to choosing a system of representents of $\mathbb{Z}/p\mathbb{Z}$). Prove that $a \in \mathbb{Q}$ if and only if the sequence $(a_k)_k$ is eventually periodic.

Exercise 8.7.26 (ISL 2020)**.** Find all functions $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{\geq 0}$ such that $f(xy) = f(x) + f(y)$ for every integers $x, y > 0$ and for which there are infintely many $n \in \mathbb{N}$ satisfying $f(k) = f(n-k)$ for every integer $0 < k < n$.

Exercise 8.7.27† (China TST 2010)**.** Let $k \geq 1$ be a rational integer. Prove that, for sufficiently large n, $\binom{n}{k}$ has at least k distinct prime factors.

Exercise 8.7.28†. Find all additive functions $f : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}$, where addition is defined componentwise. (To those who have read Section C.2, the fact that there are a nice characterisation of those functions should come off as a surprise.)

Exercise 8.7.29†. Prove that the Skolem-Mahler-Lech theorem holds over any field of characteristic zero.

Appendix A

Polynomials

Prerequisites for this chapter: none.

A.1 Fields and Polynomials

Definition A.1.1 (Field)

A *field* $(K, +, \cdot)$ is a set K with at least two elements and with two operations $+$ and $\cdot$, called addition and multiplication. These operations have the following properties: they are associative and commutative, they have inverses, they have an identity (except for 0, it doesn't have a multiplicative inverse), and multiplication distributes over addition. We usually just say that K is a field by abuse of terminology.

Here is what these terms mean: an operation $\dagger : K^2 \to K$ is *associative* if $(a \dagger b) \dagger c = a(b \dagger c)$ for any $a, b, c \in K$ (that way we can write $a \dagger b \dagger c$ without ambiguity).

It is *commutative* if $a \dagger b = b \dagger a$ for any $a, b \in K$.

It has an identity e if $a \dagger e = e \dagger a = a$ for any $a \in K$ (this is denoted 0_K for addition and 1_K for multiplication, but we usually drop the K when the context is clear).

a' is an inverse of a for $\dagger$ if $a \dagger a' = a' \dagger a = e$ (denoted $-a$ for addition and a^{-1} for multiplication).

$+$ distributes over $\cdot$ if $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$, where ab denotes $a \cdot b$.

Exercise A.1.1*. Let K be a field. Prove that $0_K a = 0_K$ for any $a \in K$.

Exercise A.1.2*. Let $\dagger$ be a binary (taking two arguments) associative operation on a set M. Suppose that M has an identity. Prove that it is unique. Similarly, prove that, if an element $g \in M$ has an inverse, then it is unique.[1]

Remark A.1.1

Note that a field must have at least two elements (the additive and multiplicative identities must be distinct), i.e. the trivial ring $R = \{0\}$ is not a field. There are various reasons for this axiom, akin to the convention that 1 isn't prime, but perhaps the simplest one is that if it were a field we would not have the uniqueness of dimension anymore since $\{0\}$ and the empty set are both bases of $\{0\}$. (This is unimportant for this appendix, see Appendix C for the definition of dimension.)

Here are some examples of fields: the familiar sets of rational numbers $\mathbb{Q}$, of real numbers $\mathbb{R}$ and of complex numbers $\mathbb{C}$. We will define a variety of other fields throughout this book, but here is one very important field: the fields $\mathbb{F}_p$ of integers modulo p, where p is a prime. You can think of it

[1] Such a structure is called a *monoid*.

as $\{0, 1, \ldots, p-1\}$ with addition and multiplication modulo p. It differs greatly from the previous fields for two reasons: because it is *finite* (we will study these fields in Chapter 4) and because it has *non-zero characteristic*[2] (see Section A.2 for a definition if you're curious, but this is unimportant for now). Why is it a field? Well, all axioms are obvious because they are true in $\mathbb{Z}$ so also in $\mathbb{Z}$ modulo p, **except** the one about multiplicative inverses. But you already know that integers which are not divisible by p have inverses modulo p since it's prime.

We now define polynomials with coefficients in a field K.

Definition A.1.2 (Polynomials)

A *polynomial* f with coefficients in K is a object $f = a_n X^n + \ldots + a_1 X + a_0$ where $a_0, \ldots, a_n \in K$. The greatest k such that $a_k \neq 0$ is called the *degree* $\deg f$ of f; the degree of the zero polynomial $\deg 0$ is $-\infty$. The set of polynomials with coefficients in K is denoted $K[X]$.

The coefficient $a_{\deg f}$ is called the *leading coefficient* of f, and a_0 is the *constant coefficient* of f. When the leading coefficient is 1, we say the polynomial is *monic* (the zero polynomial isn't monic).

Remark A.1.2

We can also consider similar objects but without the restriction that $a_k = 0$ for sufficiently large k. They are called *formal power series*. They are also very useful objects, but are not considerably used in algebraic number theory so we do not consider them here (two exceptions: see Theorem B.2.1 and Remark C.4.1). Another point to note is that, although one can obtain many very interesting results by purely formal and algebraic considerations, we lose one advantage of polynomials: we can not always evaluate them (since the resulting series might not converge, or worse, we might not even have a topology to consider convergence). Thus, they demand a bit more care if we want to do that. See Andreescu-Dospinescu [1] chapter 8 for an introduction to the wonders of formal power series.

The sum and product of two polynomials are defined intuitively, I don't think I have to explain that. The formal object X will be called a "variable", even if that makes it seem like it's not a formal object.[3] Polynomials in multiple variables are defined analogously as

$$\sum_{i_1, \ldots, i_m \geq 0} a_{i_1, \ldots, i_m} X_1^{i_1} \cdot \ldots \cdot X_k^{i_m}$$

where all but finitely many $a_{i_1, \ldots, i_m}$ are zero. The degree is now defined as the greatest value of $i_1 + \ldots + i_m$ for non-zero $a_{i_1, \ldots, i_m}$.

Exercise A.1.3*. Prove that multiplication of polynomials is associative and commutative.

A polynomial is **not** a polynomial function! A polynomial is a purely formal object: for instance the polynomial functions $x \mapsto x^p$ and $x \mapsto x$ are the same over the integers modulo p by Fermat's little theorem, but the polynomials X^p and X are distinct. That said, we can still consider them as polynomial functions when we want to (to evalute polynomials at a point for instance), but it is also important to be able to consider them only as polynomials (e.g. for Corollary A.1.1).

Here is why fields are nice: they are precisely the structure that lets us define polynomials (and be able to add them and multiply them nicely) as well as have a Euclidean division.

Proposition A.1.1 (Euclidean Division of Polynomials)

Let $f, g \in K[X]$ be polynomials, with $g \neq 0$. There exists polynomials $q, r \in K[X]$ with $\deg r < \deg g$ such that $f = gq + r$.

[2] This is a consequence of its finiteness, but it has important consequences too which explains why it is mentioned.
[3] The technical term is "indeterminate" but I prefer using "variable".

Proof

Start with the uniqueness part. If $gq+r = f = gq'+r'$, then $(q-q')g = r'-r$ and $q \neq q'$. Thus, $\deg(q-q')g \geq \deg g > \deg r' - r$ which is impossible.

We now proceed by induction on $\deg f$ to prove the existence, for a fixed g. If $\deg f < \deg g$, we already done: $f = g \cdot 0 + f$. Otherwise, let a and b be the leading coefficients of f and g respectively, which are non-zero since $\deg f \geq \deg g \geq 0$. The polynomial $f - ab^{-1}X^{\deg f - \deg g}g$ has degree less than $\deg g$, so by the induction hypothesis there exist polynomials q and r such that $\deg r < \deg g$ and

$$f - ab^{-1}X^{\deg f - \deg g}g = gq + r$$

Finally, this gives us

$$f = (q + ab^{-1}X^{\deg f - \deg g})g + r.$$

■

We now define divisibility of polynomials like we do in $\mathbb{Z}$:

Definition A.1.3 (Divisibility of Polynomials)

We say a polynomial $f \in K[X]$ *divides* a polynomial $g \in K[X]$, and write $f \mid g$, if there exists a polynomial $h \in K[X]$ such that $g = fh$.

Note that repeated applications of the Euclidean remainder yields the *Euclidean algorithm*: given two polynomials $f, g \in K[X]$ with $\deg f > \deg g$, we iteratively replace f by the remainder of its division by g. For instance, $f = X^3 + X$ and $g = X^2$ yields

$$\{X^3 + X, X^2\} \to \{X^2, X\} \to \{X, 0\} \to \{0, 0\}.$$

This will, like in $\mathbb{Z}$,[4] eventually produce the pair $\{0, h\}$ where h is the *greatest common divisor* (gcd) of f and g, i.e. a polynomial which divides both f and g, and such that, if $h' \mid f, g$ then $h' \mid h$ (in particular it is the common divisor with greatest degree, except when $f = g = 0$). Note that the gcd is only defined up to multiplication by a non-zero constant, although we will usually assume it to be monic.

Exercise A.1.4*. Prove that the gcd of 0 and 0 is 0.

Exercise A.1.5*. Prove that the Euclidean algorithm produces the gcd. Deduce that the gcd of two polynomials in $K[X]$ is also in $K[X]$. (As a consequence, the fundamental theorem of algebra Theorem A.1.1 implies that two polynomials with rational coefficients are coprime in $\mathbb{Q}[X]$ if and only if they have a common complex root.)

Exercise A.1.6* (Bézout's Lemma)**.** Consider two polynomials $f, g \in K[X]$. Prove that there exist polynomials $u, v \in K[X]$ such that $uf + vg = \gcd(f, g)$.

As another corollary of Proposition A.1.1, we get the following **extremely fundamental** fact.

Proposition A.1.2*

Let $f \in K[X]$ be a polynomial. If $f(\alpha) = 0$, then $X - \alpha \mid f$.

[4] The deep reason behind all these analogies with $\mathbb{Z}$ lies in Chapter 2: both $\mathbb{Z}$ and $K[X]$ are Euclidean domains.

Proof

Let $f = (X - \alpha)q + r$ be the Euclidean division of f by $X - \alpha$. Since $\deg X - \alpha = 1$, we have $\deg r < 1$ so r is constant. Notice that $r = r(\alpha) = f(\alpha) = 0$, which means $f = (X - \alpha)q$, i.e. $X - \alpha$ divides f.

■

Corollary A.1.1*

A polynomial $f \in K[X]$ of degree $n \geq 0$ has at most n roots in K.

Proof

Suppose for the sake of a contradiction that f had $n + 1$ roots $\alpha_1, \ldots, \alpha_{n+1}$. Using Proposition A.1.2 repeatedly, we get $f = (X - \alpha_1)f_1$, $f_1 = (X - \alpha_2)f_2$, ..., $f_n = (X - \alpha_{n+1})f_{n+1}$ so that

$$f = (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_{n+1})f_{n+1}.$$

Since f is non-zero, the degree of f_{n+1} is non-negative so $n = \deg f = n + 1 + \deg f_{n+1} \geq n + 1$ which is a contradiction.

■

Exercise A.1.7*. Let $f \in K[X_1, \ldots, X_n]$ be a polynomial in n variables and suppose $S_1, \ldots, S_n \subseteq K$ are subsets of K such that $|S_i| > \deg_{X_i} f$. If f vanishes on $S_1 \times \ldots \times S_n$, prove that $f = 0$. (This is the generalisation of Corollary A.1.1 to multivariate polynomials.)

Here is a non-trivial application of this.

Problem A.1.1

Let $n \geq 2$ be a positive integer. What is the gcd of the numbers $1^n - 1, 2^n - 1, \ldots, n^n - 1$?

Solution

Let d be this gcd. Suppose p is a prime factor of d. If $p \leq n$, then $p \mid p^p - 1$ which is impossible. Thus $p > n$. Consider the polynomial

$$X^n - 1 - (X - 1) \cdot \ldots \cdot (X - n)$$

in $\mathbb{F}_p[X]$. It has degree at most $n - 1$ and n roots (in $\mathbb{F}_p$) by assumption, thus it is the zero polynomial. Hence we have

$$X^n - 1 \equiv (X - 1) \cdot \ldots \cdot (X - n) \pmod{p}.$$

Expand the RHS and consider the coefficient of X^{n-1}: it is $-(1 + \ldots + n) = -\frac{n(n+1)}{2}$. On the other hand, since $n \geq 2$, the coefficient of X^{n-1} of the LHS is 0. Thus

$$p \mid \frac{n(n+1)}{2}.$$

Since $p > n$, this means $p = n + 1$. Thus, if $n + 1$ is composite we are already done: the gcd is 1. If $n + 1 = p$ is prime, the gcd d is a power of p and we must find out what it is. Clearly, p is odd.

By Fermat's little theorem, $p \mid k^n - 1$ for $k = 1, \ldots, n$ so $p \mid d$. It remains to prove that $p^2 \nmid d$. For this, suppose for the sake of a contradiction that $p^2 \mid (p-1)^{p-1} - 1$. Then,

$$p \mid \frac{(p-1)^{(p-1)} - 1}{(p-1)^2 - 1} = \sum_{k=0}^{\frac{p-1}{2}-1} (p-1)^{2k} \equiv \frac{p-1}{2} \pmod{p}$$

which is a contradiction so we are done in this case too: $d = n+1$ if it is prime and 1 otherwise. ■

In particular, notice that $X^{p-1} - 1 = (X-1) \cdot \ldots \cdot (X-(p-1))$ in $\mathbb{F}_p$ which will be important for Chapter 4.

Proposition A.1.2 motivates us to make the following definition.

Definition A.1.4 (Multiple Root)

We say α is a root of *multiplicity* m if $(X-\alpha)^m \mid f$ but $(X-\alpha)^{m+1} \nmid f$. The multiplicity of α is denoted $v_\alpha(f)$.

Definition A.1.5 (Derivative)

The (formal) *derivative* of a polynomial $f = \sum_{i \geq 0} a_i X^i \in K[X]$ is $f' = \sum_{i \geq 1} i a_i X^{i-1}$. The nth derivative of f is denoted $f^{(n)}$ ($f^{(0)} = f$).

Exercise A.1.8*. Prove that $(fg)' = f'g + gf'$ and $(f+g)' = f' + g'$ for any $f, g \in K[X]$. Show also that $(f^n)' = nf'f^{n-1}$ for any positive integer n, where f^k denotes the kth power and not the kth iterate. More generally, show that

$$\left(\prod_{i=1}^{n} f_i\right)' = \sum_{i=1}^{n} f_i' \prod_{j \neq i} f_j.$$

We can now give a criterion to compute the multiplicity of a root, using our notion of derivative. This will however only work as long as the *characateristic* $\operatorname{char} K$ of K is greater than the multiplicity of the root. Roughly speaking, the characteristic $c \in \mathbb{N}$ is the smallest positive number such that $c = 0$ in K if there exists one, and 0 otherwise. See Definition A.2.3 for a more rigorous definition. For instance, the characteristic of $\mathbb{F}_p$ is p while the characteristic of $\mathbb{Q}$ is 0.

Proposition A.1.3 (Multiple Roots)*

Let $f \in K[X]$ be a polynomial. If $\operatorname{char} K = 0$, for any positive integer m and any $\alpha \in K$, we have $(X-\alpha)^m \mid f$ if and only if

$$f(\alpha) = f'(\alpha) = \ldots = f^{(m-1)}(\alpha) = 0.$$

Otherwise, this only holds for $m < \operatorname{char} K$.

Here is how this theorem can fail when $v_\alpha(f) \geq c$: the derivative of $f = X^p$ over $\mathbb{F}_p$ is $pX^{p-1} = 0$, so $f^{(k)}(0) = 0$ for all $k \in \mathbb{N}$ yet X^p is clearly not divisible by X^k for all $k \in \mathbb{N}$.

Proof

We proceed by induction on m. The base case is Proposition A.1.2. We shall prove that, if $f(\alpha) = 0$, $v_\alpha(f') = v_\alpha(f) - 1$.

Let $m = v_\alpha(f) \geq 1$. Write $f = (X-\alpha)^m g$ where $X - \alpha \nmid g$. Then, by Exercise A.1.8*, $f' = m(X-\alpha)^{m-1}g + (X-\alpha)^m g'$ which is indeed divisible by $(X-\alpha)^{m-1}$ but not $(X-\alpha)^m$ as $X - \alpha \nmid g$. Here, we used the fact that m is non-zero because it is positive but less than the characteristic.

■

Using our notion of multiple roots, we get that if f has degree n, leading coefficient a, and roots $\alpha_1, \ldots, \alpha_n$ (not necessarily distinct, we count them with multiplicity) then $(X-\alpha_1)\cdot\ldots\cdot(X-\alpha_n) \mid f$ so that

$$f = (X-\alpha_1)\cdot\ldots\cdot(X-\alpha_n)g$$

for some g which must be constant equal to a by looking at the degrees. We have factorised the polynomial with its roots. The following proposition shows that we can recover the coefficients from the roots using this factorisation.

Proposition A.1.4 (Vieta's Formulas)*

Suppose $f = a_0 + \ldots + a_{n-1}X^{n-1} + X^n$ is a monic polynomial of degree n with roots $\alpha_1, \ldots, \alpha_n$ (counted with multiplicity). Then,

$$a_{n-k} = (-1)^k \sum_{i_1 < \ldots < i_k} \alpha_{i_1} \cdot \ldots \cdot \alpha_{i_k}$$

for any $k = 0, \ldots, n-1$.

Proof

It is simply the expansion of $f = (X-\alpha_1)\cdot\ldots\cdot(X-\alpha_n)$.

■

In particular, $a_0 = (-1)^n\alpha_1\cdot\ldots\cdot\alpha_n$ and $a_{n-1} = -(\alpha_1 + \ldots + \alpha_n)$. We have in fact already used a special case of these formulas in Problem A.1.1. Here are two more applications of this, to show how useful it is.

Corollary A.1.2 (Wilson's Theorem)

For any prime p, $(p-1)! \equiv -1 \pmod{p}$.

Proof

We have already seen that $1, 2, \ldots, p-1$ are exactly the roots of $X^{p-1} - 1$ in $\mathbb{F}_p$ by Fermat's little theorem. Thus, their product is $(-1)^{p-1}\cdot(-1)$ by Vieta's formulas as -1 is the constant coefficient of $X^{p-1} - 1$. This means that $(p-1)! \equiv (-1)^p \equiv -1 \pmod{p}$ as wanted (when p is odd it's clear and when $p = 2$ we have $1 = -1$).

■

Problem A.1.2 (APMO 2014 Problem 3)

Find all positive integers n such that for any integer k there exists an integer a for which a^3+a-k is divisible by n.

(Partial) Solution

This is equivalent to $x \mapsto x^3 + x$ being bijective modulo n. In particular, if it is bijective modulo n it is bijective modulo any prime factor $p \mid n$. We will show that $p = 3$. This will imply that n is a power of 3, and conversely all powers of 3 work but we have not established the tools to prove this yet. It will be proven in Chapter 5 a consequence of Hensel's lemma 5.3.1. Clearly $p = 2$ doesn't work as $2 \mid 0^3 + 0, 1^3 + 1$ so p must be odd.

Thus, we restrict ourself to the prime case. Suppose $x \mapsto x^3 + x$ is a permutation of $\mathbb{F}_p$. Then,

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv (1^3+1)(2^3+2) \cdot \ldots \cdot ((p-1)^3 + (p-1))$$

as $0^3+0 = 0$ so $x \mapsto x^3$ must also be a permutation of $\mathbb{F}_p \setminus \{0\}$. After simplifying by $1 \cdot \ldots \cdot (p-1)$, this is equivalent to

$$(1^2+1)(2^2+1) \cdot \ldots ((p-1)^2+1) \equiv 1.$$

But notice that, by Fermat's little theorem, the numbers of the form $a^2 + 1$ are the roots of the polynomial $(X-1)^{\frac{p-1}{2}} - 1$ whose constant term is $(-1)^{\frac{p-1}{2}} - 1$. Moreover, in our product, every root is present exactly twice (a^2+ and $(-a)^2+1$) so we get

$$(1^2+1)(2^2+1) \cdot \ldots ((p-1)^2+1) \equiv (\pm((-1)^{\frac{p-1}{2}} - 1))^2 \pmod{p}$$

by Vieta's formulas. But $(\pm((-1)^{\frac{p-1}{2}} - 1))^2 \in \{0, 4\}$ so for this to be congruent to 1 modulo p we must have $p = 3$. It is also easy to check that $x \mapsto x^3 + x$ is a bijection of $\mathbb{F}_3$, hence we are done (with the prime case). ■

Conversely, the following result, which is proven in Appendix B, shows that we can always achieve such a factorisation over the complex numbers. Fields where this result holds are said to be *algebraically closed*.

Theorem A.1.1 (Fundamental Theorem of Algebra)

Any polynomial $f \in \mathbb{C}[X]$ of degree $n \geq 0$ has exactly n roots, i.e.,

$$f = a(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n)$$

where $\alpha_1, \ldots, \alpha_n$ are the roots of f counted with multiplicity and a is its leading coefficient.

Over the real numbers, we have the following result.

Proposition A.1.5

Any non-zero polynomial $f \in \mathbb{R}[X]$ factorises into a product

$$a(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_m) f_1 \cdot \ldots \cdot f_k$$

where $a \in \mathbb{R}$ is its leading coefficient, $\alpha_i \in \mathbb{R}$ are its real roots, and the $f_i \in \mathbb{R}[X]$ are monic polynomials of degree 2 with no real roots.

In fact, we shall prove that non-real roots α come in pairs of conjugates $\alpha, \overline{\alpha}$, since $(X-\alpha)(X-\overline{\alpha})$ has real coefficients this will yield the result.

Proposition A.1.6*

Suppose $f \in \mathbb{R}[X]$. Then, for any $\alpha \in \mathbb{C}$, $v_\alpha(f) = v_{\overline{\alpha}}(f)$.

Proof

We have $f = (X-\alpha)^m g$ for some $g \in \mathbb{C}[X]$ if and only if $f = (X-\overline{\alpha})^m \overline{g}$, where $\overline{g}$ denotes the polynomial whose coefficients are the complex conjugates of those of g.

■

Proof of Proposition A.1.5

Write $f = a(X-\alpha_1)\cdot\ldots\cdot(X-\alpha_m)(X-\beta_1)(X-\overline{\beta}_1)\cdot\ldots\cdot(X-\beta_m)(X-\overline{\beta}_m)$ where $\alpha_i \in \mathbb{R}$ and $\beta_i \in \mathbb{C}\setminus\mathbb{R}$ using Proposition A.1.6. Then,

$$f = a(X-\alpha_1)\cdot\ldots\cdot(X-\alpha_m)f_1\cdot\ldots\cdot f_k$$

where $f_i = (X-\beta_i)(X-\overline{\beta}_i) = X^2 - 2\Re(\beta_i) + |\beta_i|^2 \in \mathbb{R}[X]$.

■

The fact that some polynomials over $\mathbb{R}[X]$ cannot be decomposed into a product of linear polynomials motivates us to make the following definition.

Definition A.1.6 (Irreducible Polynomial)

A non-zero polynomial $f \in K[X]$ is said to be *irreducible* in $K[X]$ if it can not be written as a product of two polynomials of smaller degrees. We shall also say it is irreducible *over* K.

Notice that degree 2 and 3 polynomials are irreducible if and only if they don't have a root in K, since if they can be written as a product of two polynomials of smaller degrees one of them must have degree 1. For instance, X^3+2 is irreducible in $\mathbb{Q}[X]$ since it does not have a root there, but not in $\mathbb{R}[X]$. X^2+1 is irreducible in $\mathbb{R}[X]$, but not in $\mathbb{C}[X]$. Irreducible polynomials over $\mathbb{R}$ and $\mathbb{C}$ are a bit degenerate because they have degree 1 or 2, but over $\mathbb{Q}$ there are irreducible polynomials of arbitrarily large degree.

Here is one last result, which is the only one of this section which will not be used extensively throughout this book.

Theorem A.1.2 (Lagrange Interpolation)

For any distinct $a_1, \ldots, a_{n+1} \in K$ and $b_1, \ldots, b_{n+1} \in K$ there is a unique polynomial $f \in K[X]$ of degree at most n such that $f(a_i) = b_i$ for $i = 1, \ldots, n+1$. It is given by $f = \sum_{i=1}^{n+1} b_i f_i$ where

$$f_i := \prod_{j\neq i} \frac{X-a_j}{a_i-a_j}.$$

Proof

First, let's prove uniqueness. If $f, g \in K[X]$ have degree at most n and $f(a_i) = b_i = g(a_i)$ for any $i = 1, \dots, n+1$ then $f - g$ has $n+1$ roots and has degree at most n so it is the zero polynomial, i.e. $f = g$.

For existence, notice that $f_i(a_j) = 0$ for any $j \neq i$ and $f_i(a_i) = 1$, so that

$$f(a_i) = \sum_j b_j f_j(a_i) = b_i \cdot 1 + \sum_{j \neq i} b_j \cdot 0 = b_i.$$

■

Corollary A.1.3

Let $K \subseteq L$ be two fields. If a polynomial $f \in L[X]$ of degree n reaches values in K at $n+1$ points in K, it has coefficients in K.

Proof

If $f(a_i) = b_i$ with $a_i, b_i \in K$ for $i = 1, \dots, n+1$ and distinct a_i, the Lagrange interpolation formula shows that $f \in K[X]$.

■

Exercise A.1.9*. Prove that every function $f : \mathbb{F}_p \to \mathbb{F}_p$ is polynomial.

To conclude this section, we make one final definition. Unlike what their name would suggest, rational functions are **formal** objects and are not functions, like polynomials.

Definition A.1.7 (Rational Function)

A *rational function* with coefficients in K is a quotient of two polynomials f/g with coefficients in K such that $g \neq 0$ (with the additional rule that $f/g = (hf)/(hg)$ for any non-zero $h \in K[X]$). The set of rational functions with coefficients in K is denoted $K(X)$.

The derivative of a rational function f/g is $(f'g - g'f)/(g^2)$, where $g^2 = g \cdot g$.

Exercise A.1.10*. Prove that the derivative of a rational function does not depend on its form: i.e. $(f/g)' = ((hf)/(hg))'$ for any $f, g, h \in K[X]$ with $g, h \neq 0$.

A.2 Algebraic Structures and Morphisms

We introduced the notion of a field in the last section; here, we shall define a few additional algebraic structures. There are two things to understand from this section: what an *integral domain* is[5] and what *morphisms* and *isomorphisms* are. This doesn't mean that the other definitions are useless, but you can ignore them for now. They will be used in some chapters: when this happens the reader should come to this appendix to refresh their memory.

[5] Although, usually in this book when something is obviously an integral domain and we don't want to emphasise this we will just call it a ring.

Definition A.2.1 (Ring)

We say a set R with two operations $+$ and $\cdot$ from R^2 to R is a *ring* if the following axioms are satisifed. We write ab for $a \cdot b$.

1. $+$ is associative: $(a+b)+c = a+(b+c)$ for any $a, b, c \in R$.
2. $+$ is commutative: $a+b = b+a$ for any $a, b \in R$.
3. additive identity: there is an element 0_R such that $0_R + a = a$ for any $a \in R$.
4. additive inverse: for any $a \in R$ there is an element $-a \in R$ such that $a + (-a) = 0_R$.
5. $\cdot$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a, b, c \in R$.
6. multiplicative identity: there is an element 1_R such that $1_R \cdot a = a \cdot 1_R = a$ for any $a \in R$.
7. $\cdot$ distributes over $+$: for any $a, b, c \in R$, $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$.

Exercise A.2.1*. Prove that 1_R and 0_R are unique, and that any element has a unique additive inverse and a unique multiplicative inverse if it is non-zero.

Exercise A.2.2*. Let R be a ring. Prove that $0_R a = a 0_R = 0_R$ for any $a \in R$.

A ring is like a field, but possibly without the existence of multiplicative inverse, as well as with a possibly non-commutative multiplication. Non-commutative rings will only be relevant in Chapter 2. Again, R is technically not a ring, it is $(R, +, \cdot)$ that is one, but by abuse of terminology we will say that R is a ring when the addition and multiplication are obvious. We shall usually write 0 for 0_R and 1 for 1_R, even if they might not technically be our usual $0, 1 \in \mathbb{Z}$.

Definition A.2.2 ($\mathbb{Z}/n\mathbb{Z}$)

By $\mathbb{Z}/n\mathbb{Z}$, we denote the ring with n elements of integers modulo n. In particular, $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$.

Remark A.2.1

There is a deeper story behind this notation, see the footnote in Exercise A.3.14†.

Rings have a certain number associated to them which is what distinguishes rings like $\mathbb{Z}$ from rings like $\mathbb{Z}/n\mathbb{Z}$. We have already encountered this notion in the case of fields in Proposition A.1.3.

Definition A.2.3 (Characteristic)

Let R be a ring. We say R has *characteristic* m if m is the smallest integer such that

$$\underbrace{1 + \ldots + 1}_{m \text{ times}} = 0.$$

If no such m exists we say R has characteristic 0. The characteristic of R is denoted $\operatorname{char} R$.

In other words, the characteristic of R is the smallest $m \geq 0$ such that R contains a copy of $\mathbb{Z}/m\mathbb{Z}$.

Exercise A.2.3*. Prove that $\operatorname{char} R$ is the smallest $m \geq 0$ such that R contains a copy of $\mathbb{Z}/m\mathbb{Z}$

Definition A.2.4 (Commutative Ring)

A *commutative ring* is a ring where multiplication is commutative.

We now define a field in terms of these objects, exactly like before, but hopefully this makes it clearer how these objects are connected.

Definition A.2.5 (Field)

A *field* K is a commutative ring where non-zero elements have multiplicative inverses, i.e. for any $a \in K$ there is an element $a^{-1} \in K$ such that $aa^{-1} = 1_K$.

For fields, you should think about $\mathbb{Q}$. We also have the analogous definition for non-commutative fields.

Exercise A.2.4*. Prove that the characteristic of a field is either 0 or a prime number p.

Definition A.2.6 (Skew Field)

A *skew field* K is a field but where multiplication is not necessarily commutative, i.e. a ring with multiplicative inverses: for any $0 \neq a \in K$ there is an element $a^{-1} \in K$ such that $aa^{-1} = a^{-1}a = 1_K$ (we specify both equalities because multiplication is not necessarily commutative anymore).

Finally, we define the fundamental integral domains.

Definition A.2.7 (Domain)

A *domain* is a ring where the product of two non-zero elements is non-zero. A commutative domain is called an *integral domain*.

For integral domains, you can again think about $\mathbb{Z}$. An example of a commutative ring which isn't an integral domain is $\mathbb{Z}/4\mathbb{Z}$: $2 \cdot 2 \equiv 0$ but $2 \not\equiv 0$. $\mathbb{Z}$ is really the typical example of an integral domain, more than of a ring or commutative ring.

Exercise A.2.5. Let R be a finite integral domain (i.e. with finitely cardinality). Prove that it is a field.

An important fact about integral domains is that they are precisely the subrings of fields, i.e. they are the rings which can be *embedded* in a larger field. Why is this true? It's obvious that a subring of a field is an integral domain. For the converse, given an integral domain R you can construct its *field of fractions* $\operatorname{Frac} R$, exactly like how you construct $\mathbb{Q}$ from $\mathbb{Z}$. You define formal objects a/b for $a, b \in R$ and then you say $a/b = c/d$ if $ad = bc$ and you define addition and multiplication in this obvious ways; it is then easy to check that this yields a field. For instance, for $R = K[X]$, this gives $\operatorname{Frac} R = K(X)$.

Exercise A.2.6*. Prove that a subring of a field is an integral domain.

Exercise A.2.7. What goes wrong if you try to construct the field of fractions of a commutative ring which isn't a domain?

Since integral domains can be embedded in fields, polynomials with coefficients there retain most of their properties, so we can also define polynomials with coefficients in an integral domain R. The ring of such polynomials is denoted $R[X]$, and the ring of rational functions with coefficients in R, $\operatorname{Frac} R[X]$ is denoted $R(X)$.

Exercise A.2.8*. Let R be an integral domain. Prove that $R[X]$ is also one.

In fact, perhaps the most important property we lose when restricting ourself to an integral domain, is that we can not do the Euclidean division of any f by any $g \neq 0$. Indeed, our proof Proposition A.1.1 involved dividing by the leading coefficient of g, and it is true that we can't have $X = 2Xq + r$ for some $q \in \mathbb{Z}[X]$ and $r \in \mathbb{Z}[X]$ of degree less than 1. However, this also means that there is one case when we can make this Euclidean division: when g is monic.

Finally, we explain what *morphisms* are. Imagine you have the two fields $\{0, 1\}$ and $\{a, b\}$ where a, b are formal symbols. Multiplication and addition are defined as follows. For the former $0 + 0 = 0$, $0 + 1 = 1$ and $1 + 1 = 0$ for addition, and $0 \cdot 0 = 0$, $0 \cdot 1 = 0$ and $1 \cdot 1$ for multiplication. For the latter, it's $a + a = a$, $a + b = b$ and $b + b = a$ for addition, and $a \cdot a = a$, $a \cdot b = a$ and $b \cdot b = b$.

These are defined exactly in the same way! Any reasonable person would want to conclude that they are the same, that they are both equal to $\mathbb{F}_2$. But they are not! Our definition of a field was very clear: it is a triple of a set and two operations satisfying some axioms. Here the sets are different so the triples are too, which means the fields are not the same.

Thus, we want to define formally what a "relabelling" of the elements is. This is exactly what an isomorphism is (iso = same, morphism = shape). We will in fact not define them formally in general because isomorphisms depend on the structure considered (a ring isomorphism and a *group* (to be defined later) isomorphism are different), but here is what a field isomorphism.

Definition A.2.8 (Field Isomorphism)

Let K and L be two fields. We say a function $\varphi : K \to L$ is an *isomorphism* if f is additive, multiplicative, sends 1 to 1, and is bijective, i.e.

$$\begin{aligned} \varphi(x + y) &= \varphi(x) + \varphi(y) \\ \varphi(x)\varphi(y) &= \varphi(x)\varphi(y) \\ f(1) &= 1 \end{aligned}$$

for any $x, y \in K$. If there exists such a φ, we say K and L are *isomorphic* and write $K \simeq L$.

A few words on this definition. The function φ is our "relabelling" of the elements: relabel x as $\varphi(x)$. The conditions of φ are to ensure that f *conserves the field structure*, i.e. addition gets mapped to addition, multiplication to multiplication, inverse to inverse, identity to identity. The reason why we ask that $f(1) = 1$ but not that $f(0) = 0$ is that this follows from $\varphi(0) + \varphi(0) = \varphi(0)$. However $f(1) = 1$ does not follow from $\varphi(1)\varphi(1) = \varphi(1)$: φ could be identically zero.

Similarly, $f(-x) = -f(x)$ and $f(x^{-1}) = f(x)^{-1}$ follow from the additivity and multiplicativity respectively. What we really want is for f to respect **every single aspect** of the field structure, but we have not written down all of these conditions in the definition of an isomorphism since they are redundant (of course we also want f to be bijective: this is what it means for the fields to be "the same up to relabelling").

In fact, all this talk about "conserving the structure" suggests that this might actually be an important notion, and this is why we define *morphism* as functions which preserve the structure (which is implicit, technically we should say our previous f is a **field** isomorphism, not just an isomorphism).

Definition A.2.9 (Field Morphism)

Let K and L be two fields. We say a function $\varphi : K \to L$ is an *morphism* if f is additive, multiplicative and sends 1 to 1, i.e.

$$\begin{aligned}\varphi(x+y) &= \varphi(x)+\varphi(y)\\ \varphi(x)\varphi(y) &= \varphi(x)\varphi(y)\\ \varphi(1) &= 1\end{aligned}$$

for any $x, y \in K$.

Commutative rings morphisms and isomorphisms are defined exactly the same way, because the additional structure that comes from fields is the existence of multiplicative inverse, but we have seen that the fact that φ sends inverses to inverses already follows from its multiplicativity (and the fact that $\varphi(1) = 1$).

You might think that these notions of isomorphisms and morphisms are just pedantic details about how to define formally objects. They are not. They suggest that objects which were initially defined very differently might in fact be similar. For instance, morphisms of sets are just functions since sets have no structure, and isomorphisms are bijective functions. Are bijections useless to study?

An example of fields non-trivially isomorphic is the one of $\mathbb{Q}(\pi)$ of rational functions in π and $\mathbb{Q}(e)$ of rational functions in e are isomorphic. This is not obvious, and in fact very hard to prove (we do not do it in this book).[6] A better example will be seen soon, but first we need to define groups for this (they will be used in Chapter 6).

Definition A.2.10 (Group)

We say a set G with an operation $\dagger : G^2 \to G$ is a *group* if the $\dagger$ is associative, has an identity, and each element has an inverse for $\dagger$, i.e.

1. $(a \dagger b) \dagger c = a \dagger (b \dagger c)$ for any $a, b, c \in G$.
2. there is an $e \in G$ such that $a \dagger e = e \dagger a = a$ for any $a \in G$.
3. for any $a \in G$ there is an $a^{-1} \in G$ such that $a \dagger a^{-1} = a^{-1} \dagger a = e$.

Exercise A.2.9*. Prove that the identity e of a group G is unique, and that any $a \in G$ has a unique inverse. Moreover, prove that $(xy)^{-1} = y^{-1}x^{-1}$.

The simplest example is the *cyclic group* with n elements $(\mathbb{Z}/n\mathbb{Z}, +)$ where $\mathbb{Z}/n\mathbb{Z}$ represents integers modulo n. We say it's cyclic because it's generated by only one element: the elements of $(\mathbb{Z}/n\mathbb{Z}, +)$ have the form $1 + \ldots + 1$ for some number of ones. It is *commutative* or *abelian*, which means that the operation is commutative.[7]

Note that if you consider rings as groups you must ignore their multiplicative structure, since groups have only operation (you can also consider the multiplicative group of *units* a ring, i.e. the elements which are invertible).

A slightly more elaborate example, yet still very important, is the *symmetric group* with n elements $\mathfrak{S}_n$. This is the group of permutations of $\{1, \ldots, n\}$, and the operation is composition.

Exercise A.2.10*. Check that $(\mathfrak{S}_n, \circ)$ is a group.

[6] Well, actually, I'm a bit exaggerating here because I did not find a good examples with fields, showing that $\mathbb{Q}(\pi) = \mathbb{Q}(e)$ amounts to showing they are both transcendental (see Section 1.1 for a definition), and this is what's really hard.

[7] Personally, I was only convinced by this termniology when I realised saying "let L/K be a commutative extension" seemed extremely awkward. (A field extension L/K is said to be abelian if its Galois group is, see Chapter 6.)

Morphisms of groups are extremely easy to define since groups have so little (yet so much!) structure: it's simply a function which commutes with the operation: $\varphi : G \to H$ is a morphism if $\varphi(a \dagger b) = \varphi(a) \star \varphi(b)$ for any $a, b \in G$.

Exercise A.2.11*. Prove that a morphism of groups from $(G, \dagger)$ to $(H, \star)$ maps the identity of G to the identity of H.

W nowe give an example of a non-trivial isomorphism (of groups). If p is a prime, the groups $((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ and $(\mathbb{Z}/(p-1), +)$ are isomorphic, where $(\mathbb{Z}/p\mathbb{Z})^\times$ denotes the integers mod p which are coprime with p (so that inverses exist). Since they clearly have the same number of elements, this is equivalent to $(\mathbb{Z}/p\mathbb{Z})^\times$ being cyclic, i.e. generated by one element, which we will call g. This g is such that, for any $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, there is a k such that $a = g^k$. This is exactly the definition of a primitive root! Thus, this isomorphism translates the fact that there is a primitive root modulo p, which is certainly non-trivial! Here is another very interesting example: $(\mathbb{Z}/n\mathbb{Z}, +)$ is isomorphic to $(U_n, \cdot)$, where U_n denotes the set of complex nth roots of unity. Indeed, the function $k \mapsto \exp\left(\frac{2ki\pi}{n}\right)$ is clearly an isomorphism between the two.

We will usually write our group operations multiplicatively, that is, we will write xy or $x \cdot y$ for $x \dagger y$. In this case, one should **always** write the inverse of y as y^{-1} instead of $1/y$, unless the group is already known to be abelian. Indeed, if we were to write $1/y$, would x/y mean xy^{-1} or $y^{-1}x$? Sometimes the additive notation will also be used, we shall then write $x + y$ for xy and nx for x^n. We may also write the identity e of G as 1 or 0, depending on whether we are using the additive or multiplicative notation. In addition, when the operation is obvious, we will omit it. For instance, when we consider a ring as a group (such as $\mathbb{Z}/n\mathbb{Z}$), the operation will always be addition. Indeed, it cannot be multiplication since 0 does not have an inverse. Conversely, if we write $R^\times$, the set of invertible units of R, this shall be considered as a multiplicative group (it is not additive since $0 \notin R^\times$).

Lastly, we define two important maps on morphisms.

Definition A.2.11 (Kernel)

The *kernel* $\ker \varphi$ of a morphism φ is the set of x such that $\varphi(x) = 0$. It measures how far φ is from being injective.

Definition A.2.12 (Image)

The *image* $\operatorname{im} \varphi$ of a morphism φ is the set of y such that $y = \varphi(x)$ for some x. It measures how far φ is from being surjective.

Exercise A.2.12*. Prove that the kernel of a morphism (of rings or groups) is closed under addition.

Exercise A.2.13*. Prove that a morphism of groups is injective iff its kernel is trivial, i.e. consists of only the identity.

As a final remark, in Appendix C, we will introduce another algebraic structure called *vector spaces*, and we will define morphisms for vector spaces.

A.3 Exercises

Derivatives

Exercise A.3.1†. Let $f, g \in K[X]$ be two polynomials. Prove that the derivative of $f \circ g$ is $g' \cdot f' \circ g$.

Exercise A.3.2†. Let $f \in K[X]$ be a non-constant polynomial. Prove that there are a finite number of $g, h \in K[X]$ such that $g \circ h = f$, up to affine translation, meaning $(g, h) \equiv \left(g(aX + b), \frac{h-b}{a}\right)$.

Exercise A.3.3. Let $f \in \mathbb{R}[X]$ be a polynomial. Suppose that $f \circ f$ is the square of a polynomial. Prove that f also is the square of a polynomial.

Exercise A.3.4† (USA TST 2017)**.** Let $f, g \in \mathbb{R}[X]$ be non-constant coprime polynomials. Prove that there are at most three real numbers λ such that $f + \lambda g$ is the square of a polynomial.

Exercise A.3.5 (All-Russian Olympiad 2014)**.** On a blackboard, we write (only) the polynomials $X^2 - 3X^2$ and $X^2 - 4X$ and all real numbers $c \in \mathbb{R}$. If the polynomials f and g are written on the board, we can also write $f \pm g, f \cdot g$ and $f \circ g$. Is it possible to write a polynomial of the form $X^n - 1$?

Exercise A.3.6† (Discrete Derivative)**.** Let $f \in K[X]$ be a polynomial of degree n and leading coefficient a. Define its *discrete derivative* as $\Delta f := f(X+1) - f(X)$. Prove that, for any $g \in K[X]$ $\Delta f = \Delta g$ if and only if $f - g$ is constant, and that Δf is a polynomial of degree $n-1$ with leading coefficient an where a is the leading coefficient of f. Deduce the minimal degree of a monic polynomial $f \in \mathbb{Z}[X]$ identically zero modulo m, for a given integer $m \geq 1$.

Exercise A.3.7†**.** Let $f : R \to R$ be a function. Define its discrete derivative Δf as $x \mapsto f(x+1) - f(x)$. Prove that, for any integer $n \geq 0$,

$$\Delta^n f(x) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(x+k).$$

Exercise A.3.8†**.** Let $m \geq 0$ be an integer. Prove that there is a polynomial $f_m \in \mathbb{Q}[X]$ of degree $m+1$ such that

$$\sum_{k=0}^{n} k^m = f_m(n)$$

for any $n \in \mathbb{N}$.

Roots of Unity

Exercise A.3.9† (Root of Unity Filter)**.** Let $f = \sum_i a_i X^i \in K[X]$ be a polynomial, and suppose that $\omega_1, \ldots, \omega_n \in K$ are distinct nth roots of unity. Prove that

$$\frac{f(\omega_1) + \ldots + f(\omega_n)}{n} = \sum_{n|k} a_k.$$

Deduce that, if $K = \mathbb{C}$,

$$\max_{|z|=1} |f(z)| \geq |f(0)|.$$

(You may assume the existence of a *primitive* nth root of unity ω, meaning that $\omega^k \neq 1$ for all $k < n$, or, equivalently, every nth root of unity are powers of ω. This will be proven in Chapter 3.)

Exercise A.3.10†**.** Let $f = \sum_i a_i X^i \in \mathbb{R}[X]$ be a polynomial and $\omega_1, \ldots, \omega_n \in \mathbb{C}$ be distinct nth roots of unity with $n > \deg f$. Prove that

$$\frac{|f(\omega_1)|^2 + \ldots + |f(\omega_n)|^2}{n} = \sum_i a_i^2.$$

Denote by $S(f)$ the sum of the squares of the coefficients of f. Deduce that $S(fg) = S(fX^{\deg g} g(1/X))$ for all $f, g \in \mathbb{R}[X]$. ($X^{\deg g} g(1/X)$ is the polynomial obtained by reversing the coefficients of g.)

Exercise A.3.11†**.** Let k be an integer. Prove that $\sum_{a \in \mathbb{F}_p} a^k$ is 0 if $p - 1 \nmid k$ and -1 otherwise. Deduce that any non-constant polynomial $f \in \mathbb{F}_p[X]$ satisfying $f(a) \in \{0, 1\}$ for all $a \in \mathbb{F}_p$ must have degree at least $p - 1$.

Exercise A.3.12†**.** Let $p \neq 3$ be a prime number. Suppose that a and b are integers such that $p \mid a^2 + ab + b^2$. Prove that $(a+b)^p \equiv a^p + b^p \pmod{p^3}$.

Exercise A.3.13 (China TST 2018)**.** Let k be an integer, p a prime number, and S the set of kth powers of elements of $\mathbb{F}_p$. Prove that, if $2 < |S| < p - 1$, the elements of S are not an arithmetic progression.

Group Theory

Exercise A.3.14†. Given a group G and a *normal subgroup* $H \subseteq G$, i.e. a subgroup such that

$$x + H - x = H$$

for any $x \in G$,[8] we define the *quotient* G/H of G by H as G *modulo* H[9], i.e. we say $x \equiv y \pmod{H}$ if $x - y \in H$.[10] Prove that this indeed a group, and that $|G/H| = |G|/|H|$ for any such G, H.

Exercise A.3.15† (Isomorphism Theorems)**.** Prove the following first, second, and third isomorphism theorems.

1. Let $\varphi : A \to B$ be a morphism of groups. Then, $A/\ker\varphi \simeq \operatorname{im}\varphi$. (In particular, $\ker\varphi$ is normal in A and $|\operatorname{im}\varphi| \cdot |\ker\varphi| = |A|$.)

2. Let H be a subgroup of a group G, and N a normal subgroup of G. Then, $H/H \cap N \simeq HN/N$. (In particular, you need to show that this makes sense: HN is a group and $H \cap N$ is normal in H.)

3. Let $N \subseteq H$ be normal subgroups of a group G. Then, $(G/N)/(H/N) \simeq G/H$.

Exercise A.3.16†. Let G be a finite group, $\varphi : G \to \mathbb{C}^\times$ be a non-trivial group morphism (i.e. not the constant function 1), where $(\mathbb{C}^\times, \cdot)$ is the group of non-zero complex numbers under multiplication. Prove that $\sum_{g\in G} \varphi(g) = 0$.

Exercise A.3.17† (Lagrange's Theorem)**.** Let G be a group of cardinality n (also called the *order* of G). Prove that $g^n = e$ for all $g \in G$. In other words, the order of an element divides the order of the group. More generally, prove that the order of a subgroup divides the order of the group.

Exercise A.3.18† (5/8 Theorem)**.** Let G be a non-commutative finite group. Prove that the probability

$$p(G) = \frac{|\{(x, y) \in G^2 \mid xy = yx\}|}{|G|^2}$$

that two elements commute is at most 5/8.

Exercise A.3.19† (Fundamental Theorem of Finitely Generated Abelian Groups)**.** Let G be an abelian group which is finitely generated, i.e., if we write its operation as $+$, there are $g_1, \ldots, g_k \in G$ such that any $g \in G$ can be represented as $n_1 g_1 + \ldots + n_k g_k$ for integers $n_i \in \mathbb{Z}$. Prove that there is a unique integer $n \geq 0$ (called the *rank* of the group) and a unique sequence of positive integers $d_1 \mid \ldots \mid d_m$ such that

$$(G, +) \simeq (\mathbb{Z}^n \times \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z}, +).$$

Exercise A.3.20† (Burnside's Lemma)**.** Let G be a finite group, S a finite set, and $\cdot$ a *group action* of G on S, meaning a map $\cdot : G \times S \to S$ such that $e \cdot s = s$ and $(gh) \cdot s = g \cdot (h \cdot s)$ for any $g, h \in G$ and $s \in S$. Given a $g \in G$, denote by $\operatorname{Fix}(g)$ the set of elements of s fixed by g. Prove that

$$|S/G| = \frac{1}{|G|} \sum_{g\in G} \operatorname{Fix}(g),$$

where $|S/G|$ denotes the number of (disjoint) orbits $\mathcal{O}_i = Gs_i$. Deduce the number of necklaces that have p beads which can be of a colours, where p is a prime number and two necklaces are considered to be the same up to rotation.

[8] In particular, when G is abelian, any subgroup is normal.

[9] This is where the notation $\mathbb{Z}/n\mathbb{Z}$ comes from! In fact this shows that, in reality, we should say "modulo $n\mathbb{Z}$" instead of "modulo n".

[10] A better formalism is to say that G/H is the set of cosets $g + H$ for $g \in G$. In fact, we will almost always use this definition in the solutions of exercises (since this is the only place where this will appear), but we introduced it that way to make the analogy with $\mathbb{Z}/n\mathbb{Z}$ clearer.

Miscellaneous

Exercise A.3.21† (China TST 2009)**.** Prove that there exists a real number $c > 0$ such that, for any prime number p, there are at most $cp^{2/3}$ positive integers n satisfying $n! \equiv -1 \pmod{p}$.

Exercise A.3.22† (Mason-Stothers Theorem, ABC conjecture for polynomials)**.** Suppose that $A, B, C \in \mathbb{C}[X]$ are coprime polynomials such that $A + B = C$. Prove that

$$1 + \max(\deg A, \deg B, \deg C) \leq \deg(\operatorname{rad} ABC)$$

where rad ABC is the greatest squarefree divisor of ABC (in other words, $\deg(\operatorname{rad} ABC)$ is the number of distinct complex roots of ABC). Deduce that the Fermat equation $f^n + g^n = h^n$ for $f, g, h \in \mathbb{C}[X]$ does not have non-trivial solutions for $n \geq 2$.

Exercise A.3.23†**.** Find all polynomials $f \in \mathbb{C}[X]$ which send the unit circle to itself.

Exercise A.3.24. Suppose that $f, g \in \mathbb{C}[X]$ are polynomials such that, for all $x \in \mathbb{C}$, $f(x) \in \mathbb{R}$ implies $g(x) \in \mathbb{R}$. Prove that there exists a polynomial $h \in \mathbb{R}[X]$ such that $g = h \circ f$.

Exercise A.3.25. Let $(K, +, \cdot)$ be a set satisfying the axioms of a field except possibly that $\cdot$ takes values in K. Prove that it is in fact a field.

Exercise A.3.26† (Gauss-Lucas Theorem)**.** Let $f \in \mathbb{C}[X]$ be a polynomial with roots $\alpha_1, \ldots, \alpha_k$. Prove that

$$\frac{f'}{f} = \sum_k \frac{1}{X - \alpha_k}.$$

Deduce the Gauss-Lucas theorem: if $f \in \mathbb{C}[X]$ is non-constant, the roots of f' are in the *convex hull* of the roots of f, that is, any root β of f' is a linear combination $\sum_i \lambda_i \alpha_i$ with $\sum_i \lambda_i = 1$ and non-negative $\lambda_i \in \mathbb{R}$.

Exercise A.3.27† (Sturm's Theorem)**.** Given a squarefree polynomial $f \in \mathbb{R}[X]$, define the sequence $f_0 = f$, $f_1 = f'$ and f_{n+2} is minus the remainder of the Euclidean division of f_n by f_{n+1}. Define also $V(\xi)$ as the number of sign changes in the sequence $f_0(\xi), f_1(\xi), \ldots$, ignoring zeros. Prove that the number of distinct real roots of f in the interval $]a, b]$ is $V(a) - V(b)$.[11]

Exercise A.3.28† (Ehrenfeucht's Criterion)**.** Let K be a characteristic zero field, let $f_1, \ldots, f_k \in K[X]$ be polynomials and define

$$f = f_1(X_1) + \ldots + f_k(X_k) \in K[X_1, \ldots, X_k].$$

If $k \geq 3$, prove that f is irreducible. In addition, prove that this result still holds if $k = 2$ and f_1 and f_2 have coprime degrees.

Exercise A.3.29† (IMC 2007)**.** Let $a_1, \ldots, a_n$ be integers. Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is a function such that

$$\sum_{i=1}^{n} f(ka_i + \ell) = 0$$

for any $k, \ell \in \mathbb{Z}$. Prove that f is identically zero.

Exercise A.3.30. Find all polynomials $f \in \mathbb{C}[X]$ satisfying

1. $f(X^n) = f(X)^n$ for some integer $n \geq 2$.
2. $f(X^2 + 1) = f(X^2) + 1$.
3. $f(X)f(X + 1) = f(X^2 + X + 1)$.
4. $f(X^2) = f(X)f(X + 1)$.
5. $f(X^2) = f(X)f(X - 1)$.

Exercise A.3.31. Let $f \in K[X]$ be a polynomial of degree n. Find $f(n + 1)$ if

1. (USAMO 1975) $f(k) = \frac{k}{k+1}$ for $k = 0, \ldots, n$.
2. $f(k) = 2^k$ for $k = 0, \ldots, n$.

[11] If we choose $a = -\infty$, $b = +\infty$, this gives an algorithm to compute the number of real roots of f, by looking at the signs of the leading coefficients of $f_0 f_1, \ldots$.

Appendix B

Symmetric Polynomials

Prerequisites for this chapter: Section A.1.

B.1 The Fundamental Theorem of Symmetric Polynomials

Given a commutative ring R (in our case we will consider $\mathbb{Z}$ and $\mathbb{Q}$) and an integer $n \geq 0$, we can consider the symmetric polynomials in n variables with coefficients in R. These are defined as the polynomials in n variables invariant under all permutations of these variables.

Definition B.1.1 (Symmetric Polynomials)

We say a polynomial $f \in R[X_1, \ldots, X_n]$ is *symmetric* if $f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$ for any permutation σ of $[n]$.

Exercise B.1.1. Let $f \in K(X_1, \ldots, X_n)$ be a rational function, where K is a field. Suppose f is symmetric, i.e. invariant under permutations of $X_1, \ldots, X_n$. Prove that $f = g/h$ for some symmetric polynomials $g, h \in K[X_1, \ldots, X_n]$.

As an example, $f = X^2Y + XY^2 + X^2 + Y^2$ is a symmetric polynomial in two variables, and

$$g = X^2YZ + XY^2Z + XYZ^2 + XY^2 + X^2Y + XZ^2 + X^2Z + YZ^2 + Y^2Z$$

is a symmetric polynomial in three variables.

Definition B.1.2 (Elementary Symmetric Polynomials)

The kth *elementary symmetric polynomial* for $k \geq 0$, $e_k \in R[X_1, \ldots, X_n]$, is defined by

$$e_k = \sum_{1 \leq i_1 < \ldots < i_k \leq n} X_{i_1} \cdot \ldots \cdot X_{i_k}.$$

Further, if $k > n$ then $e_k = 0$ (the empty sum) and if $k = 0$ then $e_0 = 1$ (the sum of the empty product).

The two-variable symmetric polynomials are thus simply $e_1 = X + Y$ and $e_2 = XY$. The three-variable ones are $e_1 = X + Y + Z$, $e_2 = XY + YZ + ZX$ and $e_3 = XYZ$.

We now state the fundamental theorem of symmetric polynomial.

Theorem B.1.1 (Fundamental Theorem of Symmetric Polynomials)

Suppose $f \in R[X_1, \ldots, X_n]$ is a symmetric polynomial. Then $f \in R[e_1, \ldots, e_n]$. In other words, there is a polynomial $g \in R[X_1, \ldots, X_n]$ such that

$$f(X_1, \ldots, X_n) = g(e_1, \ldots, e_n).$$

This theorem explains why we called e_k "elementary symmetric polynomials": because they generate all symmetric polynomials.

Proof

We proceed by induction on the number n of variables. For $n = 1$ this is trivial as $\sigma_1 = X$. Thus suppose it is true for $n - 1$ variables.

Now, we proceed again by induction on the degree d of f. When $f = 0$ this is obvious. Otherwise, by the first induction hypothesis,

$$f(X_1, \ldots, X_{n-1}, 0) = g(e'_1, \ldots, e'_{n-1})$$

for some $g \in K[X_1, \ldots, X_n]$, where e'_i is the ith elementary symmetric polynomial **in** $n - 1$ **variables**, i.e. $e'_i(X_1, \ldots, X_{n-1}) = e_i(X_1, \ldots, X_{n-1}, 0)$. Notice that $\deg g \leq \deg f$.

Write

$$f(X_1, \ldots, X_n) = g(e_1, \ldots, e_{n-1}) + h(X_1, \ldots, X_n).$$

We have $h(X_1, \ldots, X_{n-1}, 0) = 0$, i.e.

$$X_n \mid h(X_1, \ldots, X_{n-1}, X_n)$$

($h(X_1, \ldots, X_n)$ has a root at X_n in the ring $R[X_1, \ldots, X_{n-1}][X]$). By symmetry we also have $X_i \mid h$ for any i so $h = X_1 \cdot \ldots \cdot X_n r = e_n s$.

To conclude s is symmetric and has degree at most $\deg f - n < \deg f$ so $r = s(e_1, \ldots, e_n)$ by the second induction hypothesis and we get

$$f = g(e_1, \ldots, e_{n-1}) + e_n r(e_1, \ldots, e_n)$$

as wanted.

■

Exercise B.1.2. Prove that the decomposition of a symmetric polynomial f as $g(e_1, \ldots, e_n)$ is unique.

B.2 Newton's Formulas

Apart from elementary symmetric polynomials, there are another type of polynomials which are of particular interest.

Definition B.2.1 (Power Sum Polynomials)

The kth *power sum polynomial* for $k \geq 0$, $p_k \in R[X_1, \ldots, X_n]$, is defined by

$$p_k = X_1^k + \ldots + X_n^k.$$

Here is how they relate to the elementary symmetric polynomials.

Theorem B.2.1 (Newton's Formulas)

For any integer $k \geq 0$, we have

$$ke_k = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i} p_i = e_{k-1}p_1 - e_{k-2}p_2 + \ldots + (-1)^{k-1} p_k.$$

The main importance of these formulas is that they let us recover the e_i from the p_i by induction, as the RHS only has e_i for $i < k$. This is expressed in the following corollary.

Corollary B.2.1*

Let K be a field of characteristic zero. Then, $K(e_1, \ldots, e_n) = K(p_1, \ldots, p_n)$. In particular, if

$$p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n)$$

all lie in K, then so do

$$e_1(x_1, \ldots, x_n), \ldots, e_n(x_1, \ldots, x_n).$$

Remark B.2.1

This still holds in characteristic p as long as $n < p$, so that the k in ke_k is non-zero.

Exercise B.2.1*. Prove Corollary B.2.1.

Elementary Proof of Newton's Formulas

Let's compute the product $e_{k-1}p_i$. e_{k-i} is the sum of products of $k-i$ distinct variables, while p_i is the sum of the ith powers of all the variables. Thus, $e_{k-i}p_i$ is the sum of the product of the ith power of some variable, times $k-i$ distinct variables.

In the product of the $k-i$ distinct variable, either one of these variables will be the same as the one raised to the ith power, or not. Hence, we get $e_{k-i}p_i = r(i) + r(i+1)$ where $r(j)$ is the sum of products of one other variable raised to the $k-j$th power times j other distinct variables:

$$\sum_{i_1 < \ldots < i_{k-j}} X_{i_1} \cdot \ldots \cdot X_{i_{k-j}} \cdot \sum_{\ell \neq i_1, \ldots, i_{k-j}} X_\ell^j.$$

Thus,

$$\sum_{i=1}^{k} (-1)^{i-1} e_{k-i}p_i = (r(1)+r(2)) - (r(2)+r(3)) + \ldots + (-1)^k (r(k)+r(k+1)) = r(1) + (-1)^k r(k+1).$$

To conclude, $r(1) = ke_k$ and $r(k+1) = 0$ (there is no sum over -1 variables, or at least which is a homogeneous polynomial of degree k).

■

Proof of Newton's Formulas using Generating Functions

We now present a proof by generating functions. We work in $R[X_1, \ldots, X_k][[T]]$, i.e. the ring of

formal power series in T with coefficients in $R[X_1, \ldots, X_n]$. We have

$$(1 - X_1T) \cdot \ldots \cdot (1 - X_nT) = \sum_{k=0}^{n} (-1)^k e_k T^k$$

so, by differentiating, we get

$$\begin{aligned}
\sum_{k=0}^{n} (-1)^k k e_k T^k &= T \sum_{i=1}^{n} \left((-X_i) \prod_{j \neq i} (1 - X_j T) \right) \\
&= - \left(\sum_{i=1}^{n} \frac{X_i T}{1 - X_i T} \right) \prod_{j=1}^{n} (1 - X_j T) \\
&= - \left(\sum_{i=1}^{n} \sum_{j=1}^{\infty} (X_i T)^j \right) \left(\sum_{i=0}^{n} (-1)^i e_i T^i \right) \\
&= \left(\sum_{i=1}^{\infty} p_i T^i \right) \left(\sum_{j=0}^{n} (-1)^{i-1} e_i T^i \right).
\end{aligned}$$

By comparing the T^k coefficients, we get

$$(-1)^k = \sum_{o=1}^{k} (-1)^{k-i-1} p_i e_{k-i}$$

as wanted.

■

B.3 The Fundamental Theorem of Algebra

Recall the statement of the fundamental theorem of algebra, whose name was coined at a time where algebra was about solving polynomial equations.[1] In reality, it is a theorem about analysis and is usually proven that way. However, in this section we will present a mostly algebraic one (a completely algebraic proof is impossible because $\mathbb{R}$ is defined analytically).

Theorem B.3.1 (Fundamental Theorem of Algebra)

Any polynomial $f \in \mathbb{C}[X]$ of degree $n \geq 0$ has exactly n roots, i.e.,

$$f = a(X - \alpha_1) \cdot \ldots (X - \alpha_n)$$

where $\alpha_1, \ldots, \alpha_n$ are the roots of f counted with multiplicity and a is its leading coefficient.

By Proposition A.1.2, it suffices to show that any non-constant polynomial $f \in \mathbb{C}[X]$ has a root in $\mathbb{C}$. This is also called the d'Alembert-Gauss theorem because d'Alembert was the first one to recognise the importance of proving this result but gave a flawed proof, while Gauss was (almost) the first one to give a rigorous proof (in fact he even gave multiple proofs).

[1] Now it means abstract algebra and linear algebra, see Section A.2 and Appendix C (the section on abstract algebra does not give justice to the subject, since it was only about setting up useful definitions for this book).

Theorem B.3.2 (d'Alembert-Gauss Theorem)

Any polynomial non-constant polynomial with complex coefficients has a complex root.

Notice that we can assume the polynomial f has real coefficients, since if f has complex coefficients, $g = f\overline{f}$ has real coefficients where $\overline{f}$ denotes the polynomial obtained by applying complex conjugation to the coefficients of f. Thus, if we find a root α of g, either $\alpha \in \mathbb{R}$ in which case we can use induction on $\frac{g}{X-\alpha}$, or we know by Proposition A.1.6 that $\overline{\alpha}$ is also a root and we can use induction on $\frac{g}{(X-\alpha)(X-\overline{\alpha})}$. This would prove that g has as many complex roots as its degree, and thus f too.

We shall only use two results. The first one is a corollary of the intermediate value theorem, while the second one is left as an exercise.

Proposition B.3.1

Any polynomial $f \in \mathbb{R}[X]$ of odd degree has a real root.

Proof

Since f has odd degree, $f(-\infty)$ and $f(+\infty)$ have opposite signs so there is a root by the intermediate value theorem. (Here we work in $\mathbb{R} \cup \{+\infty, -\infty\}$, which is just a nice shortcut for not writing limits.)

■

Proposition B.3.2

Any polynomial $f \in \mathbb{C}[X]$ of degree 2 has a root $\mathbb{C}$.

Exercise B.3.1*. Prove Proposition B.3.2.

Proof that any non-constant polynomial with real coefficients has a complex root

Let $f \in \mathbb{R}[X]$ be a polynomial of degree n. We proceed by induction on $k = v_2(n)$; the case $k = 0$ is Proposition B.3.1. For the induction step, suppose $k \geq 1$ so that n is even.

Let $\alpha_1, \ldots, \alpha_n$ be the roots of f. You might wonder what that means since we don't know if they exist (in $\mathbb{C}$) or not. It's true that we don't know whether they lie in $\mathbb{C}$ or not yet, but we can *construct them formally*, just like i was constructed formally to be an object such that $i^2 = -1$. Thus we can construct $\alpha_1, \ldots, \alpha_n$ inductively such that f has n roots in some field K. (However, if you add a formal object α such that $g(\alpha)$ to a field, this will make a field only if g is irreducible. But you can factorise f into a product of irreducible polynomials then add a root of one of the factors and repeat. See Exercise 4.2.1*.)

Given a real number t, we consider the polynomial

$$g_t = \prod_{i<j} X - (\alpha_i + \alpha_j + t\alpha_i\alpha_j)$$

which has real coefficients by the fundamental theorem of symmetric polynomials: if $\prod_{i<j} X - (X_i + X_j + tX_iX_j) = h_t(X, e_1, \ldots, e_n)$ for some $h_t \in \mathbb{R}[X][X_1, \ldots, X_n]$, then

$$g_t = h_t(X, e_1(\alpha_1, \ldots, \alpha_n), \ldots, e_n(\alpha_1, \ldots, \alpha_n))$$

since $e_i(\alpha_1, \ldots, \alpha_n) \in \mathbb{R}$ by Vieta's formulas.

Notice that g_t has degree $\frac{n(n-1)}{2}$ and, since n is even, $v_2(\deg g_t) = n-1$. Hence, g_t always has a complex root $\alpha = \alpha_i + \alpha_j + t\alpha_i\alpha_j$ for some i, j by the induction hypothesis.

Now pick $\frac{n(n-1)}{2} + 1$ values of $0 \neq t \in \mathbb{R}$: by the pigeonhole principle two of them must have the same indices, $\alpha_i + \alpha_j + r\alpha_i\alpha_j$ is a complex root of g_r and $\alpha_i + \alpha_j + s\alpha_i\alpha_j$ is a complex root of g_s for the same i, j.

By subtracting these two numbers, we get $\alpha_i\alpha_j \in \mathbb{C}$. Similarly, we have $\alpha_i + \alpha_j \in \mathbb{C}$. Thus α_i and α_j are roots of a quadratic equation $X^2 - (\alpha_i + \alpha_j)X + \alpha_i\alpha_j$ with complex coefficients and hence also lie in $\mathbb{C}$ by Proposition B.3.2. In particular, we have found a complex root of f as wanted.

■

B.4 Exercises

Newton's Formulas

Exercise B.4.1. Denote by $h_k \in R[X_1, \ldots, X_n]$ the kth *complete homogeneous polynomial*, i.e. the sum of all monomials of degree k. Prove that

$$kh_k = \sum_{i=1}^{k} h_{k-i}p_i = h_{k-1}p_1 + h_{k-2}p_2 + \ldots + p_k$$

for any $k \geq 0$.

Exercise B.4.2† (Hermite's Theorem)**.** Prove that a function $f : \mathbb{F}_p \to \mathbb{F}_p$ is a bijection if and only if $\sum_{a\in\mathbb{F}_p} f(a)^k$ is 0 for $k = 1, \ldots, p-2$ and -1 for $k = p-1$.

Exercise B.4.3†**.** Suppose that $\alpha_1, \ldots, \alpha_n$ are such that $\alpha_1^k + \ldots + \alpha_k^n$ is an algebraic integer for all n. Prove that $\alpha_1, \ldots, \alpha_k$ are algebraic integers.

Algebraic Geometry[2]

Exercise B.4.4† (Resultant)**.** Let R be a commutative ring, and $f, g \in R[X]$ be two polynomials of respective degrees m and n. For any integer $k \geq 0$, denote by $R_k[X]$ the subset of $R[X]$ consisting of polynomials of degree less than k. The *resultant* $\mathrm{Res}(f, g)$ is defined as the determinant of the linear map

$$(u, v) \mapsto uf + vg$$

from $R_m[X] \times R_n[X]$ to $R_{m+n}[X]$. Prove that, if $f = \sum_i a_i X^i$ and $g = \sum_i b_i X^i$, we have[3]

$$\mathrm{Res}(f,g) = \begin{vmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \cdots & 0 & b_1 & b_0 & \cdots & 0 \\ a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 \\ a_m & a_{m-1} & \cdots & \vdots & b_n & b_{n-1} & \cdots & \vdots \\ 0 & a_m & \ddots & \vdots & 0 & b_n & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_{m-1} & \vdots & \vdots & \ddots & b_{n-1} \\ 0 & 0 & \cdots & a_m & 0 & 0 & \cdots & b_n \end{vmatrix},$$

[2]The link with symmetric polynomials is quite feeble, I admit. I included this section because of the resultant, which is a polynomial symmetric in the roots of its arguments.

[3]This is an $(m+n) \times (m+n)$ matrix, with n times the element a_0 and m times the element b_0.

and, if $f = a\prod_i X - \alpha_i$ and $g = b\prod_j X - \beta_j$, then[4]

$$\mathrm{Res}(f,g) = a^m b^n \prod_{i,j} \alpha_i - \beta_j.$$

In addition, prove that $\mathrm{Res}(f,g) \in (fR[X] + gR[X])$.[5] Finally, prove that if $f, g \in \mathbb{Z}[X]$ are monic and $uf+vg = 1$ for some $u, v \in \mathbb{Z}[X]$, $\mathrm{Res}(f,g) = \pm 1$. (It is not necessarily true that $(fR[X]+gR[X])\cap R = \mathrm{Res}(f,g)R$ for specific polynomials f, g, but we always have $\mathrm{Res}(f,g) \in fR[X]+gR[X]$ by the previous point.)

Exercise B.4.5. Prove that

- $\mathrm{Res}(fg,h) = \mathrm{Res}(f,h)\,\mathrm{Res}(g,h)$ for any $f, gh \in R[X]$.
- $\mathrm{Res}(f-gh,g) = b^{k-n}\,\mathrm{Res}(f,g)$ for any $f, g, h \in R[X]$ where k is the degree of $f-gh$, n is the degree of g and b its leading coefficient.
- $\mathrm{Res}(F(f,g),G(f,g)) = \mathrm{Res}(F,G)^k\,\mathrm{Res}(f,g)^{mn}$ where $F, G, f, g \in R[X,Y]$ are homogeneous polynomials of respective degrees m, n, k, k. Here, by $\mathrm{Res}(A,B)$ for homogeneous $A, B \in R[X,Y]$, we mean $\mathrm{Res}(A(X,1),B(X,1))$.

Exercise B.4.6† (Hilbert's Nullstellensatz)**.** Let K be an algebraically closed field. Suppose that $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ have no common zeros in K. Prove that there exist polynomials $g_1, \ldots, g_m$ such that

$$f_1 g_1 + \ldots + f_m g_m = 1.$$

Deduce that, more generally, if f is a polynomial which is zero at common roots of polynomials $f_1, \ldots, f_m$ (we do not assume anymore that they have no common roots), then there is an integer k and polynomials $g_1, \ldots, g_m$ such that

$$f^k = f_1 g_1 + \ldots + f_m g_m.$$

Exercise B.4.7† (Weak Bézout's Theorem)**.** Prove that two coprime polynomials $f, g \in K[X,Y]$ of respective degrees m and n have at most mn common roots in K. (Bézout's theorem states that they have exactly mn common roots counted with multiplicity, possibly at infinity.[6])

Exercise B.4.8†**.** Prove that $n+1$ polynomials $f_1, \ldots, f_{n+1} \in K[X_1, \ldots, X_n]$ in n variables are *algebraically dependent*, meaning that there is some non-zero polynomial $f \in K[X_1, \ldots, X_{n+1}]$ such that

$$f(f_1, \ldots, f_{n+1}) = 0.$$

Exercise B.4.9† (Transcendence Bases)**.** Let L/K be a field extension. Call a maximal set of K-algebraically independent elements of L a *transcendence basis*. Prove that, if L/K has a transcendence basis of cardinality n, then all transcendence bases have cardinality n. This n is called the *transcendence degree* $\mathrm{trdeg}_K L$. Finally, show that, if $L = K(\alpha_1, \ldots, \alpha_n)$ any maximal algebraically independent subset of $\alpha_1, \ldots, \alpha_n$ is a transcendence basis. (In particular $\mathrm{trdeg}_K L \leq n$.)

Exercise B.4.10†**.** Let K be an algebraically closed field which is contained in another field L. Suppose that $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ are polynomials with a common root in L. Prove that they also have a common root in K.

---

[4] In particular, the discriminant of f is $\frac{(-1)^{\frac{n(n-1)}{2}}}{a} \cdot \mathrm{Res}(f, f')$.

[5] In other words, the resultant provides an explicit value of a possible constant in Bézout's lemma for arbitrary rings (such as $\mathbb{Z}$).

[6] This requires some care: we need to define the multiplicity of common roots as well as what infinity means. See any introductory text to algebraic geometry, e.g. Sharevich [**shafarevich**]. See also the appendix on projective geometry of Silverman-Tate [26].

Miscellaneous

Exercise B.4.11† (ISL 2020 Generalised)**.** Let $n \geq 1$ be an integer. Find the maximal N for which there exists a monomial f of degree N which can not be written as a sum

$$\sum_{i=1}^{n} e_i f_i$$

with $f_i \in \mathbb{Z}[X_1, \ldots, X_n]$.

Exercise B.4.12† (Lagrange)**.** Given a rational function $f \in K[X_1, \ldots, X_n]$, we denote by G_f the set of permutations $\sigma \in \mathfrak{S}_n$ such that

$$f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Let $f, g \in K(X_1, \ldots, X_n)$ be two rational functions. If $G_f \subseteq G_g$, prove that there exists a rational function $r \in K[e_1, \ldots, e_n](X)$ such that

$$g = r \circ f.$$

Exercise B.4.13† (Iran Mathematical Olympiad 2012)**.** Prove that there exists a polynomial $f \in \mathbb{R}[X_0, \ldots, X_{n-1}]$ such that, for all $a_0, \ldots, a_{n-1} \in \mathbb{R}$,

$$f(a_0, \ldots, a_{n-1}) \geq 0$$

is equivalent to the polynomial $X^n + a_{n-1}X^{n-1} + \ldots + a_0$ having only real roots, if and only if $n \in \{1, 2, 3\}$.

Exercise B.4.14. Let $f \in K[X]$ be a monic polynomial with roots $\alpha_1, \ldots, \alpha_n$. Prove that its discriminant, as defined in Remark 1.3.2 or Exercise B.4.4† is equal to

$$(-1)^{\frac{n(n-1)}{2}} \cdot \prod_{i=1}^{n} f'(\alpha_i).$$

Deduce a formula for the discriminant of $X^n + aX + b$ and show that it is valid over any ring (not necessarily one where $X^n + aX + b$ has at most n roots[7]).

[7] Remember that Corollary A.1.1 is valid only over fields and integral domains.

Appendix C

Linear Algebra

Prerequisites for this chapter: Section A.1. Section A.2 is recommended.

C.1 Vector Spaces

Definition C.1.1 (Vector Space)

A *vector space* V over a field K, also called a K-vector space, is a set where you can add elements of V and also mutliply them by elements of K. More specifically, we have the following axioms.

1. associativity of addition: $(u+v)+w = u+(v+w)$ for any $u, v, w \in V$.
2. commutativity of addition: $u+v = v+u$ for any $u, v \in V$.
3. identity of addition: there is a $0_V \in V$ such that $u + 0_V = 0_V + u$ for any $u \in V$.
4. compatibility of multiplication: $(ab)v = a(bv)$ for any $a, b \in K$ and $v \in V$.
5. identity of multiplication: $1_K v = v$ for any $v \in V$ (1_K is the identity of K).
6. disitributy of multiplication: $a(u+v) = au + av$ and $u(a+b) = ua + ub$ for any $a, b \in K$ and $u, v \in V$.

The elements of the base field K are called *scalars* (and the elements of V *vectors*, although we won't use this termniology much).

These axioms are again all very obvious and you don't need to try to remember them, they are exactly the properties which let us establish the next propositions (that's why we defined it like that) so you just need to focus on what's next. As an example of vector spaces one can take the K-vector space K, the K-vector space K^n with componentwise addition and multiplication (these are regular vectors), $\mathbb{Z}/p^n\mathbb{Z}$ as a $\mathbb{F}_p$-vector space, and as a final more elaborate example the $\mathbb{R}$-vector space of functions $f : \mathbb{R} \to \mathbb{R}$ such that $f(0) = 0$ (it's closed under addition).

When the base field is obvious from context or does not matter, we will drop the K.

Definition C.1.2 (Linear Independence)

We say elements $u_1, \ldots, u_n$ of a K-vector space V are *linearly independent* if no non-trivial linear combination of them is zero, i.e. $\sum_i a_i u_i = 0$ for $a_i \in K$ implies $a_i = 0$ for all i. Otherwise, we say they are *linearly dependent*.

For instance, the vectors $(1,0)$ and $(0,1)$ are linearly independent but the vectors $(1,0)$, $(0,1)$ and $(1,1)$ aren't because $(1,0) + (0,1) - (1,1) = 0$.

Definition C.1.3 (Bases)

A *K-basis* of a K-vector space V is a family of linearly independent elements $(e_i)_{i\in I}$ such that they span all of V: any element of V is a unique linear combination $\sum_i a_i e_i$ for some $a_i \in K$ (all but finitely many zero so that the sum makes sense).

The most common basis of $\mathbb{R}^n$ for instance is family set of unit vectors

$$(1, 0 \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, \ldots, 0, 1).$$

The next proposition says that the cardinality of a basis (if there is one) does not depend on the basis, but only on the vector space. But first, here is an application (even though we have only made definitions!). When the base field K is obvious, we will drop the K and simply say "basis" and "vector space".

Problem C.1.1

There are $2n+1$ cows such that, whenever one exludes one of them, the rest can be divided into two groups of size n such that the sum of the weights of the cows in each group is the same. Prove that all cows have the same weight.

Solution

Let w_i be the weight of the ith cow. First, we solve the problem by induction when the weights are in $\mathbb{Z}$: if $\sum_{i\in I_k} w_i = \sum_{i\notin I_k, i\neq k} w_i$ then

$$\sum_{i=1}^{2n+1} w_i = w_k + \sum_{i\in I_k} w_i + \sum_{i\notin I_k, i\neq k} w_i \equiv w_k \pmod 2$$

so all weights have the same parity. If they are all even divide them by 2 and get a smaller solution (unless they are all equal to 0 in which case they are indeed equal), otherwise add 1 to all of them and divide them by 2; this yields another solution as the groups have the same size by assumption.

Now solve the problem over $\mathbb{Q}$: just multiply the weights by the lcm of the denominators to get weights in $\mathbb{Z}$ and we have already solved that case.

Finally, let's do the general case: $w_i \in \mathbb{R}$. Consider the $\mathbb{Q}$-vector space generated by the weights: $V = w_1\mathbb{Q} + \ldots + w_{2n+1}\mathbb{Q}$. Find a basis of V like this: pick any maximal subset of weights which are linearly independent $(w_i)_{i\in I}$. Indeed, any other weight w_k can be represented as a linear combination of $(w_i)_{i\in I}$ since there is a linear combination

$$aw_k + \sum_{i\in I} a_i w_i = 0$$

as $(w_k) \cup (w_i)_{i\in I}$ is linearly dependent by assumption, so

$$w_k = \sum_{i\in I} \frac{-a_i}{a} w_i$$

as $a \neq 0$ (otherwise $(w_i)_{i\in I}$ are linearly dependent).

Thus, we have found a basis $e_1, \ldots, e_m$ of V. To finish, write each w_i as $\sum_j a_{j,i} e_j$. We shall prove that $a_{j,1}, a_{j,2}, \ldots, a_{j,2n+1}$ satisfy the same conditions as the w_i (you can partition them into two groups of same sum and same size when you remove any one of them) for any j. Since

they are in $\mathbb{Q}$, by our prevous step this implies that they are all equal and thus the weights w_i are also all equal. This is however very easy: if $\sum_{i\in I} w_i = \sum_{i\in I'} w_i$ then

$$\sum_j e_j \sum_{i\in I} a_{j,i} = \sum_j e_j \sum_{i\in I'} a_{j,i}$$

so $\sum_{i\in I} a_{j,i} = \sum_{i\in I'} a_{j,i}$ by definition of a basis. We are done. ■

Now, we prove that any basis has the same cardinality if there exists a finite one. In that case we say the vector space is *finite-dimensional*. Unless otherwise stated, we will always work in the finite-dimensional case.

Proposition C.1.1 (Dimension)

Suppose $e_1, \ldots, e_n$ is a basis of a vector space V. Then, any basis of V has cardinality n. This n is called the *dimension* of V and written $\dim_K V$.

In fact we prove more.

Proposition C.1.2

Suppose $u_1, \ldots, u_n$ are linearly independent elements of V and $v_1, \ldots, v_m$ span all of V. Then $m \geq n$.

Since bases satisfy both of these conditions, we get $n \geq m$ and $m \geq n$ so $m = n$ for any bases of cardinality m and n.

Proof

We prove the contraposite: if $n > m$ then $u_1, \ldots, u_n$ are linearly dependent. Write $u_j = \sum_i a_{i,j} v_i$ with $a_{i,j} \in K$. We proceed by induction on m (when $m = 1$ it is obvious).

Pick an $a_{i,j} \neq 0$, this is possible otherwise all u_i are zero so in particular linearly dependent; without loss of generality assume $i = j = 1$. We will get rid of u_i and v_j for our induction. To do so, consider the family of vectors

$$u_1, u_2 - \frac{a_{1,2}}{a_{1,1}} u_1, u_3 - \frac{a_{1,3}}{a_{1,1}} u_1, \ldots, u_n - \frac{a_{1,n}}{a_{1,1}} u_1.$$

Clearly, these are linearly independent since you can recover $u_1, \ldots, u_n$ from them. Also,

$$u_j - \frac{a_{1,j}}{a_{1,1}} u_1 = \sum_{j\geq 2} (a_{i,j} - a_{1,i} a_{1,i} / a_{1,1}) v_i$$

has no coordinate in v_1. Thus by our induction hypothesis (e.g. on V' the space generated by $v_2, \ldots, v_m$) $u_2, \ldots, u_n$ are linearly dependent and we are done. (This idea of getting rid of coordinates will be used again in the proof of Theorem C.3.1, which states that the determinant of linearly independent vectors is non-zero.)

■

Here is a small application.

Problem C.1.2

Let $f, g \in \mathbb{R}[X]$ be two non-constant polynomials. Prove that there is an $h \in \mathbb{R}[X]$ such that fh is a polynomial in g.

Solution

This amounts to saying that some multiple of f is a polynomial in g. Let $n = \deg f$. We work in $\mathbb{R}[X]/f\mathbb{R}[X]$, i.e. $\mathbb{R}[X]$ modulo f. This an $\mathbb{R}$-vector space of dimension n as $(1, X, \dots, X^{n-1})$ is a basis.

Now consider the $n+1$ elements $1, g, g^2, \dots, g^n$, where g^k denotes the kth iterate of g. Since this family has more elements than the dimension of the vector space, they are linearly dependent: we get

$$\sum_i a_i g^i \equiv 0 \pmod{f}$$

for some not all zero $a_i \in \mathbb{R}$. This constitutes the wanted multiple of f. ■

Remark C.1.1

As this solution shows, the problem is extremely flexible. For instance, for any infinite set of non-negative integers S (e.g. the set of primes), f has a multiple whose non-zero monomials have the form X^s for some $s \in S$.

A final important result on basis, that we already saw in the proof of Problem C.1.1, is that we can always complete a family of linearly independent vectors to get a basis.

Proposition C.1.3

Any family of linearly independent vectors of a finite-dimensional vector space V can be completed into a basis by adding elements to it, and from any generating family we can extract a basis.

Exercise C.1.1*. Prove Proposition C.1.3.

As always, a quick application to finite fields. In Chapter 4 we prove that there exist fields of cardinality q for every prime power $q = p^n \neq 1$. Here we show the converse: if F is a field with q elements, then q is a prime power.

Proposition C.1.4

Suppose F is a field with q elements. Then there is some prime p and an integer n such that $q = p^n$.

Proof

The key is to consider F as a vector space over $\mathbb{F}_p$, where p is the characteristic of F. Indeed, the characteristic c is a prime, since if $0 = c = ab$ then either a or b must be zero too which means $a = c$ or $b = c$ by minimality of c.

Now F is a $\mathbb{F}_p$-vector space in the obvious way: just define $nx = \underbrace{x + \dots + x}_{n \text{ times}}$ (technically that's what we did before with the characteristic too) and this is compatible with $\mathbb{F}_p$ as $p = 0$ in F.

Since F is finite, it is also finite-dimension as a vector space: let $e_1, \dots, e_n$ be a basis (there exists one by Proposition C.1.3). Then, every element of F can be written in a unique way as

$$\sum_{i=1}^{n} a_i e_i$$

for some $a_i \in \mathbb{F}_p$. There are exactly p^n tuples $(a_1, \dots, a_n) \in \mathbb{F}_p$, so $q = p^n$ as wanted.

■

C.2 Linear Maps and Matrices

In this section, we consider morphisms of vector spaces which are called *linear maps*, or *linear transformations*.[1]

Definition C.2.1 (Linear Maps)

Let U and V be two K-vector spaces. A *linear map* $\varphi : U \to V$ is a function which is additive and homogeneous, i.e. $\varphi(x+y) = \varphi(x) + \varphi(y)$ and $\varphi(\lambda x) = \lambda\varphi(x)$ for any $x, y \in U$ and $\lambda \in K$.

For instance, the derivative map $f \mapsto f'$ is a linear map from $K[X]$ to itself (as K-vector spaces).

There is a very simple characterisation of linear maps $U \to V$. Let $u_1, \dots, u_m$ be a basis of U and $v_1, \dots, v_n$ of V. Write

$$\varphi(u_j) = \sum_i a_{i,j} v_i$$

for $j = 1, \dots, m$. Then f is uniquely defined from these $a_{i,j}$, and any system of $a_{i,j}$ gives rise to a linear map $U \to V$: if $x = \sum_j b_j u_j$ then

$$\varphi(x) = \sum_{i,j} b_j a_{i,j} v_i.$$

Note in particular that this shows that the structure of finite-dimensional vector spaces is more or less trivial: a vector space of dimension n is isomorphic to K^n. However, the profoundness of linear algebra lies precisely in what these isomorphisms are.

Remark C.2.1

When $K = \mathbb{Q}$, the $\mathbb{Q}$-linear maps are precisely the additive maps. Indeed, it follows from additivity that $\varphi(nx) = n\varphi(x)$ for $n \in \mathbb{Z}$, which implies that

$$\varphi\left(\frac{m}{n}x\right) = \frac{\varphi(mx)}{n} = \frac{m}{n}\varphi(x).$$

Additive functions are also called functions satisfying the "Cauchy equation" ($\varphi(x+y) = \varphi(x) + \varphi(y)$). This explains why this equation is unsolvable over $\mathbb{R}$: $\mathbb{R}$ is an infinite-dimensional $\mathbb{Q}$-vector space, so there are **a lot** of solutions: "just" pick a basis $(u_i)_{i \in I}$ of $\mathbb{R}$ and send u_i wherever you want. (It is however impossible, in the general case, to prove the existence of a basis of an infinite-dimensional vector space without the axiom of choice.)

Let us now comment a bit our proof of Lagrange's interpolation theorem A.1.2. What we did was consider the canonical basis $e_1, \dots, e_{n+1}$ where e_i has a 1 in the ith position and zeros everywhere else

[1] This shows that one should not call polynomial functions of degree 1 "linear", because they are not linear maps (unless the constant coefficient is 0)! One should call them "affine", because they correspond to affine transformations, not linear ones.

of the space K^{n+1} consisting of vectors $(b_1, \dots, b_{n+1})$. Then, for each element of this basis, we found polynomials f_i such that

$$(f_i(a_1), \dots, f_i(a_n)) = e_i.$$

Finally, we get the wanted result by taking linear combinations of these f_i since $e_1, \dots, e_{n+1}$ is a basis.

We come back to more abstract considerations. Given the bases $\mathcal{B} = (u_1, \dots, u_m)$ and $\mathcal{C} = (v_1, \dots, v_n)$, we denote the linear map φ in matrix form relative to the bases $\mathcal{B}$ and $\mathcal{C}$ by

$$M_{\mathcal{B}}^{\mathcal{C}}(\varphi) = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{bmatrix}.$$

Note that we have used the index j for elements of the domain, and the index i for the codomain. This means that, to get the matrix of φ, we represent $\varphi(u_1), \dots, \varphi(u_m)$ by **column** vectors:

$$\begin{bmatrix} a_{1,1} \\ a_{2,1} \\ \vdots \\ a_{m,1} \end{bmatrix}, \dots, \begin{bmatrix} a_{1,n} \\ a_{2,n} \\ \vdots \\ a_{m,n} \end{bmatrix}$$

and then piece them together.

Definition C.2.2 (Matrices)

An $m \times n$ matrix is a family $(a_{i,j})_{i,j \in [m] \times [n]}$ which is denoted by $\begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{bmatrix}$. The set of $m \times n$ matrices with coefficients in K is denoted by $K^{m \times n}$; when $n = 1$ we just write K^m.

Note that this last notation clashes with the Cartesian product, and that an element of K^m is a column vector not a row vector! To make things worse, we will even denote elements of K^m by $(a_1, \dots, a_m)$ as column vectors take too much place.

Here is how we define the product of two matrices A and B: if $A = M_{\mathcal{C}}^{\mathcal{B}}(\psi)$ and $S = M_{\mathcal{D}}^{\mathcal{C}}(\varphi)$ where $U \underset{\varphi}{\to} V \underset{\psi}{\to} W$, we want AB to correspond to $M_{\mathcal{D}}^{\mathcal{B}}(\psi \circ \varphi)$ where $D = (w_1, \dots, w_\ell)$ is a basis of W. Thus we compute

$$\psi(\varphi(u_j)) = \psi\left(\sum_k b_{k,j} v_k\right) = \sum_k b_{k,j} \psi(v_k) = \sum_k b_{k,j} \sum_i a_{i,k} w_i = \sum_i w_i \sum_k a_{i,k} b_{k,j}.$$

Hence we define $(a_{i,j})(b_{i,j}) = (c_{i,j})$ where $c_{i,j} = \sum_k a_{i,k} b_{k,j}$ (scalar product of the ith row of A with jth column of B). (In particular, the product of two matrices is only defined when the coordinates agree: $m \times n$ and $n \times \ell$.)

Definition C.2.3 (Matrix Multiplication)

The product of two matrices $(a_{i,j})$ and $(b_{i,j})$ of dimensions $m \times n$ and $n \times \ell$ is the matrix $(c_{i,j})$ of dimension $m \times \ell$ given by $c_{i,j} = \sum_k a_{i,k} b_{k,j}$.

Matrix multiplication is clearly associative, since composition is. It is however **not-commutative** in general. Similarly, addition of matrices is defined componentwise because we want $M_{\mathcal{C}}^{\mathcal{B}}(\varphi) + M_{\mathcal{C}}^{\mathcal{B}}(\psi)$ to correspond to $\varphi + \psi$. (We do not define multiplication of matrices to correspond to multiplication of linear maps because this does not make sense: $x \mapsto x \cdot x$ is not linear.)

Exercise C.2.1*. Prove that $\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}\begin{bmatrix}1 & 1\\0 & 0\end{bmatrix} = \begin{bmatrix}1 & 1\\0 & 0\end{bmatrix}$ but $\begin{bmatrix}1 & 1\\0 & 0\end{bmatrix}\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}$.

Exercise C.2.2*. Prove that matrix multiplication is *distributive* over matrix addition, i.e. $A(B+C) = AB + AC$ and $(A+B)C = AC + BC$ for any A, B, C of compatible dimensions.

Suppose we want to *invert* a linear map, i.e. find another linear map φ^{-1} such that $\varphi \circ \varphi^{-1} = \mathrm{id}$. The matrix of the identity is very simple to describe (with one basis): it's the matrix with ones on the diagonal and zero everywhere else

$$M_{\mathcal{B}}^{\mathcal{B}}(\mathrm{id}) = \begin{bmatrix}1 & 0 & \dots & 0\\0 & 1 & \dots & 0\\\vdots & \vdots & \ddots & \vdots\\0 & 0 & \dots & 1\end{bmatrix} := I_n$$

since

$$\mathrm{id}(e_j) = e_j = 0e_1 + \ldots + 0e_{j-1} + e_j + 0e_{j+1} + \ldots + 0e_n.$$

This matrix is called the *identity matrix*. Thus we would like to *invert* matrices. Why would this be useful? Well, this lets us, for instance, perform *changes of bases*: imagine that we first expressed φ with respect to the bases $\mathcal{B} = (u_1, \ldots, u_m)$ and $\mathcal{C} = (v_1, \ldots, v_n)$, but then we decided we actually preferred to express it with respect to $\mathcal{B}' = (u'_1, \ldots, u'_m)$ and $\mathcal{C}' = (v'_1, \ldots, v'_m)$. Consider the following two linear maps $\varphi_U(u_j) = u'_j$ and $\varphi_V(v_j) = v'_j$. It is clear that

$$M_{\mathcal{C}'}^{\mathcal{B}'}(\varphi) = M_{\mathcal{C}}^{\mathcal{B}}(\varphi_V \circ \varphi \circ \varphi_U^{-1})$$

since if $\varphi(u_j) = \sum_i a_{i,j} v_i$, then composing with φ_U^{-1} on the right transforms u_j into u'_j and composing with φ_V on the left transforms v_i into v'_i.

Thus,

$$M_{\mathcal{C}'}^{\mathcal{B}'}(\varphi) = M_{\mathcal{C}}^{\mathcal{B}}(\varphi_V) M_{\mathcal{C}}^{\mathcal{B}}(\varphi_U)^{-1}$$

(the matrices $M_{\mathcal{C}}^{\mathcal{B}}(\varphi_V)$ and $M_{\mathcal{C}}^{\mathcal{B}}(\varphi_U)^{-1}$ are called *change of bases matrices*). Of particular interest is the case where $U = V$, $\mathcal{B} = \mathcal{C}$ and $\mathcal{B}' = \mathcal{C}'$. In that case, we get an equality of the form $M' = NMN^{-1}$.

Finally, we prove one last result linking the surjectivity and injectivity of a linear map: if a linear map from a vector space to itself is injective, then it is surjective too and conversely. This is false in the infinite-dimension case, but this does not affect as as we only care about the finite-dimensional one. Recall what the kernel and image of a morphism are. Note that if φ is linear, then $\ker\varphi$ and $\mathrm{im}\,\varphi$ are vector spaces (as they are closed under addition, as well as multiplication by scalars).

Definition C.2.4 (Kernel and Image)

Let $\varphi : U \to V$ be a linear map. Its kernel $\ker\varphi$ is the set of $u \in U$ such that $\varphi(u) = 0$, and its image is the set of $v \in V$ such that $\varphi(u) = v$ for some $u \in U$.

Theorem C.2.1 (Rank-Nullity Theorem)

Suppose $\varphi : U \to V$ is a linear map (of finite-dimensional vector spaces). Then, $\dim\ker\varphi + \dim\mathrm{im}\,\varphi = \dim U$.

Remark C.2.2

This is called the "rank-nullity theorem" because $\dim\mathrm{im}$ is also called the rank, and nullity means $\dim\ker$.

Proof

Let $u_1, \ldots, u_k$ be a basis of $\ker \varphi$ and $\varphi(u'_1), \ldots, \varphi(u'_m)$ a basis of $\operatorname{im} \varphi$. We prove that $u_1, \ldots, u_k, u'_1, \ldots, u'_m$ is a basis of U.

First we prove that these elements are linearly independent. Suppose that

$$\sum_i a_i u_i + \sum_i b_i u'_i = 0.$$

Then, $\sum_i b_i f(u'_i) = 0$ by composing with f. Since $f(u'_1), \ldots, f(u'_m)$ are linearly independent, this means $b_1 = \ldots = b_m = 0$. Then, from $\sum_i a_i u_i = 0$, we deduce $a_i = 0$ since $u_1, \ldots, u_k$ are also linearly independent.

It remains to prove that they span all of U. Let $u \in U$ be an element. Write $f(u) = \sum_i b_i f(u'_i)$. Then, $f\left(u - \sum_i b_i u'_i\right) = 0$. This means $u - \sum_i b_i u'_i \in \ker f$, so

$$u - \sum_i b_i u'_i = \sum_i a_i u_i \iff u = \sum_i a_i u_i + \sum_i b_i u'_i$$

as wanted.

■

Corollary C.2.1*

A linear map $U \to U$ is injective if and only if it is surjective. In other words, a square matrix has a right-inverse if and only if it has a left-inverse.

Proof

A linear map is injective if and only if its kernel is trivial, i.e. has dimension 0. By the rank-nullity theorem, this is equivalent to $\dim \operatorname{im} \varphi = \dim U$, i.e. φ being surjective.

A $n \times n$ matrix A has a right-inverse if and only if the linear map from $K^{n \times n} \to K^{n \times n}$ defined by $B \mapsto AB$ is surjective, and if A^{-1} is this inverse then $A(A^{-1}A) = A$ so $A^{-1}A = I_n$ by injectivity (from the rank-nullity theorem) which means A^{-1} is a left inverse too. But if A has a left-inverse, then $B \mapsto AB$ is injective which means it's surjective too.

■

Another corollary is that this lets us deduce the existence part of the Lagrange interpolation theorem (Theorem A.1.2) from the uniqueness part: for any $a_1, \ldots, a_n \in K$, the map from the vector space $K_n[X]$ of polynomials of degree less than n to K^n given by

$$f \mapsto (f(a_1), \ldots, f(a_n))$$

is injective so must be surjective too since $K_n[X]$ and K^n both have dimension n.

Here is a combinatorial application of the fact that the right-inverse of a matrix is also its left-inverse.

Problem C.2.1

There are $2n$ boys and $2n$ girls at a party. For each pair of girls, there are exactly n boys that danced with exactly one of them. Prove that the same is true if we exchange the words "boys" and "girls" in the last sentence.

Solution

Consider the *adjacency matrix* $M = (a_{i,j})$ defined by $a_{i,j} = 1$ if the ith girl and the jth boy have danced together and -1 otherwise (so the rows correspond to the girls and the columns to the boys). We claim that the condition of the problem is exactly equivalent to

$$MM^\mathsf{T} = 2nI_{2n},$$

where M^T designates the *transpose matrix* of M, i.e. the matrix $M^\mathsf{T} = (b_{i,j})$ where $b_{i,j} = a_{j,i}$ (exchange the rows with the columns). Let's compute this product: the (i, j) coordinate is

$$c_{i,j} = \sum_k a_{i,k} b_{k,j} = \sum_k a_{i,k} a_{j,k}.$$

Now what is $a_{i,k}a_{j,k}$? $a_{i,k}$ corresponds to whether the ith girl has danced with the kth boy, and $a_{j,k}$ to whether the jth girl has danced with the kth boy. Thus $a_{i,k}a_{j,k}$ is $-1 = 1 \cdot (-1) = (-1) \cdot 1$ if exactly one of them has danced with him, and $1 = 1 \cdot 1 = (-1)(-1)$ otherwise.

We conclude that the sum $\sum_k a_{i,k}a_{j,k}$ is zero if and only if there are exactly n boys which danced with exactly one of the girls i, j: for $i \neq j$ this is exactly what the problem says! For $i = j$ the sum is trivial: $a_{i,k}^2 = 1$ so $c_{i,j} = \sum_k 1 = 2n$. We have thus proven our claim: the condition is equivalent to $MM^\mathsf{T} = 2nI_{2n}$, i.e. that $M^\mathsf{T}/2n$ is the right-inverse of M. But then $M^\mathsf{T}/2n$ is also the left-inverse of M by the rank-nullity theorem, so

$$\frac{1}{2n} M^\mathsf{T} M = I_{2n} \iff M^\mathsf{T}(M^\mathsf{T})^\mathsf{T} = 2nI_{2n}$$

which means that the statement is true with the word "boys" and "girls" exchanged (since this is what the transpose does: it exchanges the rows with the columns). ■

C.3 Determinants

The set of matrices almost form a **non-commutative** ring under addition and multiplication, except that multiplication is not always defined (only when the dimensions are compatible). However, for square matrices it is always possible. Thus, square matrices are usually nicer to study, for instance we have seen that they have a right-inverse and if and only they have a left-inverse, which is not true for other matrices (by the rank-nullity theorem). In this section, we find a criterion to determine those square matrices are invertible. Note that finding when a $n \times n$ matrix M is invertible is equivalent to finding when the rows or the columns are linearly independent. Indeed, the column are linearly independent if and only if the images of the canonical basis

$$e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)$$

by the linear map $v \mapsto Av$ from K^n to K^n are linearly independent, i.e. if and only if this map is injective (which is equivalent to A being invertible). For the rows, one can consider the map $v \mapsto A^\mathsf{T} v$, as $(AB)^\mathsf{T} = B^\mathsf{T} A^\mathsf{T}$ so A is invertible if and only if its transpose is.

Exercise C.3.1. Prove that an $m \times n$ matrix can only have a right-inverse if $m < n$, and only a left-inverse if $m > n$. When does such an inverse exist?

Exercise C.3.2*. Prove that $(AB)^\mathsf{T} = B^\mathsf{T} A^\mathsf{T}$ for any $n \times n$ matrices A, B.

Let's start with the 2×2 case. Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be such a matrix. The vectors (a, b) and (c, d) are linearly dependent if and only if there are some x, y such that $(ax + cy, bx + dy) = (0, 0)$. By rescaling x and y if necessary, we may assume $x = -c$ and $y = a$ from $ax + cy = 0$ (unless $a = c = 0$ but in that case they're clearly linearly dependent). Then, $bx + dy = 0$ becomes $ad - bc = 0$.

Thus, $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible if and only if $ad - bc \neq 0$. In fact, we can even check that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = (ad - bc) I_2.$$

Exercise C.3.3. Prove this identity.

This number $ad - bc$ is called the *determinant* $\det M$ of the matrice $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Our goal will be to define such a determinant for $n \times n$ matrices satisfying the following properties:

- $\det M$ is a homogeneous polynomial of degree n in the coordinates of M. Moreover, $\det M$ has degree 1 in each coordinate of M.
- M is invertible if and only if $\det M \neq 0$.

In fact, these properties define uniqueley the determinant up to leading coefficient (this will be proven in Theorem C.3.4)!For the sake of convenience, since we are going to be talking more about columns and rows, we denote the ith row of M by M_i and the jth column of M by M^j so that

$$M = [M^1, \cdots, M^n] = \begin{bmatrix} M_1 \\ \vdots \\ M_n \end{bmatrix}.$$

Here is how one can define the determinant of $n \times n$ matrices inductively. In Theorem C.3.4 and Theorem C.3.3, we will give another characterisations of the determinant, the last one being completely explicit. The reader may wish to take it for granted that the determinant exists for now, skip to Problem C.3.1 to see an application and come back later to read the proofs.

Definition C.3.1 (Determinant)

Let $A = (a_{i,j})$ be a matrix. Denote by $A_{i,j}$ the matrix obtained by removing the ith row and the jth column. We define the *determinant* inductively by $\det[a] = a$ and

$$\det A = a_{1,1} \det A_{1,1} - a_{2,1} A_{2,1} + \ldots + (-1)^n a_{n,1} A_{n,1}.$$

Remark C.3.1

We shall also sometimes denote the determinant of $\begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix}$ as

$$\begin{vmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{vmatrix}.$$

Here is an example for the determinant of 3×3 matrices.

$$\begin{aligned} \det \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} &= a_{1,1} \det \begin{bmatrix} a_{2,2} & a_{2,3} \\ a_{3,2} & a_{3,3} \end{bmatrix} - a_{2,1} \det \begin{bmatrix} a_{1,2} & a_{1,3} \\ a_{3,2} & a_{3,3} \end{bmatrix} + a_{3,1} \det \begin{bmatrix} a_{1,2} & a_{1,3} \\ a_{2,2} & a_{2,3} \end{bmatrix} \\ &= a_{1,1}(a_{2,2}a_{3,3} - a_{2,3}a_{3,2}) - a_{2,1}(a_{1,2}a_{3,3} - a_{1,3}a_{3,2}) + a_{3,1}(a_{1,2}a_{2,3} - a_{2,2}a_{1,3}). \end{aligned}$$

We shall get a more explicit formula for the determinant in Theorem C.3.3, but for now we shall use this one. Let's prove that it is linear in each column (we say the determinant is *multilinear* in the columns).

Proposition C.3.1

The determinant is linear in each column, i.e., for any $k \in [n]$, $t \in K$ and $C, C' \in K^n$, we have

$$\det[A_1, \ldots, A_{k-1}, tC + C', A_{k+1}, \ldots, A_n] = t \det[A^1, \ldots, A^{k-1}, C, A^{k+1}, \ldots, A^n] + \det[M^1, \ldots, A^{k-1}, C', A_{k+1}, \ldots, A^n].$$

Proof

This follows easily from our inductive definition. For the sake of convenience we shall write $\det^k_D(M) = \det[M^1, \ldots, M_{k-1}, D, M_{k+1}, \ldots, M^n]$ for any $D \in K^N$ and any M. Let $C = (c_i)$ and $C' = (c'_i)$. First suppose $k = 1$. Then,

$$\det^k_{tC+C'}(A) = \sum_i (tc_i + c'_i) \det A_{i,1} = t \sum_i c_i \det A_{i,1} + \sum_i c'_i \det A_{i,1} = t \det^k_C(A) + \det^k_{C'}(A).$$

Otherwise,

$$\det^k_{tC+C'}(A) = \sum_i a_{i,1} \det^{k-1}_{tC+C'} A_{i,1}$$

which is linear by the induction hypothesis.

■

Thus, the determinant is invariant under addition of two columns of the matrix if and only if the determinant of a matrix with two identical columns is 0. Before showing this however, we prove that the determinant changes by a sign when we exchange two columns. This should satisfy the reader who was disappointed by the lack of symmetry in our definition.

Proposition C.3.2

The determinant of a matrix is multiplied by -1 when exchanging two of its columns (which are distinct).

Proof

Without loss of generality suppose $j > i$. We prove the claim when exchanging two consecutive columns. Iterating this process yields the desired conclusion: indeed if we do the switches

$$i \mapsto i + 1 \mapsto \ldots \mapsto i + (j - i),$$

the kth column goes to the $k - 1$th column for $i + 1 \leq k \leq j$, and then if we do the switches

$$\underbrace{j-1}_{\text{originally } j} \mapsto j - 2 \mapsto \ldots \mapsto j - 1(j - 1 - i)$$

we have exchanged at the end exchanged only the original ith column with the original jth column. In total, we made $(-1)^{(j-i)+(j-1-i)} = -1$ switches of consecutive columns, so the determinant is negated.

To prove that this for consecutive columns, we introduce a similar notation to the one we did before:

$$\det^k_{C,C'}(A) = \det[A^1, \ldots, A^{k-1}, C, C', A^{k+2}, \ldots, A^n].$$

We have

$$\begin{aligned} 0 &= \det^k_{A^k+A^{k+1},A^k+A^{k+1}}(A) \\ &= \det^k_{A^k,A^k}(A) + \det^k_{A^{k+1},A^{k+1}}(A) + \det^k_{A^k,A^{k+1}}(A) + \det^k_{A^{k+1},A^k}(A) \\ &= \det A + \det^k_{A^{k+1},A^k}(A) \end{aligned}$$

as wanted since the first two determinants are zero as the matrices have two equal columns.

■

Proposition C.3.3

The determinant of a matrix with two identical columns is zero.

Proof

By induction again (what else can we do when we defined the determinant inductively?). When $n = 1, 2$ this is obvious. Otherwise, by switching some columns, we may assume the second and third ones are equal by Proposition C.3.2. Then

$$\det A = \sum_i a_{i,1} \det A_{i,1}$$

and all $A_{i,1}$ have two identical columns so habe zero determinant by the induction hypothesis.

■

Exercise C.3.4*. Prove that $\det I_n = 1$.

Exercise C.3.5*. Prove that the determinant of a matrix with a zero column is zero.

Exercise C.3.6. Prove that the determinant of a non-invertible matrix is 0.

With this we can almost prove that the determinant is non-zero if and only if the matrix is invertible. But first, we need to know how to compute a certain kind of determinants: determinants of *upper triangular matrices*, i.e. matrices $M = (a_{i,j})$ such that $a_{i,j} = 0$ for $j > i$

$$\begin{bmatrix} a_{1,1} & 0 & \cdots & 0 \\ a_{2,1} & a_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{bmatrix}.$$

Here is a sketch of how we are going to proceed to prove that the determinant of an invertible matrix is non-zero, using upper triangular matrices.

The determinant is invariant under *column operations*, i.e. adding a scalar times a column to another column. Indeed,

$$\det^k_{A^k+tA^i}(A) = \det^k_{A^k}(A) + t \det^k_{A^i}(A) = \det A$$

since $\det_{A^i}(A) = 0$ as it has two equal columns. Thus, we shall transform A into an upper triangular matrix using column operations and exchanging columns. The determinant of this matrix will then be $\pm \det A$ so we compute it with the following proposition and as a result we conclude that $\det A \neq 0$. This idea of transforming A into a triangular matrix is also what we did to prove that bases all had the same cardinality in Proposition C.1.2.

Proposition C.3.4

The determinant of an upper triangular matrix $A = (a_{i,j})$ is the product of the elements on the diagonal $a_{1,1} \cdot a_{2,2} \cdot \ldots a_{n,n}$.

Proof

By induction! It's clearly true for $n = 1$ and for $n \geq 2$ we have

$$\det A = a_{1,1} \det A_{1,1} - a_{2,1}A_{2,1} + \ldots + (-1)^n a_{n,1}A_{n,1}.$$

Now notice that $A_{i,1}$ has one row full of zeros (the one correspond to the first row of A) which means $\det A_{i,1} = 0$ by Exercise C.3.5*, i.e. $\det A = a_{1,1} \det A_{1,1} = a_{1,1}a_{2,2} \cdot \ldots \cdot a_{n,n}$ by the induction hypothesis.

■

Theorem C.3.1

Any $n \times n$ matrix A is invertible if and only if its determinant $\det A$ is non-zero.

Proof

As said before, we will transform A into an upper triangular matrix by making column operations and exchanging columns. Since this leaves the space generated by the columns unchanged and changes the determinant by a factor of ± 1, it will suffice to prove that an upper triangular matrix is invertible if and only if its diagonal has no zero element. This is Exercise C.3.7*.

Here is how we do it. We proceed by induction on n ($n = 1$ is trivial as always). If the first row of A is all zero then we can directly apply the induction hypothesis on $A_{1,1}$. Otherwise, suppose that $a_i \neq 0$. By exchanging the ith column with the first one, we can assume $i = 1$.

Now, consider the matrix

$$\left(A^1, A^2 - \frac{a_{1,2}}{a_{1,1}}A^1, A^3 - \frac{a_{1,3}}{a_{1,1}}A^1, \ldots, A^n - \frac{a_{1,n}}{a_{1,1}}A^1\right).$$

It is column equivalent to A and its first row is zero, except for $a_{1,1}$. Now apply the induction hypothesis to this matrix.

■

Exercise C.3.7*. Prove that an upper triangular matrix is invertible if and only if its determinant is non-zero, i.e. if the elements on its diagonal are non-zero.

We are finally ready for some applications. We shall first give a proof that algebraic integers are closed under addition and multiplication using our machinery. In fact we even have the following more general criterion.

Proposition C.3.5

An algebraic number α is an algebraic integer if and only if there is a finitely generated $\mathbb{Z}$-module M such that $\alpha M \subseteq M$. (A module is like a vector space except it can be over any ring, not necessary a field. In this case a $\mathbb{Z}$-module is a space where you can add and subtract elements since multiplication by integers is trivial. Finitely generated means that $M = u_1\mathbb{Z} + \ldots + u_m\mathbb{Z}$ for some $u_1, \ldots, u_m$.)

Proof

If α is an algebraic integer, then we can take $M = \mathbb{Z} + \alpha\mathbb{Z} + \ldots + \alpha^{n-1}\mathbb{Z}$ where n is the degree of α. For the converse, suppose M is a finitely generated $\mathbb{Z}$-module such that $\alpha M \subseteq M$.

Let $u_1, \ldots, u_m$ be a system of generators of M. Write

$$\alpha u_j = \sum_i a_{i,j} u_i$$

with $a_{i,j} \in \mathbb{Z}$. Subtracting αu_j from both sides, we get that the vectors

$$(a_{1,j}, \ldots, a_{j-1,j}, a_{j,j} - \alpha, a_{j+1,j}, \ldots, u_{m,j})$$

are linearly independent over $\mathbb{C}$. Let $A = (a_{i,j})$. The previous remark means that the rows of $A - \alpha I_m$ are linearly dependent, i.e. $A - \alpha I_m$ has determinant zero. But the determinant $\det(A - \alpha I_m)$ is a polynomial in α with integer coefficients since A has integer coordinates. Moreover, from Lemma C.3.1, we see that its leading coefficient is $(-1)^m$ so $\alpha \in \overline{\mathbb{Z}}$ as wanted.

■

Corollary C.3.1

The set of algebraic integers $\overline{\mathbb{Z}}$ is closed under addition and multiplication.

Proof

If α and β are algebraic integers of respective degrees m and n, then

$$M = \mathbb{Z}[\alpha, \beta] := \sum_{0 \leq i \leq m-1, 0 \leq j \leq n-1} \alpha^i \beta^j \mathbb{Z}$$

is a finitely generated $\mathbb{Z}$-module such that $(\alpha + \beta)M \subseteq M$ and $\alpha\beta M \subseteq M$. Thus $\alpha + \beta$ and $\alpha\beta$ also are algebraic integers.

■

Exercise C.3.8. Prove that $\overline{\mathbb{Z}}$ is *integrally closed*, meaning that, if f is a monic polynomial with algebraic integer coefficients, then any of its root is also an algebraic integer. (This is also Exercise 1.5.22†.)

Before presenting more applications, we need two last results. Here is an explicit formula for the determinant which will make our life a lot easier. It can easily be proven by induction. Theorem C.3.3 will determine exactly when those $\varepsilon(\sigma)$ are 1 and when they are -1.

Lemma C.3.1

The determinant of an $n \times n$ matrix $A = (a_{i,j})$ is equal to

$$\det \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1),1} \cdot \ldots \cdot a_{\sigma(n),n}$$

where the sum is taken over all permutations σ of $[n]$ and $\varepsilon(\sigma) \in \{-1, 1\}$. Moreover, $\sigma(\mathrm{id}) = 1$ (i.e. the coefficient of $a_{1,1} \cdot \ldots \cdot a_{n,n}$ is 1).

Exercise C.3.9*. Prove Lemma C.3.1.

Now, we compute a very important determinant, and then we can move on to applications.

Theorem C.3.2 (Vandermonde Determinant)

Let $x_1, \cdots, x_n \in K$ be elements. We have

$$\det \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{bmatrix} = \prod_{i<j}(x_i - x_j)$$

Proof

Note that this determinant is zero when $x_i = x_j$ for some $i \neq j$ since it then has two equal columns. Now replace x_i by a variable X_i and consider this determinant as a polynomial in $X_1, \ldots, X_n$. The previous observation implies that it is divisible by $X_i - X_j$ for any i, j, i.e. by $\prod_{i<j} X_i - X_j$. In addition, Lemma C.3.1 shows that the degree of the determinant is $\frac{n(n-1)}{2}$ which is the same as $\prod_{i<j} X_i - X_j$ so they are equal up to a multiplicative constant. The same lemma shows that the coefficient of

$$X_1 X_2^2 X_3^3 \cdot \ldots \cdot X_n^n$$

in the determinant is 1, so it is equal to $\prod_{i<j} X_i - X_j$ since it has the same coefficient.

■

From this we deduce a very important corollary.

Corollary C.3.2*

If $x_1, \ldots, x_n$ are distinct numbers, then the vectors

$$(1, x_1, \ldots, x_1^n), \ldots, (1, x_n, \ldots, x_n^n)$$

are linearly independent.

Remark C.3.2

In fact, we didn't need to do all this to prove this corollary. Indeed, the invertibility of the matrix

$$M = \begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{bmatrix}$$

when $x_1, \ldots, x_n$ are distinct is exactly what Lagrange interpolation A.1.2 gives us. Indeed, the non-explicit form of the theorem says precisely that the linear map $x \mapsto Mx$ from K^n to itself is surjective. I hope the reader doesn't feel too disheartened by this, there are times where the explicit value of the determinant will be useful to us (in the exercises).

Here is an arithmetic application, which is exactly how we will use the Vandermonde determinant in this book (in the exercises).

Problem C.3.1

Let p is a prime number and $a_1, \ldots, a_m$ integers which are not divisible by p. Suppose $p \mid a_1^k + \ldots + a_m^k$ for $k = 1, \ldots, m$. Prove that $p \mid m$.

Solution

Collect the a_i which are equal modulo p together to get

$$p \mid \sum_{i=1}^{n} c_i b_i^n$$

for some positive integers $\sum_i c_i = m$ and distinct $b_i \in \mathbb{F}_p$. We have a system of equations

$$\begin{cases} c_1 + \ldots + c_n \equiv 0 \\ c_1 b_1 + \ldots + c_n b_n \equiv 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ c_1 b_1^n + \ldots + c_n b_n^n \equiv 0. \end{cases}$$

Since the b_i are distinct modulo p, the vectors $(1, \ldots, b_1^n), \ldots, (1, \ldots, b_n^n)$ are linearly independent in $\mathbb{F}_p$ by Vandermonde. Thus, we must have $c_1 \equiv \ldots \equiv c_n \equiv 0$. Since $m = \sum_i c_i$, we have $p \mid m$ as wanted. ■

As we saw from the first example, matrices are deeply linked with system of linear equations. In hindsight, this is obvious: the system

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,n}x_n = b_2 \\ a_{2,1}x_1 + a_{2,2}x_2 + \ldots + a_{1,n}x_n = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n,1}x_1 + a_{n,2}x_2 + \ldots + a_{n,n}x_n = b_n \end{cases}$$

is equivalent to

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} = x_1 \begin{bmatrix} a_{1,1} \\ a_{2,1} \\ \vdots \\ a_{n,1} \end{bmatrix} + x_2 \begin{bmatrix} a_{1,2} \\ a_{2,2} \\ \vdots \\ a_{n,2} \end{bmatrix} + \ldots + x_n \begin{bmatrix} a_{1,n} \\ a_{2,n} \\ \vdots \\ a_{n,n} \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

i.e. to $XA = B$ where $X = (x_i)$, $A = (a_{i,j})$ and $B = (b_i)$. In particular, when A is invertible there is a unique solution, so if we have at a some point in a problem we reach such a system of equations and have a trivial solution, then we know what the x_i are since it's the only solution.

As a last application of determinants, we give a different solution to the cows problem C.1.1.

Alternative Solution to the Cows Problem C.1.1

Again, let w_i be weight of the ith cow. Write

$$\sum_{i \in I_k} w_i = \sum_{i \in J_k} w_i$$

where $|I_k| = |J_k| = n$ and $I_k \cup J_k = [2n+1] \setminus \{k\}$ and suppose $w_{2n+1} \in I_k$ for $k \neq 2n+1$.

Consider the system of $2n$ linear equations in $2n$ unknowns

$$\sum_{i\in J_k} w_i - \sum_{i\in I_k, i\neq 2n+1} w_i = -w_{2n+1}$$

for $k = 1, \ldots, 2n$. The determinant of the associated matrix has the form

$$\begin{bmatrix} 0 & \pm 1 & \pm 1 & \cdots & \pm 1 \\ \pm 1 & 0 & \pm 1 & \cdots & \pm 1 \\ \pm 1 & \pm 1 & 0 & \cdots & \pm 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \pm 1 & \pm 1 & \pm 1 & \cdots & 0 \end{bmatrix}$$

where there are 0s on the diagonal and a 1 in the (i, j) coordinate if $i \in J_j$ and a -1 otherwise. We wish to show that this determinant is non-zero. Thus, there will be a unique solution to the system, and since $w_1 = \ldots = w_{2n} = w_{2n+1}$ is such a solution it will imply that they are indeed all equal. Modulo 2, the determinant is simply

$$\begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix} = \sum_{\sigma\in\mathfrak{S}_{2n}} \varepsilon(\sigma) a_{1,\sigma(1)} \cdot \ldots \cdot a_{n,\sigma(n)} \equiv \sum_{\sigma\in\mathfrak{S}_{2n}} a_{1,\sigma(1)} \cdot \ldots \cdot a_{2n,\sigma(2n)}$$

where the matrix above is $A = (a_{i,j})$. Now, $a_{1,\sigma(1)} \cdot \ldots \cdot a_{2n,\sigma(2n)}$ is 1 if and only if σ has no fixed point. Thus, this determinant is congruent to the number of *derangements*, i.e. permutations without fixed points. Exercise C.3.10* implies that this number is odd so non-zero, so the original determinant was also odd and in particular non-zero and we are done. ■

Remark C.3.3

One can also compute directly

$$\begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix},$$

as a consequence of, e.g., Exercise C.5.6.

Exercise C.3.10*. Prove that the number of derangements of $[m]$ is

$$\sum_{i=0}^{m} \frac{(-1)^i m!}{i!}$$

and that this number is odd if m is even and even if m is odd.

All right, now let's finish with the determinant.

Definition C.3.2 (Signature)

The *signature* $\varepsilon(\sigma)$ of a permutation σ of $[n]$ is

$$\prod_{1\leq i<j\leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Note that since σ is a permutation, its signature is in $\{-1, 1\}$. Thus, the signature of a permutation is -1 raised to its number of inversions, i.e. the number of $j > i$ such $\sigma(j) < \sigma(i)$ (an inversion has a contribution of -1 in the signature).

This definition of the signature is in fact not always convenient to work with, so we shall also mention another one. One can see that when we apply a *transposition* to σ, i.e. switch two of its values $\sigma(i)$ and $\sigma(j)$, the signature is multiplied by -1. Since any permutation is a composition of transpositions, the signature is 1 if there are an even number of transpositions and -1 otherwise. In the first case we say the permutation is *even*, and in the second one that it is *odd*.

In particular it does not depend on which transpositions we choose. for example, if one starts with the sequence $(1, \dots, 2m)$ and switches a pair of elements at each step, one will never be able to go back to the original tuple after an odd number of times since the signature will be -1 while the signature of the identity is 1.

As another consequence of this characterisation, we see that the signature is a morphism of groups $\mathfrak{S}_n \to \{-1, 1\}$: indeeed $\varepsilon(\sigma \circ \sigma') = \varepsilon(\sigma) \cdot \varepsilon(\sigma')$ (this is obvious if you consider σ and σ' as a composition of transpositions).

Exercise C.3.11*. Prove that the signature is negated when one exchanges two values of σ (i.e. compose a transposition with σ).

Exercise C.3.12*. Prove that transpositions $\tau_{i,j} : i \leftrightarrow j$ and $k \mapsto k$ for $k \neq i, j$ generate all permutations (through composition).

Remark C.3.4

Proposition C.3.2 now reads as follow: when we apply a transposition to the columns, the determinant gets multiplied by -1. Thus, when we apply a permutation σ to the columns, the determinant gets multiplied by $\varepsilon(\sigma)$. (This is also a direct corollary of the next theorem.)

We get the following refinement of Lemma C.3.1 by induction.

Theorem C.3.3

The determinant of an $n \times n$ matrix $A = (a_{i,j})$ is equal to

$$\det \begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{bmatrix} = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1),1} \cdot \ldots \cdot a_{\sigma(n),n}$$

where the sum is taken over all permutations σ of $[n]$.

Exercise C.3.13*. Prove Theorem C.3.3.

Since permutations are symmetric with respect to the rows and the columns, we get that the determinant is also symmetric with respect to the rows or the columns. In particular, our expansion with respect to one column that we defined the determinant with also holds for rows (and using Proposition C.3.2 it holds for **any** row and any column).

Corollary C.3.3

For any square matrix A, $\det A = \det A^{\mathsf{T}}$.

Exercise C.3.14*. Prove that $\det A = \det A^{\mathsf{T}}$ for any square matrix A.

As promised in the beginning of the section, the determinant is the unique solution of a certain functional equation. In fact, this is equation is more or less equivalent to our inductive definition as we shall see. As a consequence, we will see that this implies the multiplicativity of the determinant.

Theorem C.3.4

The determinant of $n \times n$ matrices is the only function D which is multilinear (linear in all columns), zero when two columns are the same, and such that $D(I_n) = 1$.

Proof

We proceed by induction on n. When $n = 1$ it's obvious. For the inductive step, consider the canonical basis of K^n, i.e. the column vectors e_i with a 1 in ith position and zeros everywhere else.

The same proof as Proposition C.3.2 shows that when we exchange two columns, D gets multiplied by -1 (since the only thing we used there was the multilinearity). Note that if $A = (a_{i,j})$ is an $(n-1) \times (n-1)$ matrix, then

$$D_k : A \mapsto D \begin{bmatrix} 0 & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n,1} & \cdots & a_{1,n-1} \end{bmatrix}$$

where the first column is E^k, the kth row has only zeros, and the other rows have the matrix A (a bit distorted if $k \neq 1, n$) also satisfies the conditions of the theorem, except possibly the unitary condition. One can check that $D_k(I_{n-1}) = (-1)^{k-1}$ by exchanging some columns (Exercise C.3.15*), thus $D_k(A) = (-1)^k \det A$ by the induction hypothesis. Notice also that, for any $b_1, \ldots, b_{n-1}$

$$D \begin{bmatrix} 0 & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & b_1 & \cdots & b_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n,1} & \cdots & a_{1,n-1} \end{bmatrix} = D_k(A)$$

since by adding the first column E^k to the other ones we can get rid of the b_i as this doesn't change the determinant.

Finally, using the multilinearity we have

$$D(A) = D\left(\sum_{i=1}^{n} a_{i,1} E^i, A^2, \ldots, A^n\right) = \sum_{i=1}^{n} a_{i,1} D_i(A_{1,i})$$

by the previous remark. Since $D_i(A_{1,i}) = (-1)^{i-1} \det A$, this is the recurrence we originally defined the determinant with so we are done.

■

Exercise C.3.15*. Prove that $D_k(I_{n-1}) = (-1)^{k-1}$.

From this we deduce the following.

Proposition C.3.6 (Multiplicativity of the Determinant)*

The determinant is multiplicative, i.e. for any $n \times n$ matrice A and B we have $\det(AB) = \det(A)\det(B)$.

Proof

Fix B. The function $A \mapsto \det(AB)/\det(B)$ satisfies all conditions of Theorem C.3.4 so is equal to $\det(A)$.

■

Exercise C.3.16. Prove that the determinant is multiplicative by using the explicit formula of Theorem C.3.3.

As an important corollary, we get $\det(A^{-1}) = \det(A)^{-1}$ since

$$\det(A)\det(A^{-1}) = \det(I_n) = 1.$$

This result also lets us define the determinant of a linear map, although we won't be using this here.

Corollary C.3.4

We can define the determinant of a linear map $\varphi : U \to U$ as the determinant of any matrix $M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ representing φ.

Proof

We need to show that this is well-defined. If M is a matrix representing φ, then the other matrices representing φ have the form NMN^{-1} for an invertible N (see Section C.2). Since the determinant is multiplicative, we have

$$\det(NMN^{-1}) = \det(N)\det(M)\det(N)^{-1} = \det(M)$$

as wanted.

■

Remark C.3.5

With this notion of determinant of a linear map, the norm $N_{L/K}(\alpha)$ is sometimes defined as the determinant of the linear map from L to L defined by $x \mapsto x\alpha$ (see Chapter 6).

Exercise C.3.17. Let L/K be a finite extension. Prove that the determinant of the K-linear map $L \to L$ defined by $x \mapsto x\alpha$ is the norm of α defined in Definition 6.2.3.

Finally, one might be interested in knowing when, say, a matrix with integer coordinates has an inverse with integer coordinates as well. This is achieved by Proposition C.3.6 and the following result, which gives an explicit formula for the inverse of a given matrix.

Proposition C.3.7

The *adjugate* of A, $\operatorname{adj} A := ((-1)^{i+j}\det(A_{j,i}))$ satisfies $A \operatorname{adj} A = (\det A)I_n = \operatorname{adj} A A$.

Remark C.3.6

The transpose of the adjugate, $\operatorname{com} A := ((-1)^{i+j}\det(A_{i,j}))$, is called the *comatrix* of A.

Proof

Let's compute $(b_{i,j}) = A \operatorname{adj} A$. We have $b_{i,j} = \sum_{k=1}^{n} a_{i,k}(-1)^{j+k} \det(A_{j,k})$. When $i = j$ this is the ith row expansion of the determinant so is indeed equal to $\det A$. When $i \neq j$, it is still the expansion of a determinant, but not of A: it is $(-1)^{i+j}$ times the determinant of the matrix obtained by replacing the ith row of A by its jth row. This matrix has two identical rows so its determinant is zero.

Thus we have $b_{i,j} = 0$ if $i \neq j$ and $b_{i,i} = \det A$, i.e. $A \operatorname{adj} A = (\det A) I_n$. The coordinates of $\operatorname{adj} AA$ are treated in a similar fashion, by noting that they are column expansions of certain determinants this time.

■

Remark C.3.7

There is another way to argue that $\operatorname{adj} AA$ is also equal to $(\det A) I_n$ once we have proven $A \operatorname{adj} A$ is. Note that this is a polynomial equation in the coordinates of A, so if it holds sufficiently many times in a fixed infinite field K it must always hold (e.g. by Exercise A.1.7*). Suppose that $\det A$ is non-zero. Then, $\operatorname{adj} A / \det A$ is the inverse of A so it commutes with A as wanted. Finally, $(\operatorname{adj} AA - (\det A) I_n) \det A$ is zero for all $A \subseteq K^{n \times n}$ so must be identically zero, which implies $\operatorname{adj} A = (\det A) I_n$ since the determinant is not the zero polynomial.

Exercise C.3.18*. Prove that $\operatorname{adj} AA = (\det A) I_n$.

In fact, this also gives another proof Theorem C.3.1. This follows from the more general corollary below, which answers our question about invertible matrices with integer coefficients.

Corollary C.3.5*

Let A be a matrix with coefficients in a commutative ring R. A is invertible in R (i.e. A has an inverse with coordinates in R) if and only if $\det A$ is a unit of R.

For instance, a matrix with integer coordinates has an inverse with integer coordinates if and only if its determinant is ± 1.

Proof

If A^{-1} has coordinates in R, then $\det(A) \det(A^{-1}) = 1$ so $\det A$ is a unit. Conversely, if $u \det A = 1$, then $A(u \operatorname{adj}(A)) = I_n$.

■

C.4 Linear Recurrences

In this short section, we derive the formula for linear recurrences using the Vandermonde determinant, which will be used **a lot** in this book.[2]

[2] Mainly in the exercises, though.

Definition C.4.1 (Linear Recurrences)

We say a sequence $(u_n)_{n\in\mathbb{Z}}$ is a *linear recurrence* if there is some $k \geq 1$ and numbers $a_0, \ldots, a_{k-1} \in K$ such that $a_0 \neq 0$ and

$$u_{n+k} = \sum_{i=0}^{k-1} a_i u_{n+i}$$

for all i. The smallest such k is called the *order* of the linear recurrence, and the polynomial $X^k - a_{k-1}X^{k-1} - \ldots - a_1 X - a_0$ is its *characteristic polynomial*. This polynomial is also called the *characteristic polynomial* of the above equation (and the equation is called the equation *associated* with f).

Theorem C.4.1 (Linear Recurrences)

Let K be characteristic zero field and $(u_n)_{n\in\mathbb{Z}}$ be a linear recurrence of elements of K with characteristic polynomials f. Suppose the distinct roots of f are $\alpha_1, \ldots, \alpha_r$ with multiplicity $m_1, \ldots, m_r$. Then, there exist polynomials $f_1, \ldots, f_r$ of degrees less than $m_1, \ldots, m_r$ respectively such that

$$u_n = f_1(n)\alpha_1^n + \ldots + f_r(n)\alpha_r(n)$$

for all $n \in \mathbb{Z}$.

Proof

Let d be the degree of f. Consider the K-vector space of sequences satisfying the equation associated with f (which is indeed a vector space as it is closed under addition). This space has dimension d: indeed for any $(x_0, \ldots, x_{d-1}) \in K^d$ there is a unique sequence solution to the recurrence $(u_n)_n$ such that $u_0 = x_0, \ldots, u_{d-1} = x_{d-1}$. Thus, the dimension of this space is the same as $\dim K^d = d$.

Now we prove that all sequences of the form $u_n = f_1(n)\alpha_1^n + \ldots + f_k(n)\alpha_r^n$ are solutions. Since these sequences also form a K-vector space with generating family given by

$$u_n = n(n-1)\cdot\ldots\cdot(n-(k-1))\alpha_i^n$$

for $k = 0, \ldots, m_i - 1$ and $i = 1, \ldots, r$. Thus we want to have

$$(n+d)(n+d-1)\cdot\ldots\cdot(n+d-(k-1))\alpha_i^{n+j} = \sum_{j=0}^{d-1}(n+j)(n+j-1)\cdot\ldots\cdot(n+j-(k-1))\alpha_i^{n+j}$$

which is equivalent to

$$(X^n f)^{(k)}(\alpha_i) = 0$$

and that's true because α_i is a root of multiplicity $m_i > k$ of $X^n f$.

Finally, to show that all solutions have this form we want to prove that the dimension of the space of solution of this form is the same as the dimension of the space of all solutions, i.e. d. Since our generating family had exactly $m_1 + \ldots + m_r = d$ elements, this is equivalent to it being a basis.

Thus, we want to show it is linearly indepndent. Suppose that a linear combination was zero, i.e.

$$u_n \sum_i f_i(n)\alpha_i^n = 0$$

for all n. We shall prove that $f_i(n) = 0$ for all n and each i, thus implying that $f_i = 0$ since K has characteristic zero. We proceed by induction on $\sum_i \deg f_i$, the base case follows from

the Vandermonde determinant C.3.2. For the induction step, suppose $\deg f_1 \geq 1$ without loss of generality. Consider the sequence

$$v_n = u_{n+1} - \alpha_1 u_n = \sum_i (\alpha_i f_i(n+1) - \alpha_1 f_i(n))\alpha_i^n.$$

Since $\deg(\alpha_i f_i(X+1) - \alpha_1 f_i) \leq \deg f_i$ for $i \geq 1$ and $\deg(\alpha_1(f_i(X+1) - f_i)) \leq \deg f_i - 1$, by the induction hypothesis we have $\alpha_i f_i(X+1) - \alpha_1 f_i = 0$ for all i. This means that they are constant, but we have already treated this case so we are done.

■

Remark C.4.1

This theorem is equivalent to the existence of a (unique) *partial fraction decomposition* of any rational function, meaning that, given a rational function $h = f/g$ with $g = \prod_{i=1}^r (X-\alpha_i)^{m_i}$ and $\deg g > \deg f$, i.e. $\deg h < 0$, there are polynomials f_i of degree at most $m_i - 1$ such that

$$h = \sum_{i=1}^r \frac{f_i}{(X-\alpha_i)^{m_i}}.$$

In fact, if we fix $g = \sum_{i=0}^d a_i X^i$, the rational function with denominator g and negative degree correspond exactly to the generating functions of linear recurrences with characteristic polynomial $\widehat{g} = X^d g(1/X) = \sum_{i=0}^d a_{d-i} X^i$. Indeed, suppose that $(u_n)_{n\geq 0}$ is such a sequence. Then, since $u_{n+d} = -\frac{1}{a_0}\sum_{k=0}^{d-1} a_{d-k} u_{n+k}$, we have

$$\begin{aligned}
h &:= \sum_{n=0}^{\infty} u_n X^n \\
&= \left(\sum_{n=0}^{d-1} u_n X^n\right) + \sum_{n=0}^{\infty} u_{n+d} X^{n+d} \\
&= \left(\sum_{n=0}^{d-1} u_n X^n\right) + \sum_{n=0}^{\infty} -\frac{X^{n+d}}{a_0} \sum_{k=0}^{d-1} a_{d-k} u_{n+k} \\
&= \left(\sum_{n=0}^{d-1} u_n X^n\right) - \frac{1}{a_0} \sum_{k=0}^{d-1} a_{d-k} X^{d-k} \sum_{n=0}^{\infty} u_{n+k} X^{n+k} \\
&= \left(\sum_{n=0}^{d-1} u_n X^n + \sum_{k=0}^{d-1} \frac{a_{d-k}}{a_0} \sum_{n=0}^{k-1} u_n X^{d-k+n}\right) - \frac{1}{a_0} \sum_{k=0}^{d-1} a_{d-k} X^{d-k} \sum_{n=0}^{\infty} u_n X^n \\
&:= f - \frac{(a_0 - g)h}{a_0}
\end{aligned}$$

so $h = f - \frac{(a_0-g)h}{a_0}$, i.e. $h = \frac{f}{1-\left(1-\frac{g}{a_0}\right)} = \frac{a_0 f}{g}$ as wanted. Note that f can be any polynomial of degree less than d since

$$f = u_0 + (u_1 + u_0 a_1/a_0)X + (u_2 + u_1 a_1/a_0 + u_0 a_2/a_0)X^2 + \dots$$

so we can pick the u_i inductively to get any f (equivalently, the matrix of the coefficients of f represented as linear combinations of the u_i is upper-triangular with no zero coordinate on the diagonal so is invertible).

On the other hand, since the roots of $\widehat{g}$ are the $\frac{1}{\alpha_i}$, by our characterisation of linear recurrences, there are polynomials f_i of degree at most $m_i - 1$ such that $u_n = \sum_{i=1}^r f_i(n)(1/\alpha_i)^n$. Hence, we

also have

$$h = \sum_{n=0}^{\infty} X^n \sum_{i=1}^{r} f_i(n)(1/\alpha_i)^n$$
$$= \sum_{i=1}^{r} \sum_{n=0}^{\infty} f_i(n)(X/\alpha_i)^n.$$

Now, note that the f_i are linear combinations of $(X+k)(X+k-1)\cdot\ldots\cdot(X+1)$ so it suffices to prove that the result holds for these polynomials. For this, simply note that differentiating k times

$$\sum_{n=0}^{\infty}(X/\alpha)^n = \frac{1}{1-X/\alpha} = \frac{-\alpha}{X-\alpha}$$

gives

$$\sum_{n=0}^{\infty}(n+k)(n+k-1)\cdot\ldots\cdot(n+1)(X/\alpha)^n = \frac{k!}{(X-\alpha)^{k+1}}$$

as wanted.

Remark C.4.2

This also works for fields of characteristic $p \neq 0$, but one needs the condition that no root has multiplicity $\geq p+1$, otherwise $n \mapsto f_i(n)$ could be identically zero without f_i being zero (e.g. $f_i = n^p - n$). For instance the equation $u_{n+4} = u_n$ has characteristic polynomial $(X-1)^4$ but the space of solutions of the form $\sum_i f_i(n)\alpha_i^n$ has dimension 2 while the space of solutions of $u_{n+4} = u_n$ has dimension 4 so not all solutions have the wanted form.

Exercise C.4.1. Prove that Theorem C.4.1 holds in a field K of characteristic $p \neq 0$ as long as the multiplicities of the roots of the characteristic polynomial are at most p. In particular, for a fixed characteristic equation, it holds for sufficiently large p.

As a corollary, we get the following result, which is not obvious at first sight.

Corollary C.4.1

The product and sum of two linear recurrences are also linear recurrences.

C.5 Exercises

Vector Spaces and Bases

Exercise C.5.1 (Grassmann's Formula)**.** Let U be a vector space and V, W be two finite-dimensional subspaces of U. Prove that

$$\dim(V+W) = \dim V + \dim W - \dim(V \cap W).$$

Exercise C.5.2 (Noether's Lemma)**.** Let U, V, W be finite-dimensional vector spaces, and let $\varphi : U \to V, \psi : V \to W$ be linear maps. Suppose that $\operatorname{im}\varphi \subseteq \ker\psi$. Prove that there exists a linear map τ such that $\psi = \tau \circ \varphi$. Similarly, if $\operatorname{im}\varphi \subseteq \operatorname{im}\psi$, prove that there is a linear map τ such that $\varphi = \psi \circ \tau$.

Exercise C.5.3†**.** Given a vector space V of dimension n, we say a subspace H of V is a *hyperplane* of V if it has dimension $n-1$. Prove that H is a hyperplane of K^n if and only if there are elements $a_1, \ldots, a_n \in K$ not all zero such that

$$H = \{(x_1, \ldots, x_n) \in K^n \mid a_1x_1 + \ldots + a_nx_n = 0\}.$$

Exercise C.5.4. Let E be a vector space with subspaces $E_1, \ldots, E_n$. Suppose that $E_1 \cup \ldots \cup E_n$ is a vector space. Prove that one E_i contains all others.

Exercise C.5.5. Let $z_1, \ldots, z_{n+1} \in \mathbb{C}$ be distinct complex numbers. Prove that $(X - z_1)^n, \ldots, (X + z_{n+1})^n$ is a $\mathbb{C}$-basis of the space of complex polynomials with degree at most n.

Determinants

Exercise C.5.6. Let $a_0, \ldots, a_{n-1}$ be elements of K and ω a primitive nth root of unity. Prove that the *circulant determinant*

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{bmatrix}$$

is equal to

$$f(\omega)f(\omega^2) \cdot \ldots \cdot f(\omega^{n-1})$$

where $f = a_0 + \ldots + a_{n-1}X^{n-1}$. Deduce that this determinant is congruent to $a_0 + \ldots + a_{p-1}$ modulo p when $n = p$ is prime and $a_1, \ldots, a_p$ are integers.

Exercise C.5.7 (Cramer's Rule)**.** Consider the system of equations $MV = X$ where M is an $n \times n$ matrix and $V = (v_i)_{i \in [\![1,n]\!]}$ and $X = (x_i)_{i \in [\![1,n]\!]}$ are column vectors. Prove that, for any $k \in [\![1, n]\!]$, v_k is equal to $\det M / \det M_{k,X}$, where $M_{k,X}$ denotes the matrix $[M^1, \ldots, M^{k-1}, X, M^{k+1}, \ldots, M^n]$ obtained from M by replacing the kth column by X.

Exercise C.5.8†**.** Let $(u_n)_{n \geq 0}$ be a sequence of elements of a field K. Suppose that the $(m+1) \times (m+1)$ determinant $\det(u_{n+i+j})_{i,j \in [\![0,m]\!]}$ is 0 for all sufficiently large n. Prove that there is some N such that $(u_n)_{n \geq N}$ is a linear recurrence of order at most m.

Exercise C.5.9†**.** Let $f_1, \ldots, f_n : \mathbb{N} \to \mathbb{C}$ be functions which grow at different rates, i.e.

$$\frac{f_1(m)}{f_2(m)}, \frac{f_2(m)}{f_3(m)}, \ldots, \frac{f_{n-1}(m)}{f_n(m)} \underset{m \to \infty}{\longrightarrow} 0$$

Prove that there exists n integers $m_1, \ldots, m_n$ such that the tuples

$$(f_1(m_1), \ldots, f_n(m_1)), \ldots, (f_1(m_n), \ldots, f_n(m_n))$$

are linearly independent over $\mathbb{C}$.

Exercise C.5.10. Suppose that K is an infinite field and that $A \subseteq K^{n \times n}$ is such that $\det(A + M) = \det M$ for any $M \subseteq K^{n \times n}$. Prove that $A = 0$.

Exercise C.5.11. Let $a_1, \ldots, a_n$ be integers. Prove that

$$\prod_{i<j} \frac{a_i - a_j}{i - j}$$

is an integer by expressing it as the determinant of a matrix with integer coordinates.

Algebraic Combinatorics

Exercise C.5.12†**.** Let $A_1, \ldots, A_{n+1}$ be non-empty subsets of $[n]$. Prove that there exist disjoint subsets I and J of $[n+1]$ such that

$$\bigcup_{i \in I} A_i = \bigcup_{j \in J} A_j.$$

Exercise C.5.13. Let p be a prime number and $a_1, \ldots, a_{p+1}$ real numbers. Suppose that, whenever we remove one of the a_i, we can divide the remaining ones into a certain amount of groups, depending on i, each with the same arithmetic mean (and at least two groups). Prove that $a_1 = \ldots = a_{p+1}$.

Exercise C.5.14. We have n coins of unknown masses and a balance. We are allowed to place some of the coins on one side of the balance and an equal number of coins on the other side. After thus distributing the coins, the balance gives a comparison of the total mass of each side, either by indicating that the two masses are equal or by indicating that a particular side is the more massive of the two. Show that at least $n-1$ such comparisons are required to determine whether all of the coins are of equal mass.

The Characteristic Polynomial and Eigenvalues

Exercise C.5.15 (Characteristic Polynomial)**.** Let K be an algebraically closed field. Let $M \subseteq K^{n\times n}$ be an $n \times n$ matrix. Define its *characteristic polynomial* as $\chi_M = \det(M - XI_n)$. Its roots (counted with multiplicity) are called the *eigenvalues* $\lambda_1, \ldots, \lambda_n \in K$ of M. Prove that $\det M$ is the product of the eigenvalues of M, and that $\operatorname{Tr} M$ is the sum of the eigenvalues. In addition, prove that λ is an eigenvalue of M if and only if there is a non-zero column vector V such that $MV = \lambda V$ (in other words, M acts like a homothety on V). Conclude that, if $f \in \mathbb{C}[X]$ is a polynomial, the eigenvalues of $f(M)$ are $f(\lambda_i)$ (with multiplicity). (We are interpreting $1 \in K$ as I_n for $f(M)$ here, i.e., if $f = X+1$, $f(M)$ is $M + I_n$.) In particular, the eigenvalues of $M + I\alpha$ are $\lambda_1 + \alpha, \ldots, \lambda_n + \alpha$, and the eigenvalues of M^k are $\lambda_1^k, \ldots, \lambda_n^k$.[3]

Exercise C.5.16 (Cayley-Hamilton Theorem)**.** Prove that, for any $n \times n$ matrix M, $\chi_M(M) = 0$ where χ_M is the characteristic polynomial of M and $0 = 0I_n$. Conclude that, if every eigenvalue of M is zero, M is *nilpotent*, i.e. $M^k = 0$ for some k.[4]

Exercise C.5.17. Let $A \subseteq \mathbb{C}^{n\times n}$ be a *Hermitian matrix*, i.e. $A = \overline{A^\intercal}$. Prove that all its eigenvalues are real.

Exercise C.5.18. Let M be a square matrix with integer coordinates and p a prime number. Prove that $\operatorname{Tr} M^p \equiv \operatorname{Tr} M \pmod p$.

Exercise C.5.19. Let p be a prime number, and G be a finite (multiplicative) group of $n \times n$ matrices with integer coordinates. Prove that two distinct elements of G stay distinct modulo p. What if the elements of G only have algebraic integer coordinates and p is an algebraic integer with all conjugates greater than 2 in absolute value?

Miscellaneous

Exercise C.5.20 (USA TST 2019)**.** For which integers n does there exist a function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ such that

$$f, f + \mathrm{id}, f + 2\mathrm{id}, \ldots, f + m\mathrm{id}$$

are all bijections?

Exercise C.5.21 (Finite Fields Kakeya Conjecture, Zeev Dvir)**.** Let $n \geq 1$ an integer and $\mathbb{F}$ a finite field. We say a set $S \subseteq \mathbb{F}^n$ is a *Kakeya set* if it contains a line in every direction, i.e., for every $y \in \mathbb{F}^n$, there exists an $x \in \mathbb{F}^n$ such that S contains the line $x + y\mathbb{F}$. Prove that any polynomial of degree less than $|\mathbb{F}|$ vanishing on a Kakeya set must be zero. Deduce that there is a constant $c_n > 0$ such that, for any finite field $\mathbb{F}$, any Kakeya set of $\mathbb{F}^n$ has cardinality at least $c_n p^n$.

Exercise C.5.22 (Siegel's Lemma)**.** Let $a = (a_{i,j})$ be an $m \times n$ matrix with integer coordinates. Prove that, if $n > m$, the system

$$\sum_{j=1}^{n} a_{i,j} x_j = 0$$

[3] One of the advantages of the characteristic polynomial is that we are able to use algebraic number theory, or more generally polynomial theory, to deduce linear algebra results, since the eigenvalues say a lot about a matrix (if we combine this with the Cayley-Hamilton theorem). See for instance Exercise C.5.18 and the third solution of Exercise C.5.19.

[4] Note that if, in the definition of χ_M, we replace det by an arbitrary multilinear form in the coordinates of M, such as the *permanent*) $\operatorname{perm}(A) = \sum_{\sigma\in\mathfrak{S}_n} a_{1,\sigma(1)} \cdot \ldots \cdot a_{n,\sigma(n)}$, the result becomes false, so we cannot just say that "$\chi_M(M) = \det(M - MI_n) = \det 0 = 0$" (this "proof" is nonsense because the scalar 0 is not the matrix 0, but the point is that this intuition is fundamentally incorrect).

for $i = 1, \ldots, n$ always has a solution in integers with

$$\max_i |x_i| \leq \left(n \max_{i,j} |a_{i,j}| \right)^{\frac{m}{n-m}}.$$

Exercise C.5.23. Define the *trace* of a matrix as the sum of its diagonal coefficients, and the trace of a linear map as the trace of any matrix representing it. Prove that this doesn't depend on the basis chosen and is thus well-defined. In addition, let L/K be a finite separable extension with embeddings $\sigma_1, \ldots, \sigma_n$ and let $\alpha \in K$. Prove that the trace of the linear map $x \mapsto x\alpha$ is

$$\sum_{i=1}^{n} \sigma_i(\alpha).$$

This function is called the *trace* $\mathrm{Tr}_{L/K}$ *of* L/K.

Exercise C.5.24. How many invertible $n \times n$ matrices are there in $\mathbb{F}_p$? Deduce the number of (additive) subgroups of cardinality p^m that $(\mathbb{Z}/p\mathbb{Z})^n$ has.

Exercise C.5.25†. Let K be a field, and let $S \subseteq K^2$ be a set of points. Prove that there exists a polynomial $f \in K[X, Y]$ of degree at most $\sqrt{2n}$ such that $f(x, y) = 0$ for every $(x, y) \in S$.

Exercise C.5.26†. Given an $m \times n$ matrix M, we define its *row rank* as the maximal number of linearly independent rows of M. Similarly, its *column rank* is the maximal number of linearly independent columns of M. Prove that these two numbers are the same, called the rank of M and denoted $\operatorname{rank} M$.

Exercise C.5.27. Let $A, B \in R^{n \times n}$. Prove that $\operatorname{com}(AB) = \operatorname{com}(A) \operatorname{com}(B)$.

Exercise C.5.28 (Nakayama's Lemma)**.** Let R be a commutative ring, I an *ideal* of a R, i.e. an *R-module* inside R[5], and M a finitely-generated R-module. Suppose that $IM = M$, where IM does not mean the set of products of elements of I and M, but instead the R-module it generates (i.e. the set of linear combinations of products). Prove that there exists an element $r \equiv 1 \pmod{I}$ of R such that $rM = 0$.

[5]See also Proposition C.3.5. A module is like a vector space but the underlying structure is not necessarily a field (in this case it's R).

Solutions

Chapter 1

Algebraic Numbers and Integers

1.1 Definition

Exercise 1.1.1. Is $\frac{i}{2}$ an algebraic integer?

Solution

Suppose that $f(i/2) = 0$ for some monic $f \in \mathbb{Z}[X]$. Note that the real part and imaginary part are both polynomials in $1/2$ with integer coefficients, and that one of them has leading coefficient ± 1 (which one it is depends on the parity of $\deg f$). Thus $1/2$ would be an algebraic integers, contradicting Proposition 1.1.1. ■

Exercise 1.1.2 (Rational Root Theorem)**.** Let $f \in \mathbb{Z}[X]$ be a polynomial. Suppose that u/v is a rational root of f, written in irreducible form. Prove that u divides the constant coefficient of f and v divides its leading coefficient. (This is a generalisation of Proposition 1.1.1.)

Solution

Let $f = \sum_{i=0}^{n} a_i X^i$, We have

$$\sum_{i=0}^{n} a_i u^i v^{n-i} = 0.$$

Modulo v, we get $a_n u^n \equiv 0$, i.e. $v \mid a_n$ since u and v are coprime by assumption. Similarly, modulo u we get $a_0 v^n \equiv 0$, i.e. $u \mid a_0$. ■

1.2 Minimal Polynomial

Exercise 1.2.1*. Prove that the minimal polynomial of an algebraic number is irreducible and that an irreducible polynomial is always the minimal polynomial of its roots.

Solution

Let α be an algebraic number. Assume, for the sake of a contradiction, that $\pi_\alpha = fg$ with $0 < \deg f, \deg g < \deg \pi_\alpha$. Then, one of f or g must vanish at α, a contradiction since they have smaller degree.

Conversely, let $\pi \in \mathbb{Q}[X]$ be a monic irreducible polynomial and let α be one of its roots. By Proposition 1.2.1, $\pi_\alpha \mid \pi$. since π is irreducible and both π_α and π are monic, this must mean that they are equal. ■

Exercise 1.2.2. Prove that $Y^4 - 3$ is irreducible in $\mathbb{Q}[X]$.

Solution

The roots of $Y^4 - 3$ are $i^k \sqrt[4]{3}$ where and $k = 0, \ldots, 3$. Note that none of these are rational so the only potential way to factorise $Y^4 - 3$ would be as a product of two degree 2 polynomials, but the constant term of such a degree 2 divisor would have the form $\pm i^k \sqrt{3}$ by Vieta's formulas A.1.4 which is not rational. This can also be seen as a special case of the Eisenstein criterion 5.1.4. ■

Exercise 1.2.3*. Prove that any algebraic number of degree n has n distinct conjugates.

Solution

suppose α be an algebraic number of degree n with less than n distinct conjugates; i.e. it's minimal polynomial π has a double root. Then $\gcd(\pi, \pi')$ has degree at least 1 by Proposition A.1.3 and at most $n - 1$, and divides π. Thus π is not irreducible, contradicting Exercise 1.2.1*. ■

Exercise 1.2.4*. Prove that the conjugates of an algebraic integer are also algebraic integers.

Solution

Let α be an algebraic integer, i.e. a root of a monic polynomial $f \in \mathbb{Z}[X]$. Then, $f(\beta) = 0$ for any conjugate β of α by Proposition 1.2.1 so any conjugate β is also an algebraic integer. ■

Exercise 1.2.5. We call an algebraic number of degree 2 a *quadratic number*. Characterise quadratic integers.

Solution

By Proposition 1.2.2, a quadratic integer α is a root of a monic polynomial $f \in \mathbb{Z}[X]$ of degree 2 which is not rational. Write $f = X^2 + uX + v$. Then,

$$\alpha = \frac{-u \pm \sqrt{u^2 - 4v}}{2}.$$

In particular, this has the form $\frac{a \pm \sqrt{b}}{2}$ for some $b \equiv 1 \pmod 4$ and odd a if u is odd, since the square of an odd rational integer is 1 mod 4, and the form $a \pm \sqrt{b}$ for $a, b \in \mathbb{Z}$ if u is even. This is our wanted characterisation: the former is a root of $X^2 + uX + v$ where $u = -a$ and $u^2 - 4v = b$ which has a solution as $u^2 \equiv b \pmod 4$, while the latter is a root of $X^2 + uX + v$ where $u = -2a$ and $u^2 - 4v = 4b$ (again possible since $u^2 \equiv 4b \pmod 4$). ■

1.3 Symmetric Polynomials

Exercise 1.3.1. Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number with conjugates $\alpha_1, \dots \alpha_n$ and $f \in \mathbb{Q}[X_1, \dots, X_n]$ be a symmetric monic polynomial. Show that $f(\alpha_1, \dots, \alpha_n)$ is rational. Further, prove that if α is an algebraic integer and f has integer coefficients, $f(\alpha_1, \dots, \alpha_n)$ is in fact a rational integer.

Solution

Write $f(X_1, \dots, X_n) = g(e_1, \dots, e_n)$ with $g \in \mathbb{Z}[X]$. Then,

$$f(\alpha_1, \dots, \alpha_n) = g(e_1(\alpha_1, \dots, \alpha_n), \dots, e_n(\alpha_1, \dots, \alpha_n))$$

is a rational integer as $e_k(\alpha_1, \dots, \alpha_n)$ is $\pm$ the coefficient of X^{n-k} of the minimal polynomial π_α of α by Vieta's formulas A.1.4, and hence a rational integer. ■

Exercise 1.3.2*. Prove that $\overline{\mathbb{Z}}$ is closed under multiplication.

Solution

Let m and n be the degree of two algebraic integers α and β. The polynomial

$$f = \prod_{i,j} X - \alpha_i \beta_j = \prod_i \alpha_i^n \prod_j X/\alpha_i - \beta_j = \prod_i \alpha_i^n \pi_\beta(X/\alpha_i)$$

is symmetric as a polynomial (over the ring $\mathbb{Z}[X]$) in $\alpha_1, \dots, \alpha_m$ (note that $Y^n \pi_\beta(X/Y)$ is indeed a polynomial in Y) and hence takes value in

$$\mathbb{Z}[X][e_1(\alpha_1, \dots, \alpha_n), \dots, e_n(\alpha_1, \dots, \alpha_n)] = \mathbb{Z}[X].$$

■

Exercise 1.3.3*. Prove Proposition 1.3.1.

Solution

Note that the assumption $f \equiv g \pmod m$ implies that $a \equiv b \pmod m$. By multiplying f and g by the inverse of their leading coefficient modulo m, we may thus assume that they are monic. Let $s = h(e_1, \dots, e_n)$ with $h \in \mathbb{Z}[X]$ be a symmetric polynomial in $\mathbb{Z}[X_1, \dots, X_n]$. Then,

$$e_k(\alpha_1, \dots, \alpha_n) \equiv e_k(\beta_1, \dots, \beta_n)$$

by Vieta's formulas since $f \equiv g \pmod m$. Finally, this implies that

$$\begin{aligned} s(\alpha_1, \dots, \alpha_n) &= h(e_1(\alpha_1, \dots, \alpha_n), \dots, e_n(\alpha_1, \dots, \alpha_n)) \\ &\equiv h(e_1(\beta - 1, \dots, \beta_n), \dots, e_n(\beta_1, \dots, \beta_n)) \\ &= s(\beta_1, \dots, \beta_n) \end{aligned}$$

as wanted. ■

1.4 Worked Examples

Exercise 1.4.1*. Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number. Prove that there exists a rational integer $N \neq 0$ such that $N\alpha$ is an algebraic integer.

Solution

Let α be an algebraic number with minimal polynomial $f = X^n + \ldots + a_1X + a_0 \in \mathbb{Q}[X]$. Let N be the lcm of the denominators of $a_{n-1}, \ldots, a_0$. Then,

$$N^n f(X/N) = X^n + Na_{n-1}X^{n-1} + N^2a_{n-2}X^{n-2} + \ldots + N^{n-1}a_1X + N^n a_0$$

has integer coefficients and is zero at $N\alpha$, as wanted. ■

1.5 Exercises

Elementary-Looking Problems

Exercise 1.5.1†. Find all non-zero rational integers $a, b, c \in \mathbb{Z}$ such that $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ and $\frac{b}{a} + \frac{c}{b} + \frac{a}{c}$ are also integers.

Solution

Notice that the polynomial

$$\left(X - \frac{a}{b}\right)\left(X - \frac{b}{c}\right)\left(X - \frac{c}{a}\right) = X^3 - \left(\frac{a}{b} + \frac{b}{c} + \frac{c}{a}\right)X^2 + \left(\frac{b}{a} + \frac{c}{b} + \frac{a}{c}\right)X - 1$$

has integer coefficients by assumption. Thus, $\frac{a}{b}, \frac{b}{c}, \frac{c}{a}$ are rational algebraic integers, i.e. rational integers. Since their product is 1, they must all be ± 1, i.e. $|a| = |b| = |c|$. Conversely, these clearly work. ■

Exercise 1.5.3† (USAMO 2009)**.** Let $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ be two non-constant sequences of rational numbers such that $(a_i - a_j)(b_i - b_j) \in \mathbb{Z}$ for any i, j. Prove that there exists a non-zero rational number r such that $r(a_i - a_j)$ and $\frac{b_i - b_j}{r}$ are integers for any i, j.

Solution

Without loss of generality, by translating the sequences, we may assume that $a_0 = b_0 = 0$. Thus, setting $j = 0$, we have $a_i b_i \in \mathbb{Z}$ for all i. The condition $(a_i - a_j)(b_i - b_j) \in \mathbb{Z}$ then reads $a_i b_j + a_j b_i \in \mathbb{Z}$. We deduce that $a_i b_j$ and $a_j b_i$ are algebraic integers, since they are roots of

$$(X - a_i b_j)(X - a_j b_i) = X^2 - X(a_i b_j + a_j b_i) + a_i b_i a_j b_j \in \mathbb{Z}[X].$$

Since they are rational, they must be rational integers, i.e. $a_i b_j \in \mathbb{Z}$ for every i, j. Choose k such that $a_k \neq 0$, there exists one since $(a_n)_{n\geq 0}$ is non-constant. Let d be the gcd of the numbers $a_k b_j$. Then, $r = a_k/d$ works. Indeed, we already have that $rb_j \in \mathbb{Z}$ for all j so it remains to show that $a_i/r \in \mathbb{Z}$ for all i. By Bézout's lemma, d is a linear combination of some $a_k b_j$, so that $ra_i = da_i/a_k$ is a linear combination of some $a_i b_j$ and thus an integer as wanted. ■

Exercise 1.5.5† (Adapted from Irish Mathematical Olympiad 1998)**.** Let $x \in \mathbb{R}$ be a real number such that both $x^2 - x$ and $x^n - x$ for some $n \geq 3$ are rational. Prove that x is rational.

Solution

Let $a = x^2 - x$. Suppose for the sake of a contradiction that x is irrational, so that its minimal polynomial is $X^2 - X - a$. Let y be its other conjugate. Then, $x^n - x = y^n - y$. Since the root of $X^2 - X - a$ are $\frac{1 \pm \sqrt{4a+1}}{2}$, we get

$$\left(\frac{1}{2} + \delta\right)^n - \left(\frac{1}{2} + \delta\right) = \left(\frac{1}{2} - \delta\right)^n - \left(\frac{1}{2} - \delta\right),$$

where $\delta = \frac{\sqrt{4a+1}}{2}$. We shall prove that this is only possible for $\delta \in \{0, \pm 1/2\}$, which is a contradiction since δ is irrational by assumption. Since this is equation is symmetric between δ and $-\delta$, it suffices to prove that it has no positive solution $\delta \neq \frac{1}{2}$. By dividing it by $\delta - 1/2$, we wish to show that

$$\frac{\left(\frac{1}{2} + \delta\right)^n - 1}{\delta - \frac{1}{2}} + \left(\frac{1}{2} - \delta\right)^{n-1} - 2 = \sum_{i=0}^{n-1} \left(\frac{1}{2} + \delta\right)^i + \left(\frac{1}{2} - \delta\right)^{n-1} - 2$$

is positive for positive δ.

Suppose first that $\delta \leq \frac{1}{2}$. Then, we have

$$\sum_{i=0}^{n-2} \left(\frac{1}{2} + \delta\right)^i > \sum_{i=0}^{n-2} \left(\frac{1}{2}\right)^i = 2 - \left(\frac{1}{2}\right)^{n-2}$$

and

$$\left(\frac{1}{2} + \delta\right)^{n-1} + \left(\frac{1}{2} - \delta\right)^{n-1} \geq \left(\frac{1}{2}\right)^{n-1} + \left(\frac{1}{2}\right)^{n-1} = \left(\frac{1}{2}\right)^{n-1}$$

by the power mean inequality.

Now, if $\delta \geq \frac{1}{2}$ the inequality is trivial: since $n \geq 3$ we have

$$\sum_{i=0}^{n-2} \left(\frac{1}{2} + \delta\right)^i \geq 1 + 1 = 2$$

and

$$\left(\frac{1}{2} + \delta\right)^{n-1} + \left(\frac{1}{2} - \delta\right)^{n-1} > 0.$$

■

Exercise 1.5.9†. Let $|x| < 1$ be a complex number. Define

$$S_n = \sum_{k=0}^{\infty} k^n x^k.$$

Suppose that there is an integer $N \geq 0$ such that $S_N, S_{N+1}, \ldots$ are all rational integers. Prove that S_n is a rational integer for any integer $n \geq 0$.

Solution

We shall prove that $S_0 = \frac{1}{1-x}$ is a rational integer, and that this implies that S_n is a rational

integer for all n. By differentiating the equality

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$$

n times, we get

$$R_n := \sum_{k=0}^{\infty} (k+1)(k+2)\cdot\ldots\cdot(k+n)x^k = \frac{(-1)^n n!}{(1-x)^n}.$$

Define $f_n(X) := (X+1)\cdot\ldots\cdot(X+m)$. Since each f_m is monic and has degree n, they form a $\mathbb{Z}$-basis of $\mathbb{Z}[X]$, meaning that any element of $\mathbb{Z}[X]$ can be represented as a linear combination $\sum_k a_k f_k$ for some $a_i \in \mathbb{Z}$. This is in particular the case for X^n, say $X^n = \sum_{i=0}^n a_{k,n} f_k$ so that

$$S_n = \sum_{i=0}^{n} a_{k,n} R_i.$$

This shows that, if $\frac{1}{1-x}$ is a rational integer, then so is R_n for all n and hence S_n for all n.

Now, note that S_N is a polynomial with integer coefficients in $\frac{1}{1-x}$, so $\frac{1}{1-x}$ and thus x is algebraic.

Now, write f_n as a linear of X^k, i.e. $f_n = \sum_{k=0}^n b_{k,n} X^k$ (this is just regular expansion). Let p be a large rational prime which divides neither the numerator or the denominator of the norm of $1-x$, so that $1-x$ is invertible modulo p by Exercise 1.5.24†. Then,

$$R_n = \sum_{k=0}^{n} b_{k,n} S_k = \frac{(-1)^n n!}{(1-x)^n}$$

is divisible by p for $n \geq p$. Thus, we deduce that $\sum_{k=0}^N b_{k,n} S_k$ is congruent to a rational integer modulo p. The idea now is to take many n so that the vectors $(b_{0,n}, \ldots, b_{N,n})$ are linearly independent using Exercise C.5.9†, i.e. so that they have a non-zero determinant. Then, for p sufficiently large, p the determinant is also non-zero modulo p. Since the inverse of a matrix with coordinates in $\mathbb{F}_p$ also has coordinates in $\mathbb{F}_p$, this implies that $S_0, \ldots, S_N$ are congruent to rational integers modulo p. By taking p sufficiently large and using Exercise 1.5.26†, we deduce that $S_0, \ldots, S_N$ are rational numbers. Finally, we shall look at the p-adic valuation of $S_0 = \frac{1}{1-x}$ to prove that it's an integer.

To use Exercise C.5.9†, we need to prove that $b_{0,n}, \ldots, b_{N,n}$ all grow at different rates. We have

$$b_{n,k} = n! \sum_{1 \leq i_1 < \ldots < i_k \leq n} \frac{1}{i_1 \cdot \ldots \cdot i_k} \sim \frac{n!}{k!} \left(\sum_{i=1}^{n} \frac{1}{i} \right)^k \sim \frac{n! \log(n)^k}{k!}$$

which shows that the assumptions are satisfied. As said before, we get that $S_0, \ldots, S_N$ are congruent to rational integers modulo p. Thus, for p sufficiently large, they must all be rational. Finally, suppose some prime p divides the denominator of $\frac{1}{1-x}$. Since $b_{k,n}$ for a fixed k eventually becomes divisible by anything, $\sum_{k=0}^N b_{n,k} S_k$ is a rational integer for sufficiently large n. However, it is congruent modulo 1 to $\frac{(-1)n!}{(1-x)^n}$ which is not an integer since $v_p(n!) < n$ by Legendre's formula 8.3.5; this is a contradiction. ■

Exercise 1.5.10†. Let $n \geq 3$ be an integer. Suppose that there exist a regular n-gon with integer coordinates. Prove that $n = 4$.

Solution

Let A, B, C be three consecutive vertices. Since the sum of the angles of the n-gon is $(n-2)\pi$, the angle $\angle ABC$ is $\pi\frac{n-2}{n} = \pi - \frac{2\pi}{n}$. By the cosine law, we have

$$\frac{1+\cos\frac{4\pi}{n}}{2} = \cos\left(\frac{2\pi}{n}\right)^2 = \cos\left(\pi - \frac{2\pi}{n}\right)^2 = \frac{(AB^2+BC^2-AC^2)^2}{4AB^2\cdot BC^2}.$$

Since A, B, C have integer coordinates, this is rational so $\cos\frac{4\pi}{n}$ is rational. Finally, using Problem 1.1.1, we must have $n \in \{1, 2, 4, 8\}$. It remains to prove that $n = 8$ is impossible.

We have $\angle BAC = \angle BCA = \frac{\pi}{n}$. By the sine law,

$$\frac{AB^2}{\cos\left(\frac{\pi}{n}\right)^2} = \frac{AC^2}{\cos\left(\frac{2\pi}{n}\right)^2}.$$

This is impossible since the RHS is rational while the LHS isn't for $n = 8$ (we are again using the identity $\cos(x)^2 = \frac{1+\cos(x)^2}{2}$). ■

Exercise 1.5.11†. Let $\mathcal{P}$ be a polygon with rational sidelengths for which there exists a real number $\alpha \in \mathbb{R}$ such that all its angles are rational multiples of α, except possibly one. Prove that $\cos\alpha$ is algebraic.

Solution

Note that $\cos\alpha$ being algebraic is equivalent to $\exp(i\alpha)$ being algebraic, since if z is algebraic then so is $z + \overline{z} = 2\Re(z)$. Without loss of generality, we may assume that the angles which are rational multiple of α are in fact positive integer multiples of α, by rescaling α.

Let X_k denote the kth vertex and let n denote the number of vertices. Represent the polygon by complex numbers: X_k is represented by $x_k \in \mathbb{C}$. We have

$$\frac{x_k - x_{k+1}}{x_k - x_{k-1}} = \exp(i\angle X_{k-1}X_kX_{k+1})\frac{|x_k - x_{k+1}|}{|x_k - x_{k-1}|}.$$

Without loss of generality, we may assume that the angle which is potentially not an integer multiple of α is $X_{n-1}X_nX_1$, so that $\angle X_{k-1}X_kX_{k+1}$ is $a_k\alpha$ for some $a_k \in \mathbb{N}$ for $k = 1, \ldots, n-1$. Denote also $\frac{|x_k - x_{k+1}|}{|x_k - x_{k-1}|}$ by $r_k \in \mathbb{Q}$. Thus, the condition reads

$$\frac{x_k - x_{k+1}}{x_k - x_{k-1}} = r_k\exp(ia_k\alpha).$$

By rescaling the x_i, we may assume that $x_1 - x_n = 1$. Thus,

$$x_1 - x_2 = r_1\exp(ia_1\alpha) := s_1\exp(ib_1\alpha).$$

This implies that

$$x_2 - x_3 = (x_2 - x_1)r_2\exp(ia_2\alpha) = -r_1r_2\exp(i(a_1+a_2)\alpha) := s_2\exp(b_2\alpha).$$

Continuing like that, we get

$$x_k - x_{k+1} = -r_ks_{k-1}\exp(i(b_{k-1}+a_k)\alpha) := s_k\exp(ib_k\alpha)$$

for some $s_k \in \mathbb{Q}$ and $b_k \in \mathbb{N}$. Finally, since

$$\sum_{k=1}^{n-1} s_k\exp(ib_i\alpha) = \sum_{k=1}^{n-1} x_k - x_{k+1} = x_1 - x_n = 1,$$

$\exp(i\alpha)$ is algebraic as wanted since it's a root of

$$s_{n-1}X^{b_{n-1}} + s_{n-2}X^{b_{n-2}} + \ldots + s_1X^{b_1} - 1.$$

■

Exercise 1.5.15†. Let $\omega_1, \ldots, \omega_m$ be nth roots of unity. Prove that $|\omega_1 + \ldots + \omega_n|$ is either zero or greater than m^{-n}.

Solution

Let $\omega = \exp\left(\frac{2i\pi}{n}\right)$ be a primitive nth rooth of unity so that each ω_i is a power of ω, say ω^{k_i}. We shall multiply

$$\omega_1 + \ldots + \omega_m = \omega^{k_1} + \ldots + \omega_m^{k_m}$$

by its conjugates, which are among $\omega^{\ell k_1} + \ldots + \omega_m^{\ell k_m}$ by the fundamental theorem of symmetric polynomials. Suppose that it is non-zero. Taking the product over its conjugates, we get that

$$\prod_{\ell} \omega^{\ell k_1} + \ldots + \omega_m^{\ell k_m}$$

is a non-zero rational integer. Thus, it is at least one in absolute value. Since $|\omega^{\ell k_1} + \ldots + \omega_m^{\ell k_m}| \leq m$ by the triangular inequality, we finally get

$$m^{n-1}|\omega_1 + \ldots + \omega_m| \geq 1,$$

i.e. $|\omega_1 + \ldots + \omega_m| \geq m^{1-n} \geq m^{-n}$ as wanted. ■

Remark 1.5.1

In fact, since ω has only $\varphi(n)$ conjugates and not n (see Chapter 3), we get the stronger bound $|\omega_1 + \ldots + \omega_m| \geq m^{1-\varphi(n)}$.

Exercise 1.5.16†. Let $n \geq 1$ and $n_1, \ldots, n_k$ be integers. Prove that

$$\left|\cos\left(\frac{2\pi n_1}{n}\right) + \ldots + \cos\left(\frac{2\pi n_k}{n}\right)\right|$$

is either zero or greater than $\frac{1}{2(2k)^{n/2}}$.

Solution

We imitate our proof of Exercise 1.5.15†: since $2\cos\left(\frac{2\ell\pi}{n}\right) = \exp\left(\frac{2\ell i\pi}{n}\right) + \exp\left(-\frac{2\ell i\pi}{n}\right)$, the fundamental theorem of symmetric polynomials shows that

$$\prod_{\ell} 2\cos\left(\frac{2\ell n_1\pi}{n}\right) + \ldots + 2\cos\left(\frac{2\ell n_k\pi}{n}\right)$$

is an integer, where the product is taken over the conjugates of $2\cos\left(\frac{2n_1\pi}{n}\right) + \ldots + 2\cos\left(\frac{2n_k\pi}{n}\right)$. Suppose that it is non-zero, so that this product is non-zero too. Then, as

$$\left|2\cos\left(\frac{2\ell n_1\pi}{n}\right) + \ldots + 2\cos\left(\frac{2\ell n_k\pi}{n}\right)\right| \leq 2k$$

by the triangular inequality, we have

$$(2k)^{n/2}\left|2\cos\left(\frac{2n_1\pi}{n}\right)+\ldots+2\cos\left(\frac{2n_k\pi}{n}\right)\right|\geq\prod_{\ell}\left|2\cos\left(\frac{2\ell n_1\pi}{n}\right)+\ldots+2\cos\left(\frac{2\ell n_k\pi}{n}\right)\right|\geq 1$$

since $2\cos\left(\frac{2n_1\pi}{n}\right)+\ldots+2\cos\left(\frac{2n_k\pi}{n}\right)$ has at most $\frac{n+1}{2}\geq n/2+1$ conjugates (since $\cos x=\cos(2\pi-x)$ so half the potential conjugates get discarded). Thus, we get

$$\left|\cos\left(\frac{2\pi n_1}{n}\right)+\ldots+\cos\left(\frac{2\pi n_k}{n}\right)\right|\geq\frac{1}{2(2k)^{n/2}}$$

as wanted. ■

Remark 1.5.2

In fact, since $\cos\left(\frac{2\ell\pi}{n}\right)$ has only $\varphi(n)/2$ conjugates for $n>2$ and not n (see Chapter 3), we get the stronger bound

$$\left|\cos\left(\frac{2\pi n_1}{n}\right)+\ldots+\cos\left(\frac{2\pi n_k}{n}\right)\right|\geq\frac{k}{2(2k)^{\varphi(n)/2}}$$

for $n>2$ (for $n\leq 2$ we get the bound 1).

Exercise 1.5.17† (USA TST 2014)**.** Let N be an integer. Prove that there exists a rational prime p and an element $\alpha\in\mathbb{F}_p^\times$ such that the orbit $\{1,\alpha,\alpha^2,\ldots\}$ has cardinality at least N and is sum-free, meaning that $\alpha^i+\alpha^j\neq\alpha^k$ for any i,j,k. (You may assume that, for any n, there exist infinitely many primes for which there is an element of order n in $\mathbb{F}_p$. This will be proven in Chapter 3.)

Solution

Let us fix the order n of α and suppose that any prime p for which there is an element of order n fails. Let $\omega=\exp\left(\frac{2i\pi}{n}\right)$ be a primitive nth root of unity. By Proposition 1.3.1, we have

$$\prod_{i,j,k}\alpha^i+\alpha^j-\alpha^k\equiv\prod_{i,j,k}\omega^i+\omega^j-\omega^k.$$

Thus, if the LHS is divisible by infinitely many primes, the RHS must be zero. However, it is easy to see that, when ζ is a root of unity, $\zeta+1$ is also one if and only if $\zeta=\exp\left(\frac{\pm 2i\pi}{3}\right)$. Indeed, if $\zeta=\exp(i\theta)$, then, by looking at the imaginary part of $\zeta+1$, we get $\zeta+1=\exp(i(2\pi-\theta))$. Then, by looking at the real parts we get $\cos(\theta)+1=\cos(2\pi-\theta)=-\cos(\theta)$ which gives $\cos(\theta)=-\frac{1}{2}$ as wanted. Thus, if $6\nmid n$, $\omega^i+\omega^j=\omega^k$ is impossible since this implies $\omega^{i-j}+1=\omega^{k-i}$ so ω^{k-i} would be $\exp\left(\frac{2\pi}{6}\right)$. We are done: we just need to choose an $n\geq N$ which is not divisible by 3. (As a bonus, if $6\mid n$ then any p fails since $\alpha^{n/3}+1=-\alpha^{2n/3}=\alpha^{n/6}$, while for $6\nmid n$ we have proven that all sufficiently large p work.) ■

Properties of Algebraic Numbers

Exercise 1.5.20†**.** Let $\alpha\in\overline{\mathbb{Q}}$ be an algebraic number with conjugates $\alpha_1,\ldots,\alpha_n$ and $f\in\mathbb{Q}[X]$ be a polynomial. Prove that the m conjugates of $f(\alpha)$ are each represented exactly $\frac{n}{m}$ times among $f(\alpha_1),\ldots,f(\alpha_n)$.

Solution

First, note that these are all conjugates since if $f(\alpha)$ is a root of g, then α is a root of $f \circ g$ so the same goes for its conjugates. Second, note that there are no other conjugates since $\prod_{i=1}^{n} X - f(\alpha_i)$ has rational coefficients by the fundamental theorem of symmetric polynomials. Finally, since the roots of this polynomial are exactly the roots of $\pi_{f(\alpha)}$ (which is irreducible), it must be a power of $\pi_{f(\alpha)}$, say $\pi_{f(\alpha)}^{k}$. Then, each $f(\alpha_i)$ is repeated k times and $f(\alpha)$ has degree $\frac{n}{k}$ as wanted. ■

Exercise 1.5.21. Let $\alpha_1, \ldots, \alpha_m \in \overline{\mathbb{Q}}$ be algebraic number and $f \in \mathbb{Q}[X_1, \ldots, X_m]$ a polynomial. Denote the conjugates of α_k by $\alpha_k^{(1)}, \ldots, \alpha_k^{(n_i)}$. Prove that the conjugates of $f(\alpha_1, \ldots, \alpha_k)$ are among

$$\{f(\alpha_1^{(i_1)}, \ldots, \alpha_m^{(i_m)}) \mid i_k = 1, \ldots, n_k\}.$$

Solution

This is a consequence of the fundamental theorem of symmetric polynomials. (For a rigorous proof, one may induct on m.) ■

Exercise 1.5.22†. Let $f \in \overline{\mathbb{Z}}[X]$ be a monic polynomial and α be one of its roots. Prove that α is an algebraic integer.

Solution

Let $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in \overline{\mathbb{Z}}[X]$ be a polynomial and let $a_k^{(1)}, \ldots, a_k^{(n_k)}$ be the conjugates of a_k. The fundamental theorem of symmetric polynomials then shows that the polynomial

$$\prod_{i_0, \ldots, i_{n-1}} X^n + a_{n-1}^{(i_{n-1})} + \ldots + a_0^{(i_0)}$$

has integer coefficients. Since it is monic, its roots are algebraic integers, and since it is divisible by f, the same goes for f.

Alternatively, one can use Proposition C.3.5: $M = \mathbb{Z}[a_{n-1}, \ldots, a_0]$ is a finitely generated $\mathbb{Z}$-module such that $\alpha M \subseteq M$ for any root α of f. ■

Exercise 1.5.23†. We say an algebraic integer $\alpha \in \overline{\mathbb{Z}}$ is a *unit* if there exists an algebraic integer $\alpha' \in \overline{\mathbb{Z}}$ such that $\alpha\alpha' = 1$. Characterise all units.

Solution

Let $\alpha \in \overline{\mathbb{Q}}$ be a non-zero algebraic number and let $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ be its minimal polynomial. Then, $1/\alpha$ is a root of $a_0X^n + a_1X^{n-1} + \ldots + 1$ which shows that its degree is at most n. By reiterating this process, we get that the degree of α is also at most n, which implies that we have equality. Hence

$$X^n + \frac{a_1}{a_0}X^{n-1} + \ldots + \frac{1}{a_0}$$

is the minimal polynomial of $1/\alpha$. In particular, for $\alpha \in \overline{\mathbb{Z}}$, $1/\alpha$ is an algebraic integer if and only if $a_0 \mid 1$, i.e. $a_0 = \pm 1$. This is also equivalent to $|\,\mathrm{N}(\alpha)| = 1$. An alternative solution is given

in Exercise 7.1.1*: if α is invertible than so are its conjugates so the same goes for the product of its conjugates, i.e. its norm. Hence, $|\mathrm{N}(\alpha)| = 1$ if α is invertible. Conversely, if $N(\alpha) = \pm 1$, then $\pm\alpha_2 \cdot \ldots \cdot \alpha_n$ is the inverse of α, where $\alpha_2, \ldots, \alpha_n$ are its conjugates distinct from itself. ■

Exercise 1.5.24†. Let m be a rational integer. We say an algebraic integer $\alpha \in \overline{\mathbb{Z}}$ is a *unit mod m* if there exists an algebraic integer $\alpha' \in \overline{\mathbb{Z}}$ such that $\alpha\alpha' \equiv 1 \pmod{m}$. Characterise all units mod m.

Solution

Here we imitate the second solution of Exercise 1.5.23†. If α is invertible modulo m, then so are its conjugates so the same goes for its norm. Conversely, if its norm is invertible modulo m, then $(\mathrm{N}(\alpha))^{-1}\alpha_2 \cdot \ldots \cdot \alpha_n$ is the inverse of α, where $\alpha_2, \ldots, \alpha_n$ are its conjugates distinct from itself■

Exercise 1.5.26†. Let $\alpha \in \overline{\mathbb{Z}}$ be an non-rational algebraic integer. Prove that there are a finite number of rational integers m such that α is congruent to a rational integer mod m.

Solution

Suppose that $\alpha \equiv k \pmod{m}$ for some $k \in \mathbb{Z}$. Then, all its conjugates are also congruent to k modulo m (by conjugating both sides) which implies

$$\pi_\alpha \equiv (X - k)^n \pmod{m}$$

where $n \geq 2$ is the degree of α. In particular, π_α has a double root modulo m, so m divides the discriminant of π_α by Remark 1.3.2. Since π_α has distinct roots by Exercise 1.2.3*, the discriminant is non-zero so there are indeed a finite number of such m. ■

Exercise 1.5.27† (Kronecker's Theorem)**.** Let $\alpha \in \overline{\mathbb{Z}}$ be a non-zero algebraic integer such that all its conjugates have module at most 1. Prove that it is a root of unity.

Solution

Let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α. By the fundamental theorem of symmetric polynomials,

$$f_m := \prod_{i=1}^{n} X - \alpha_i^m$$

has integer coefficients for all positive integers α. Moreover, its coefficients are bounded: by the triangular inequality,

$$|e_k(\alpha_1, \ldots, \alpha_n)| = \left| \sum_{i_1 < \ldots < i_k} \alpha_{i_1} \cdot \ldots \cdot \alpha_{i_k} \right| \leq \sum_{i_1 < \ldots < i_k} 1 = \binom{k}{n}.$$

Thus, there exist r and s such that $f_{2^r} = f_{2^{r+s}}$. This means that raising the roots $\alpha_i^{2^r}$ of f_{2^r} to the 2^s power permutes them. If we iterate this permutation starting from α^{2^r}, we will eventually cycle back to α^{2^r}, i.e.

$$\alpha^{2^r} = \alpha^{2^{r+ks}}$$

for some $k > 0$. Since $\alpha \neq 0$, it must be a root of unity. ■

Exercise 1.5.28†. Determine all non-zero algebraic integers $\alpha \in \overline{\mathbb{Z}}$ such that all its conjugates are **real** and have module at most 2.

Solution

Let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α. Notice that $\frac{\alpha_k + i\sqrt{4-\alpha_k^2}}{2}$ has module 1. Now,

$$\left(X - \frac{\alpha_k + i\sqrt{4-\alpha_k^2}}{2}\right)\left(X - \frac{\alpha_k - i\sqrt{4-\alpha_k^2}}{2}\right) = X^2 - \alpha_k X + 1$$

so that

$$\prod_{k=1}^{n}\left(X - \frac{\alpha_k + i\sqrt{4-\alpha_k^2}}{2}\right)\left(X - \frac{\alpha_k - i\sqrt{4-\alpha_k^2}}{2}\right)$$

has integer coefficients. Since all its roots have module 1, by Kronecker's theorem 1.5.27†, we get that $\frac{\alpha + i\sqrt{4-\alpha^2}}{2}$ is a root of unity. Since $\alpha/2$ is its real part, we get $\alpha = 2\cos\left(\frac{2k\pi}{m}\right)$ for some k, m. Conversely, such α work since the conjugates of

$$2\cos\left(\frac{2k\pi}{m}\right) = \exp\left(\frac{2ki\pi}{m}\right) + \exp\left(-\frac{2ki\pi}{m}\right)$$

are among $2\cos\left(\frac{2\ell\pi}{m}\right)$ for $\ell \in \mathbb{Z}$ by the fundamental theorem of symmetric polynomials. ■

Exercise 1.5.29†. Suppose that ω is a root of unity whose real part is an algebraic integer. Prove that $\omega^4 = 1$.

Solution

Suppose that $\omega^2 \neq 1$. Then, by the triangular inequality,

$$\Re(\omega) = \frac{\omega + \omega^{-1}}{2} < \frac{1+1}{2} = 1$$

since the inequality case would imply $\omega = \omega^{-1}$, i.e. $\omega^2 = 1$. Notice that, since the conjugates of roots of unity are roots of unity, the conjugates of $\Re(\omega) = \frac{\omega+\omega^{-1}}{2}$ also all have absolute value at most 1 by the triangular inequality, and are algebraic integers by assumption. Thus, the product of $\Re(\omega)$ and its conjugates has absolute value strictly less than 1. Since it's an integer it must hence be zero, which implies $\Re(\omega) = 0$, i.e. $\omega = \pm i$ which satisfies $\omega^4 = 1$ as wanted. ■

Exercise 1.5.30†. Let $\omega_1, \ldots, \omega_n$ be roots of unity. Suppose that $\frac{1}{n}(\omega_1 + \ldots + \omega_n)$ is a non-zero algebraic integer. Prove that $\omega_1 = \ldots = \omega_n$.[1]

Solution

Notice that, by the triangular inequality, if $\omega_1, \ldots, \omega_n$ are not all equal, then $\frac{1}{n}(\omega_1 + \ldots + \omega_n)$ has absolute value strictly less than 1. Since its conjugates all have absolute value at most 1 by the triangular inequality, the product of $\frac{1}{n}(\omega_1 + \ldots + \omega_n)$ with its conjugates has absolute value strictly less than 1. Since it's a rational integer, it must be zero. This implies $\frac{1}{n}(\omega_1 + \ldots + \omega_n) = 0$,

[1] In fact, any algebraic integer that can be written as a linear combination of roots of unity with rational coefficients can also be written as a linear combination of roots of unity with integer coefficients. However, this is a difficult result to prove (see Exercise 3.5.26† for a special case).

contradicting our initial assumption. ■

Exercise 1.5.31†. Let $\alpha \in \overline{\mathbb{Z}}$ be an algebraic number and let p be a rational prime. Must it follow that $\alpha^n \equiv 0 \pmod{p}$ or $\alpha^n \equiv 1 \pmod{p}$ for some $n \in \mathbb{N}$?[2]

Solution

The answer is **No**. As a counterexample, we can try to find an α such that the sequence $(\alpha^n)_{n\geq 1}$ is constant modulo p and not congruent to 1 modulo p. The simplest possible p is $p = 2$, so let's pick $p = 2$. Then, one of the simplest ways to achieve $\alpha^2 \equiv \alpha \pmod{2}$ and $\alpha \not\equiv 0, 1 \pmod{2}$ is to choose α such that $\alpha^2 = \alpha - 2$. Such an α must clearly be irrational. By Exercise 1.5.24†, α is not invertible modulo 2, but it is also non-zero since $2 = \alpha\beta$ is not divisible by $2 \cdot 2$, where β is the other conjugate of α. Indeed, if 2 divided α, then it would also divide β: $\alpha/2$ is an algebraic integer so its conjugate $\beta/2$ is as well byExercise 1.2.4*. We can also show directly that $\alpha \not\equiv \pmod{2}$ without invoking Exercise 1.5.24†: if $\frac{\alpha-1}{2}$ were an integer, then so would $\frac{\beta-1}{2}$, so their product

$$\frac{\alpha-1}{2} \cdot \frac{\beta-1}{2} = \frac{\alpha\beta - (\alpha+\beta) + 1}{4} = \frac{2-1+1}{4} = \frac{1}{2}$$

which is not the case.

A more elaborate example, which also sheds a lot of light on the situation, is the following. Consider a prime $p \equiv 1 \pmod{4}$ and factorise it as $\pi\overline{\pi}$ in the Gaussian integers $\mathbb{Z}[i]$. By **??**, π and $\overline{\pi}$ aren't associates so, with the help of the Chinese remainder theorem (in $\mathbb{Z}[i]$), we can pick an $\alpha \in \mathbb{Z}[i]$ congruent to 0 modulo π and to 1 modulo $\overline{\pi}$. Then, the powers of α are clearly congruent to α modulo π and $\overline{\pi}$, so modulo $p = \pi\overline{\pi}$. However, α is congruent to neither 0 or 1 modulo p. In fact, this is the only way such a counterexample happens, but we need to replace the factorisation in prime elements (which doesn't always hold) by the factorisation in prime ideals (which always holds). ■

[2] In Chapter 4, we prove that the answer is positive for sufficiently large p.

Chapter 2

Quadratic Integers

Exercise 2.0.1. Why is the "naive" approach of factorising the equation as $x^2 = (y-1)(y^2+y+1)$ difficult to conclude with? Why does our solution not work as well for the equation $x^2 - 1 = y^3$?

Solution

One reason is that both of these approaches transform one diophantine equation into **two** simultaneous diophantine equations. On the other hand, since i and $-i$ are conjugate, $(x+i)(x-i) = y^3$ gives us only one equation, since, from $(x+i)^3 = (a+bi)^3$, we also get $(x-i)^3 = (a-bi)^3$ by conjugating. ■

2.1 General Definitions

Exercise 2.1.1*. Prove that $\mathbb{Z} + \alpha\mathbb{Z}$ is a ring for any quadratic integer α. This amounts to checking that it is closed under addition, subtraction, and multiplication. What happens if α is a quadratic number which is not an integer?

Solution

Suppose that $\alpha^2 - u\alpha - v = 0$, i.e. $\alpha^2 = u\alpha + v$ where $u, v \in \mathbb{Z}$. We have

$$(a + b\alpha) \pm (c + d\alpha) = (a \pm c) + (b \pm d)\alpha$$

and

$$\begin{aligned}(a + b\alpha)(c + d\alpha) &= ac + (ad + bc)\alpha + bd\alpha^2 \\ &= ac + (ad + bc)\alpha + bd(u\alpha + v) \\ &= (ac + bdv) + (ad + bc + bdu)\alpha\end{aligned}$$

If α is not a quadratic integer, then α^2 is not a linear combination of 1 and α with rational integer coefficients, so $\mathbb{Z}[\alpha]$ would not be closed under multiplication with this definition (and thus not a ring). ■

Exercise 2.1.2*. Prove that $\alpha + \alpha\mathbb{Q}$ is a ring for any quadratic integer α. This amounts to checking that it is closed under addition, subtraction, multiplication, and division.

Solution

The same proof as the one of Exercise 2.1.1* shows that it is a ring, so it remains to prove that every non-zero element has inverses. If we multiply $a+b\alpha$ by $a+b\overline{\alpha}$ where $\overline{\alpha}$ is the other conjugate of α, we get a rational number c by the fundamental theorem of symmetric polynomials. Moreover, this number is zero only if one of $a+b\alpha$ and $a+b\overline{\alpha}$ is zero, which implies that the other is too since they are conjugate. Indeed, if $f(a+bX)$ has a root at α it has one at $\overline{\alpha}$ too.

Hence, when $a+b\alpha$ is non-zero, it has an inverse

$$\frac{a+b\overline{\alpha}}{c}.$$

To conclude, note that, if $\alpha^2+u\alpha+v=0$, then $\overline{\alpha}=-u-\alpha$ by Vieta's formulas so $\overline{\alpha}\in\mathbb{Q}(\alpha)$.■

Exercise 2.1.3*. Let α be a quadratic number and $\beta\in\mathbb{Q}(\alpha)$. Show that β has degree 1 or 2.

Solution

As in Exercise 2.1.2*, let $\overline{\alpha}\in\mathbb{Q}(\alpha)$ be the conjugate of α. Let $\beta=a+b\alpha$ with $a,b\in\mathbb{Q}$. Then

$$(X-(a+b\alpha))(X-(a+b\overline{\alpha}))$$

has rational coefficients by the fundamental theorem of symmetric polynomials so β has degree at most 2 as wanted. ■

Exercise 2.1.4*. Prove that a quadratic field K is equal to $\mathbb{Q}(\sqrt{d})$ for some squarefree rational integer $d\neq 1$. Moreover, prove that such fields are pairwise non-isomorphic (and in particular distinct), meaning that, for distinct squarefree $a,b\neq 1$, there does not exist a bijective function $f:\mathbb{Q}(\sqrt{a})\to\mathbb{Q}(\sqrt{b})$ such that $f(x+y)=f(x)+f(y)$ and $f(xy)=f(x)f(y)$ for any $x,y\in\mathbb{Q}(\sqrt{a})$.

Solution

Let α be a quadratic number, i.e. a root of aX^2+bX+c for some $a,b,c\in\mathbb{Z}$. Then, $\alpha=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$ so $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{b^2-4ac})$. By letting d be the squarefree part of b^2-4ac (but conserving its sign), we thus get $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{d})$ as wanted (and $d\neq 1$ since it does not only have rational elements).

Let a,b be squarefree and suppose $f:\mathbb{Q}(\sqrt{u})\to\mathbb{Q}(\sqrt{v})$ is an isomorphism. We will show that $a=b$. Note that $f(1)^2=f(1)$ so $f(1)=1$ or 0 but the latter is impossible since then $f(x)=f(x)f(1)=0$ for all x. We have

$$f(u)=f(1)+f(1)+\ldots+f(1)=uf(1)=u$$

and $f(u)=f(\sqrt{u})^2$ so $\sqrt{u}\in\mathbb{Q}(\sqrt{v})$. Thus, the problem of showing that $\mathbb{Q}(\sqrt{u})$ and $\mathbb{Q}(\sqrt{v})$ are non-isomorphic when $u\neq v$ reduces to showing that they are distinct. This is easy: if $\sqrt{u}=a+b\sqrt{v}$ then $u=a^2+vb^2+2ab\sqrt{v}$ so $a=0$ or $b=0$ since $\sqrt{v}$ is irrational but the former means that u is a perfect square and the latter that u/v is one, i.e. that $u=1$ or $u=v$. ■

Exercise 2.1.5*. Prove that the conjugate is well defined.

Solution

This amounts to the fact that every element of $\mathbb{Q}(\sqrt{d})$ can be written in a unique way as $a+b\sqrt{d}$ with $a, b \in \mathbb{Q}$ which is true since $\sqrt{d}$ is irrational. ■

Exercise 2.1.6*. Let $d \neq 1$ be a rational squarefree number. Prove that the conjugation satisifes $\overline{\alpha+\beta} = \overline{\alpha}+\overline{\beta}$ and $\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$ for all $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$. Such a function is called an *automorphism* of $\mathbb{Q}(\sqrt{d})$ if it is also bijective.

Solution

We have

$$(a - b\sqrt{d}) + (a' - b'\sqrt{}) = (a+b) - (a'+b')\sqrt{d}$$

and

$$(a - b\sqrt{d})(a' - b'\sqrt{d}) = (aa' + bb'\sqrt{d}) - (ab' + ba')\sqrt{d}.$$

■

Exercise 2.1.7. Let $d \neq 1$ be a rational squarefree number. Prove that the only automorphisms of $\mathbb{Q}(\sqrt{d})$ are the identity and conjugation.

Solution

Let f by an automorphism of $\mathbb{Q}(\sqrt{d})$. Since f is bijective and $f(1)^2 = f(1)$, we must have $f(1) = 1$ as otherwise $f(x) = f(x)f(1) = 0$ for all x. By induction we have $f(nx) = f(x) + \ldots + f(x) = nf(x)$ for any $n \in \mathbb{Z}_{\geq 1}$, by it is clearly true for $n = 0$ since $f(0) + f(0) = f(0)$ and for $n < 0$ since $f(-n) = f(0) - f(n) = -f(n)$ thus $f(nx) = nf(x)$ for any $n \in \mathbb{Z}$. Since

$$nf(xm/n) = f(xm) = mf(x),$$

we also have $f(ax) = af(x)$ for any $a \in \mathbb{Q}$; in particular f fixes $\mathbb{Q}$. To finish, $f(d) = f(\sqrt{d})^2$ so $f(\sqrt{d}) = \pm\sqrt{d}$. Since $f(a + b\sqrt{d}) = a + bf(\sqrt{d})$, the plus sign gives the identity and the minus sign the conjugation. ■

Exercise 2.1.8*. Let $d \neq 1$ be a squarefree rational integer, and $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$. Prove that $N(\alpha\beta) = N(\alpha)N(\beta)$.

Solution

Let $\alpha = a + b\sqrt{d}$ and $\beta = a' + b'\sqrt{d}$. Then,

$$N(\alpha)N(\beta) = (a^2 - db^2)(a'^2 - db'^2)$$

and

$$N(\alpha\beta) = N((aa' + dbb') + (ab' + ba')\sqrt{d}) = (aa' + dbb')^2 - d(ab' + ba')^2.$$

To conclude, both sides are equal to $(aa')^2 + (dbb')^2 - d((ab')^2 + (ba')^2)$. ■

Exercise 2.1.9. Prove Exercise 2.1.8* without any computations using Exercise 2.1.6*.

Solution

We have

$$N(\alpha)N(\beta) = \alpha\overline{\alpha}\beta\overline{\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = N(\alpha\beta).$$

■

Exercise 2.1.10. Let $d < 0$ be a squarefree integer. Prove that the conjugate of an element of $\mathbb{Q}(\sqrt{d})$ is the same as its complex conjugate. In particular, the norm over $\mathbb{Q}(\sqrt{d})$ is the module squared.

Solution

When $d < 0$, the complex conjugate of $\sqrt{d}$ is $-\sqrt{d}$. Since rational numbers are real, this means that the complex conjugate of $a + b\sqrt{d}$ for $a, b \in \mathbb{Q}$ is $a - b\sqrt{d}$. ■

2.2 Unique Factorisation

Exercise 2.2.1*. Let $d \neq 1$ be a squarefree rational integer. Prove that the product of two units of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is still a unit, and that the conjugate of a unit is also a unit.

Solution

If $uu' = 1$ and $vv' = 1$ then $(uv)(u'v') = 1$ and $\overline{u}\overline{u'} = 1$. ■

Exercise 2.2.2*. Let $d \neq 1$ be a squarefree rational integer. Prove that $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a unit if and only if $|N(\alpha)| = 1$.

Solution

If $N(\alpha) = \alpha\overline{\alpha} = \pm 1$, then it is clear α is a unit. Now suppose α is a uni. By Exercise 2.2.1*, $\overline{\alpha}$ is also a unit, which means $N(\alpha) = \alpha\overline{\alpha}$ is one too. However the only rational integer units are ± 1 by Proposition 1.1.1. ■

Exercise 2.2.3*. Determine the units of the ring $\mathbb{Z}[i]$.

Solution

$a + bi$ is a unit of $\mathbb{Z}[i]$ if and only if its norm $a^2 + b^2$ is 1 by Exercise 2.2.2* since its positive. This means $a = \pm 1$ and $b = 0$ or $a = 0$ and $b = \pm 1$, i.e. $a + bi \in \{1, -1, i, -i\}$. ■

Exercise 2.2.4*. Prove that an associate of a prime is also prime.

Solution

If p and q are associates, $p \mid \alpha$ if and only if $q \mid \alpha$. ■

Exercise 2.2.5*. Prove that the conjugate of a prime is also a prime.

Solution

$p \mid \eta$ iff $\overline{p} \mid \overline{\eta}$ so if $\overline{p} \mid \alpha\beta$ then $p \mid \overline{\alpha}\overline{\beta}$ which implies $p \mid \overline{\alpha}$ or $p \mid \overline{\alpha}$, i.e. $\overline{p} \mid \alpha$ or $\overline{p} \mid \beta$ as wanted. ■

Exercise 2.2.6*. Prove that primes are irreducible.

Solution

If $p = \alpha\beta$ is prime, then p must divide α or β, we may assume it divides α, i.e. $\alpha = p\gamma$. Then,

$$p = \alpha\beta = p\gamma\beta \implies \beta\gamma = 1$$

so β is a unit as wanted. ■

Exercise 2.2.7*. Let $d \neq 1$ be a squarefree rational integer and let $x \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ be a quadratic integer. Suppose that $|N(x)|$ is a rational prime. Prove x is irreducible.

Solution

If $x = \alpha\beta$ then $N(x) = N(\alpha)N(\beta)$ so if $N(x)$ is a rational prime then $N(\alpha)$ or $N(\beta)$ must be ± 1 by the uniqueness of the prime factorisation in $\mathbb{Z}$, i.e. one of them is a unit. ■

Exercise 2.2.8*. Suppose a prime p divides another prime q. Prove that p and q are associates.

Solution

Write $q = \alpha p$. Since q is irreducible by Exercise 2.2.6* and p is not a unit, α must be a unit. ■

Exercise 2.2.9*. Prove that p is a prime element of R if and only if it is non-zero and $R \pmod p$ is an integral domain (this means that the product of two non-zero elements is still non-zero). In particular, if $R \pmod p$ is a field (this means that elements which are not divisible by p have an inverse mod p), p is prime.

Solution

$\alpha\beta$ is divisible by p if and only if it is zero modulo p, so p is prime iff when $\alpha\beta$ is zero modulo p, α or β must already be zero modulo p. This is exactly what it means for $R \pmod p$ to be an integral domain. ■

Exercise 2.2.10. Let $d \neq 1$ be a squarefree rational integer and let $p \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ be a prime. Prove that p divides exactly one rational prime $q \in \mathbb{Z}$.

Solution

First we prove uniqueness. Suppose $p \mid q$ and $p \mid r$ for distinct rational primes q and r. By Bézout, let $aq + br = 1$ for some $a, b \in \mathbb{Z}$. Then $p \mid aq + br = 1$ which means that it's a unit and is a contradiction.

For existence, consider the prime factorisation $\pm q_1^{n_1} \cdot \ldots \cdot q_k^{n_k}$ of the norm $N(p)$ of p. Since $p \mid N(p)$, p must divide one of the q_i since it's prime. ■

Exercise 2.2.11. Prove that 2 is irreducible in $\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ but not prime.

Solution

First, note that 2 is not prime since $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$ but 2 divides neither of these factors. Now, suppose $2 = \alpha\beta$ and that neither of α and β are units. Then,

$$4 = N(2) = N(\alpha)N(\beta)$$

so $N(\alpha) = N(\beta) = \pm 2$ as they are different from ± 1. If we write $\alpha = a + b\sqrt{-5}$, we have $N(\alpha) = a^2 + 5b^2$ which cannot be equal to 2 and is thus a contradiction. ■

Exercise 2.2.12. Show that the primes of Definition 2.2.2 must all be prime elements, and that there is at least one associate of each prime element in that set. (Conversely, if we have unique factorisation, any such set of primes work. This explains why we consider all primes defined in Definition 2.2.3.)

Solution

Suppose p is a prime as in Definition 2.2.2 and $p \mid \alpha\beta$. Write $\alpha = up_1^{a_1} \cdot \ldots \cdot p_n^{a_n}$ and $\beta = vq_1^{b_1} \cdot \ldots \cdot q_m^{b_m}$ the prime factorisations of α and β. Then, by the uniqueness of the prime factorisation, p must be equal to some p_i or q_i times a unit w. In the first case, $p \mid p_i \mid \alpha$ and in the second case $p \mid q_i \mid \beta$.

Now suppose p is a prime as in Definition 2.2.3 and consider its prime factorisation $p_1^{a_1} \cdot \ldots \cdot p_n^{a_n}$. Then p must divide one of the p_i since it's prime, which means it is associate to it by Exercise 2.2.8*. ■

Exercise 2.2.13*. Prove that a greatest common divisor γ of α and β really is a greatest common divisor of α and β, in the sense that if $\gamma \mid \alpha, \beta$ and $\delta \mid \alpha, \beta$ then $\delta \mid \gamma$.

Solution

Since $\alpha, \beta \in \alpha R + \beta R$, we have $\alpha, \beta \in \gamma R$, i.e. $\gamma \mid \alpha, \beta$. Now suppose $\delta \mid \alpha, \beta$. Let x and y be such that $x\alpha + y\beta = \gamma$. Then,

$$\delta \mid x\alpha + y\beta = \gamma.$$

■

Exercise 2.2.14*. Prove that an associate greatest common divisor is also a greatest common divisor, and that the greatest common divisor of two elements is unique up to association.

Solution

If γ and δ are two gcds of α and β then, by Exercise 2.2.13*, $\gamma \mid \delta \mid \gamma$ so they are associates. ■

Exercise 2.2.15. Let R be a Euclidean domain with Euclidean function f. Show that, if $f(\alpha) = 0$, then $\alpha = 0$, and if $f()\alpha) = 1$, then α is a unit or zero.

Solution

If $\alpha \neq 0$, consider the Euclidean division of 0 by α: $0 = \rho\alpha + \tau$. Then $f(\tau) < f(\alpha) = 0$ which is impossible.

For the second part, suppose that α is non-zero and $f(\alpha) = 1$. Then, if we perform the Euclidean division of any β by α: $\beta = \alpha\rho + \tau$, we have $f(\tau) < f(\alpha) = 1$, i.e. $f(\tau) = 0$. By the first part, this means that $\tau = 0$. Hence, α divides everything, and in particular it divides 1, i.e. it is a unit. ■

Exercise 2.2.16*. Prove that a Euclidean domain is a Bézout domain.

Solution

Let R be a Euclidean domain with Euclidean function f. Let α, β be two elements of R. Consider a non-zero element $\gamma \in \alpha R + \beta R$ such that $f(\gamma)$ is minimal. We will show that $\alpha R + \beta R = \gamma R$. Suppose otherwise, that there is a $\delta \in \alpha R + \beta R$ such that the Euclidean division $\delta = \rho\gamma + \tau$ has τ non-zero (otherwise $\gamma \mid \delta$, i.e. $\delta \in \gamma R$). Then, $f(\tau) < f(\gamma)$ but $\tau \in \alpha R + \beta R$ and is non-zero too so that contradicts the minimality of γ. ■

Exercise 2.2.17*. Prove that irreducible elements are prime in a Bézout domain.

Solution

Let x be an irreducible element in a Bézout domain R. By Exercise 2.2.9*, it suffices to show that every $x \nmid \alpha$ has an inverse modulo p. Since R is a Bézout domain, there is some β such that

$$xR + \alpha R = \beta R.$$

In particular $\beta \mid x$ so β is a unit or a unit times x. The latter is not possible since β also divides α, thus β is unit. Without loss of generality, $\beta = 1$ by Exercise 2.2.14*. Since $\beta = ax + b\alpha$ for some $a, b \in R$ by definition, modulo x we have $b\alpha \equiv 1$ as wanted. ■

2.3 Gaussian Integers

Exercise 2.3.1*. Let $n \in \mathbb{Z}$ be a rational integer and p an odd rational prime. If $n^2 \equiv -1 \pmod{p}$, prove that $p \equiv 1 \pmod{4}$.

Solution

Suppose that $p \mid n^2 + 1$. Then the order of n modulo p is 4, indeed $n^4 \equiv (-1)^4 = 1$ so the order divides 4 and $n^2 \equiv -1 \not\equiv 1$ so the order is not divisible by 2. Since the order divides $p - 1$ by Fermat's little theorem (see Exercise 3.3.4*), we have $4 \mid p - 1$, i.e. $p \equiv 1 \pmod{4}$ as wanted. ■

Exercise 2.3.2*. Let $p \equiv 1 \pmod{4}$ be a rational prime. Prove that there exist a rational integer n such that $n^2 \equiv -1 \pmod{p}$. (Hint: Consider $(p-1)!$.)

Solution

By Wilson's theorem, $(p-1)! \equiv -1 \pmod{p}$. Hence,

$$\begin{aligned} -1 &\equiv (p-1)! \\ &= \prod_{k=1}^{\frac{p-1}{2}} k \cdot \prod_{k=1}^{\frac{p-1}{2}} p-k \\ &\equiv \prod_{k=1}^{\frac{p-1}{2}} k \prod_{k=1}^{\frac{p-1}{2}} -k \\ &= (-1)^{\frac{p-1}{2}} \left(\prod_{k=1}^{\frac{p-1}{2}} k \right)^2 \\ &\equiv \left(\prod_{k=1}^{\frac{p-1}{2}} k \right)^2 \end{aligned}$$

since $p \equiv 1 \pmod{4}$. ■

Exercise 2.3.3. Which rational integers can be written as a sum of two squares of rational integers?

Solution

Since the norm of $\mathbb{Z}[i]$ is multiplicative, if m and n are sums of two squares, then so are mn. In particular, all integers with only prime factors equal to 2 or congruent to 1 modulo 4 are sums of two squares. Also, perfect squares times these numbers are sums of two squares.

Now suppose that $n = a^2 + b^2$ is a sum of two squares but not of this form, i.e. there is some prime $p \equiv -1 \pmod{4}$ such that $v_p(n)$ is odd. If $p \nmid b$ then $p \mid (ab^{-1})^2 + 1$ which is impossible by Exercise 2.3.1*. Thus $p \mid a, b$. We can now proceed by infinite descente on $n/p^2 = (a/p)^2 + (b/p)^2$ (or equivalently suppose n was the minimal counterexample and reach a contradiction). ■

Exercise 2.3.4*. Find all rational integer solutions to the equation $x^2 + 1 = y^3$. (This is the example we considered in the beginning of the chapter.)

Solution

Note that any solution of $x^2 + 1 = y^3$ must have y odd since $x^2 + 1$ is congruent to 1 or 2 modulo 4. Thus, y is not divisible by $1 + i$. Write the equation as $(x + i)(x - i) = y^3$. The gcd of the two factors divide $(x + i) - (x - i) = 2i$ but is not divisible by $1 + i$ so is 1. This means that

$$x + i = u\alpha^3$$

for some unit u. Since the units of $\mathbb{Z}[i]$ are $1, -1, i, -i$ and they are all cubes $(1^3, (-1)^3, (-i)^3, i^3)$, we can assume $u = 1$. The rest of the solution is the same as in the introduction of the chapter. ■

2.4 Eisenstein Integers

Exercise 2.4.1*. Prove that the norm of $a+bj$ is a^2-ab+b^2. (Bonus: do it without any computations using cyclotomic polynomials from Chapter 3.)

Solution

$$(a+bj)(a+b\overline{j}) = a^2 + ab(j+\overline{j}) + bj\overline{j} = a^2 - ab + b^2$$

since $j + \overline{j} = -1$ and $j\overline{j} = 1$ by Vieta (j is a root of $X^2 + X + 1 = 0$). For the bonus, one can note that $N(a + bj) = \Phi_6(a, b)$ by Exercise 3.1.8*. ■

Exercise 2.4.2*. Determine the units of $\mathbb{Z}[j]$.

Solution

$a + bj$ is a unit if and only if $a^2 - ab + b^2 = \pm 1$. If $ab \leq 0$ we get $a = 0$ and $b = \pm 1$ as well as $a = \pm 1$ and $b = 0$, and if $ab > 0$ then $a^2 - ab + b^2 = (a - b)^2 + ab \geq 0^2 + 1$ which means $a = b = \pm 1$. In conclusion, the units of $\mathbb{Z}[j]$ are ± 1, $\pm j$ and $\pm(1 + j) = \pm j^2$. (Note that these are all roots of unity.) ■

Exercise 2.4.3*. Prove that $\mathbb{Z}[j]$ is norm-Euclidean.

Solution

Let $\alpha, \beta \in \mathbb{Z}[j]$ be two elements with $\beta \neq 0$. Write $\frac{\alpha}{\beta} = x + yj$ and let m and n be rational integers such that $|x - m| \leq \frac{1}{2}$ and $|y - n| \leq \frac{1}{2}$. Thus, $|N(x + yi - (m + ni))| \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1$.

Hence,

$$|N(\alpha - \beta(m + ni))| = |N(\beta)| \cdot |N(x + yi - (m + ni))| < |N(\beta)|$$

which means that the remainder $\tau = \alpha - \beta(m + ni)$ works since it has norm less than $N(\beta)$. ■

Exercise 2.4.4. Characterise the primes of $\mathbb{Z}[j]$. Conclude that when $p \equiv 1 \pmod 3$ there exist rational integers a and b such that $p = a^2 - ab + b^2$. (You may assume that there is an $x \in \mathbb{Z}$ such that $x^2 + x + 1 \equiv 0 \pmod p$ if $p \equiv 1 \pmod 3$. This will be proven in Chapter 3, as a corollary of Theorem 3.3.1.)

Solution

As in the $\mathbb{Z}[i]$ case, it suffices to find the prime factorisation of rational primes (this can also be seen as a corollary of prime divides exactly one rational prime). Indeed, if α is a prime of $\mathbb{Z}[j]$, then $N(\alpha) = \alpha\overline{\alpha}$ has at most two rational prime factors: if it has one then $N(\alpha)$ is prime in $\mathbb{Z}$. Otherwise, $N(\alpha) = \pm p^2$ α is an associate of a rational prime p.

Thus, suppose $N(\alpha) = p$ for some rational prime p ($N(\alpha)$ is positive). Write $\alpha = a + bj$. Then, $N(\alpha) = a^2 - ab + b^2$. Clearly, $p \nmid b$ as otherwise $p^2 \mid N(\alpha) = p$. Thus, $p \mid (-a \cdot b^{-1}) + (-a \cdot b^{-1}) + 1$.

We wish to find which rational primes divide a number of the form $x^2 + x + 1$. Note that $x^3 - 1 = (x + 1)(x^2 + x + 1)$ so $x^3 \equiv 1 \pmod p$. The order of x modulo p divides 3. If it is 1 then $x^2 + x + 1 \equiv 3$ so $p = 3$ which factorises as $(1 - j)(1 - \overline{j}) = -j^2(1 - j)^2$ (it ramifies).

Otherwise, the order must be 3. Since it divides $p - 1$, we have $p \equiv 1 \pmod 3$. In particular, primes congruent to -1 modulo 3 stay inert in $\mathbb{Z}[j]$. Finally, if $p \equiv 1 \pmod 3$, by Theorem 3.3.1, there exists an x such that $p \mid x^2 + x + 1 = (x - j)(x - j^2)$. Since $p \nmid x - j, x - j^2$, this means these primes split as a product of two Eisenstein primes $a + bj$ and $a - bj$. (In particular $p = a^2 - ab + b^2$.) ■

Exercise 2.4.5*. Let $\theta \in \mathbb{Z}[j]$ be an Eisenstein integer. Prove that, if $\lambda \nmid \theta$, then $\theta \equiv \pm 1 \pmod{\lambda}$. In that case, prove that we also have $\theta^3 \equiv \pm 1 \pmod{\lambda^4}$.

Solution

Modulo λ, every element of $\mathbb{Z}[j]$ is congruent to a rational integer. Indeed, $a + bj \equiv a + b \pmod{1 - j}$. Moreover, $\lambda \mid 3$ so every rational integer is congruent modulo λ to 0 or ± 1.

Let $\theta = \eta\lambda \pm 1$. We shall show that $\lambda^3 \frac{\theta^3 \mp 1}{\theta \mp 1} = \theta^2 \pm \theta + 1$. We have

$$\begin{aligned}
\theta^2 \pm \theta + 1 &= (\eta\lambda \pm 1)^2 \pm (\eta\lambda \pm 1) + 1 \\
&= \eta^2\lambda^2 \pm 2\eta\lambda + 1 \pm \eta\lambda + 1 + 1 \\
&= \eta^2\lambda^2 \pm 3\lambda\eta + 3 \\
&\equiv \eta^2\lambda^2 + 3 \pmod{\lambda^3} \\
&= \lambda^2(\eta^2 - j^2) \\
&= \lambda^2(\eta - j)(\eta + j)
\end{aligned}$$

since any $\lambda \nmid \eta$ is congruent to $j \equiv 1$ or $-j \equiv -1$ modulo λ. ■

Exercise 2.4.6*. Let $\alpha, \beta \in \mathbb{Z}[j]$ be coprime Eisenstein integers non-divisible by λ. Prove that, if

$$\lambda \mid \alpha^3 + \beta^3 = (\alpha + \beta)(\alpha + \beta j)(\alpha + \beta j^2),$$

each pair of factors has gcd λ.

Solution

Modulo λ, $j \equiv 1$ so all the factors are the same modulo λ and are thus all divisible by λ. If $\gamma \mid \alpha + \beta, \alpha + \beta j$ then $\gamma\beta(1 - j)$ which implies $\gamma \mid 1 - j = \lambda$ since it is coprime with β (it divides $\alpha + \beta$). By sysmmetry between j and j^2 (they are conjugate), we reach the same conclusion if $\gamma \mid \alpha + \beta, \alpha + \beta j^2$.

Finally, if $\gamma \mid \alpha + \beta j, \alpha + \beta j^2$ then $\gamma \mid \beta j(1 - j)$ but γ is coprime with β since it divides $\alpha + \beta j$ which implies $\gamma \mid 1 - j = \lambda$ again. ■

Exercise 2.4.7. Check the computational details: $\pm 1 \pm \mu \pm \eta$ is never zero mod λ^4 for units μ, η and $\pm 1 \pm \mu \equiv 0 \pmod{\lambda^3}$ implies $\mu = \pm 1$.

Solution

We have seen in Exercise 2.4.2* that the units of $\mathbb{Z}[j]$ are roots of unity. Thus, the norms of $\pm\varepsilon, \pm 2 \pm \varepsilon, \pm 1 \pm \mu$ have absolute value less than $3 \cdot 3$ by the triangular inequality (because the conjugates of roots of unity are still roots of unity and thus have absolute value 1). In particular, for it to be divisible by $N(\lambda^4) = 81$, it must be zero, i.e. $\pm\varepsilon = 0$, $\pm 2 \pm \varepsilon = 0$ and $\pm 1 \pm \mu = 0$. The first two cases are impossible, and the last one implies $\mu = \pm 1$ as wanted. ■

2.5 Hurwitz Integers

Exercise 2.5.1*. Prove that $\mathbf{ij} = \mathbf{k} = -\mathbf{ji}$, $\mathbf{jk} = \mathbf{i} = -\mathbf{kj}$ and $\mathbf{ki} = \mathbf{j} = -\mathbf{ik}$ follows from $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{ijk} = -1$ and associativity of the multiplication.

Solution

We have

1. $\mathbf{ij} = -\mathbf{ijkk} = \mathbf{k}$.
2. $\mathbf{kj} = \mathbf{ijj} = -\mathbf{i}$.
3. $\mathbf{jk} = -\mathbf{iijk} = \mathbf{i}$.
4. $\mathbf{ik} = \mathbf{jkk} = -\mathbf{j}$.
5. $\mathbf{ki} = -\mathbf{kkj} = \mathbf{j}$.
6. $\mathbf{ji} = \mathbf{kii} = -\mathbf{k}$.

■

Exercise 2.5.2. Prove that $\mathbf{i}, \mathbf{j}, \mathbf{k}$ are distinct.

Solution

Exercise 2.5.1* tells us that everything is cyclic between $\mathbf{i}, \mathbf{j}, \mathbf{k}$ so assume $\mathbf{i} = \mathbf{j}$. Then we get $k = \mathbf{ij} = \mathbf{i}^2 = -1$ and

$$-\mathbf{i} = \mathbf{ki} = \mathbf{j} = \mathbf{i}$$

so $\mathbf{i} = 0$ which is an obvious contradiction. ■

Exercise 2.5.3*. Let $\alpha, \beta, \gamma \in \mathbb{H}$ be quaternions. Prove that $(\alpha\beta)\gamma = \alpha(\beta\gamma)$. (We say multiplication is *associative*. This is why we can write $\alpha\beta\gamma$ without ambiguity.)

Solution

The simplest (and neatest) way to see this is to use the representation by matrices given by Remark 2.5.2, since multiplication of matrices is associative. Without matrices, but still with a bit of (implicit) linear algebra, we can do the following. We shall prove that $(xy)z = x(yz)$ for any $x, y, z \in \{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$. Since real numbers commute with everything and multiplication is clearly associative when one of the factor is real, we thus get $(xy)z = x(yz)$ for any x, y, z which are linear combinations with real coefficients of $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$, i.e. all quaternions (since if $(xy)z = x(yz)$ and $(wy)z = w(yz)$ then $((x + w)y)z = (x + w)(yz)$ too).

When one of x, y, z is 1 we trivially have $(xy)z = x(yz)$ by the previous remark (since 1 is real). Thus, suppose without loss of generality by cyclicity (Exercise 2.5.1*) that $x = \mathbf{i}$. We distinguish all possible cases.

1. $y = z = \mathbf{j}$. We have
$$(\mathbf{ij})\mathbf{j} = \mathbf{kj} = -\mathbf{i} = \mathbf{i}(\mathbf{jj}).$$
2. $y = z = \mathbf{k}$. We have
$$(\mathbf{ik})\mathbf{k} = -\mathbf{jk} = -\mathbf{i} = \mathbf{i}(\mathbf{kk}).$$
3. $y = \mathbf{j}$, $z = \mathbf{k}$. We have
$$(\mathbf{ij})\mathbf{k} = \mathbf{kk} = -1 = \mathbf{ii} = \mathbf{i}(\mathbf{jk}).$$
4. $y = \mathbf{k}$, $z = \mathbf{j}$. We have
$$(\mathbf{ik})\mathbf{j} = -\mathbf{jj} = 1 = -\mathbf{ii} = \mathbf{i}(\mathbf{kj}).$$

5. $y = \mathbf{i}$, $z = \mathbf{j}$. We have
$$(\mathbf{ii})\mathbf{j} = -\mathbf{j} = \mathbf{ik} = \mathbf{i}(\mathbf{ij}).$$
6. $y = \mathbf{i}$, $z = \mathbf{k}$. We have
$$(\mathbf{ii})\mathbf{k} = -\mathbf{k} = -\mathbf{ij} = \mathbf{i}(\mathbf{ik}).$$
7. $y = \mathbf{j}$, $z = \mathbf{i}$. We have
$$(\mathbf{ij})\mathbf{i} = \mathbf{ki} = -\mathbf{j} = \mathbf{ik} = \mathbf{i}(\mathbf{ji}).$$
8. $y = \mathbf{k}$, $z = \mathbf{i}$. We have
$$(\mathbf{ik})\mathbf{i} = -\mathbf{ji} = \mathbf{k} = \mathbf{ij} = \mathbf{i}(\mathbf{ki}).$$
9. $y = z = \mathbf{i}$. We trivially have
$$(\mathbf{ii})\mathbf{i} = \mathbf{i}(\mathbf{ii}).$$

■

Exercise 2.5.4. Prove that there are infinitely many square roots of -1 in $\mathbb{H}$.

Solution

We have
$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})^2 = (a^2 - b^2 - c^2 - d^2) + 2ab\mathbf{i} + 2ac\mathbf{j} + 2ad\mathbf{k}$$
because the other terms cancel out because of Exercise 2.5.1*, for instance $b\mathbf{i}c\mathbf{i} + c\mathbf{j}b\mathbf{i} = 0$. In particular, if $a = 0$, $(b\mathbf{i} + c\mathbf{j} + d\mathbf{k})^2 = -(b^2 + c^2 + d^2)$ and there are thus clearly infinitely many square roots of any negative number. ■

Exercise 2.5.5*. Prove that, for any $\alpha, \beta \in \mathbb{H}$, $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$ and $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$ (this is because multiplication is not commutative anymore).

Solution

It is clear that conjugation is additive:
$$(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) + (a' - b'\mathbf{i} - c'\mathbf{j} - d'\mathbf{k}) = (a + a') - (b + b')\mathbf{i} - (c + c)\mathbf{j} - (d + d')\mathbf{k}.$$
For multiplicativity, one can see that
$$\begin{aligned}(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) + (a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')\mathbf{i} \\ + (ac' + ca' + db' - bd')\mathbf{j} + (ad' + da' + bc' - cb')\mathbf{k}.\end{aligned}$$
If we exchange (a, b, c, d) with (a', b', c', d') and switch the signs of b, c, d, b', c', d' one can see that it is the same as taking the conjugate: both give
$$(aa' - bb' - cc' - dd') - (ab' + ba' + cd' - dc')\mathbf{i} - (ac' + ca' + db' - bd')\mathbf{j} - (ad' + da' + bc' - cb')\mathbf{k}$$
(a times something switches sign because a stays the same but the other factor switches sign, and $cd' - dc'$ switches sign too because $(c, d) \leftrightarrow (c', d')$). ■

Exercise 2.5.6*. Check that $(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k})$ is indeed $a^2 + b^2 + c^2 + d^2$.

Solution

$(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k})(a-\mathbf{i}-c\mathbf{j}-d\mathbf{k}) = a^2+b^2+c^2+d^2$ because the non-real terms cancel out because of Exercise 2.5.1*, for instance $b\mathbf{i}(-c\mathbf{j})+c\mathbf{j}(-b\mathbf{i}) = 0$. ■

Exercise 2.5.7*. Prove that $\mathbb{H}$ is a skew field. This amounts to checking that elements have multiplicative inverses (i.e. for any α there is a β such that $\alpha\beta = \beta\alpha = 1$).

Solution

This follows from Exercise 2.5.6*: the inverse of $a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$ is $\frac{a-b\mathbf{i}-c\mathbf{j}-d\mathbf{k}}{a^2+b^2+c^2+d^2}$. ■

Exercise 2.5.8*. Prove that the norm is multiplicative: for any $\alpha, \beta \in \mathbb{H}$, $N(\alpha\beta) = N(\alpha)N(\beta)$.

Solution

This follows from Exercise 2.5.5*:

$$N(\alpha\beta) = \alpha\beta\overline{\beta}\overline{\alpha} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$$

because real numbers commute with every quaternion and $\beta\overline{\beta}$ is a real number. ■

Exercise 2.5.9*. Prove that $H = \{\frac{a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}}{2} \mid a \equiv b \equiv c \equiv d \pmod 2\}$. Deduce that the elements of H have integral norms.

Solution

When you multiply two such elements you get back an element of the same form:.Indeed, it is clear when one of the factors is in $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$. For the same reason, we can consider a, b, c, d modulo 2. Thus, we just need to show that the product of two such elements with odd a, b, c, d still has this form, which is true for $\frac{1+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2} \cdot \frac{1-\mathbf{i}-\mathbf{j}-\mathbf{k}}{2} = 1$.

From this we conclude that H is included in this set. However it is also clear that H contains this set so they are equal. ■

Exercise 2.5.10*. Determine the units of H.

Solution

$\alpha = a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$ is a unit if and only if $a^2+b^2+c^2+d^2 = N(\alpha) = \pm 1$. This means

$$\alpha \in \left\{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}, \frac{1\pm\mathbf{i}\pm\mathbf{j}\pm\mathbf{k}}{2}\right\}.$$

Indeed, either a, b, c, d are all integers in which case one of them is ± 1 and the rest 0, or they are all half integers in which case they must all be $\frac{\pm 1}{2}$ as otherwise the sum is too big. ■

Exercise 2.5.11*. Let $\alpha, \beta, \gamma \in H$. Prove that $\alpha \lceil \beta$ implies $\alpha \lceil \beta\gamma$ but does not always imply $\alpha \lceil \gamma\beta$.

Solution

Suppose that $\alpha \lceil \beta$, i.e. $\beta = \alpha\delta$. Then $\beta\gamma = \alpha(\delta\gamma)$ so $\alpha \lceil \beta\gamma$ too.

For the second part, a very simple counter-example is $\alpha = \beta = 1 + \mathbf{i} + \mathbf{j}$ and $\gamma = \mathbf{i}$. Suppose that $\alpha \lceil \gamma\beta$. This means that there exists a $\delta \in H$ such that $\alpha\delta = \gamma\beta$, i.e.

$$(1 + \mathbf{i} + \mathbf{j})\delta = \mathbf{i}(1 + \mathbf{i} + \mathbf{j}).$$

In other words, 3 divides

$$(1 - \mathbf{i} - \mathbf{j})\mathbf{i}(1 + \mathbf{i} + \mathbf{j}).$$

However, this is equal to

$$(\mathbf{i} + 1 + \mathbf{k})(1 + \mathbf{i} + \mathbf{j}) = 1 + 2\mathbf{j} + 2\mathbf{k}$$

which is clearly not divisible by 3. ■

Exercise 2.5.12*. Prove that being left-associate is an *equivalence relation*, i.e., for any α, β, γ, α is a left-associate of itself, α is a left-associate of β if and only if β is a left-associate of α, and if α is a left-associate of β and β is a left associate of γ then α is a left-associate of γ.

Solution

We have $\alpha = \alpha \cdot 1$,

$$\alpha = \beta\varepsilon \iff \beta = \alpha\varepsilon^{-1},$$

and

$$\alpha = \beta\varepsilon, \beta = \gamma\eta \implies \alpha = \gamma\eta\varepsilon.$$

■

Exercise 2.5.13*. Prove that a left-gcd γ of α and β satisifies the following property: $\gamma \lceil \alpha, \beta$ and if $\delta \lceil \alpha, \beta$ then $\delta \lceil \gamma$.

Solution

Since $\alpha, \beta \in \gamma R$, we have $\gamma \lceil \alpha, \beta$. Write $\gamma = \alpha x + \beta y$. If $\delta \lceil \alpha, \beta$, then $\delta \lceil \alpha x + \beta y = \gamma$ by Exercise 2.5.11*. ■

Exercise 2.5.14. Prove that $1 + \mathbf{i}$ and $1 - \mathbf{j}$ do not have a left-gcd in $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$. In particular, it is not left-Bézout and thus not left-Euclidean too (and the same holds for being right-Bézout and right-Euclidean by symmetry).

Solution

Let $L = \mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$. Suppose otherwise and let γ be a left-gcd. Note that $1 + \mathbf{i}$ has norm 2 so γ must have norm 1 or 2. If it has norm 1, it is a unit so $(1 + \mathbf{i})L + (1 - \mathbf{j})L = \gamma L$. Let α and β be such that $(1 + \mathbf{i})\alpha + (1 - \mathbf{j})\beta = 1$. Then,

$$1 = (1+\mathbf{i})\alpha+(1-\mathbf{j})\beta = (1+\mathbf{i})\alpha+(1+bfi)(1/2-\mathbf{i}/2-\mathbf{j}/2+\mathbf{k}/2)\beta = (1+\mathbf{i})(\alpha+(1/2-\mathbf{i}/2-\mathbf{j}/2+\mathbf{k}/2)\beta)$$

which is impossible since the norm of the LHS is divisible by 2 since the second factor is a Hurwitz integer so has integral norm by Exercise 2.5.9*.

If γ has norm 2 (this is what happens in H), then, since γ left-divides $1 + \mathbf{i}$ and $1 - \mathbf{j}$ and has

the same norm as them it is a left-associate of them and thus $1+\mathbf{i}$ and $1-\mathbf{j}$ are left-associates too by Exercise 2.5.12*. This is a contradiction since the only units of L are $\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}$ by Exercise 2.5.10*. ■

Exercise 2.5.15*. Prove Proposition 2.5.1.

Solution

By symmetry, suppose R is a left-Euclid domain with Euclidean function f. Let $\gamma \in \alpha R + \beta R$ be a non-zero element such that $f(\gamma)$ is minimal. Suppose for the sake of a contradiction that $\alpha \notin \gamma R$. Write $\alpha = \gamma\rho + \tau$ for some non-zero τ with $f(\tau) < f(\gamma)$. This contradicts the minimality of $f(\gamma)$ since $\tau \in \alpha R + \beta R$ too. Thus $\alpha \in \gamma R$ and by symmetry β too. ■

Exercise 2.5.16*. Prove Proposition 2.5.3.

Solution

We proceed by induction on $N(\alpha)$, the base case is the units. If α is irreducible it is its own factorisation, otherwise write $\alpha = \beta\gamma$ with $N(\beta), N(\gamma) > 1$. Then $N(\beta), N(\gamma) < N(\alpha)$ so they can be written as a product of irreducible elements and thus α too. ■

Exercise 2.5.17. Prove that there is an irreducible Hurwitz integer $x \in H$ for which there exist α and β such that $x \mid \alpha\beta$ but x left-divides neither α nor β.

Solution

$1+\mathbf{i}$ has norm 2 which is a rational prime so is irreducible. In addition, $1+\mathbf{i} \mid 2 = (1+\mathbf{j})(1-\mathbf{j})$ but $1+\mathbf{i}$ left-divides neither of $1+\mathbf{j}$ and $1-\mathbf{j}$. Indeed, if it did, then there would be a unit η such that $1+\mathbf{j} = (1+\mathbf{i})\eta$ since they have the same norm. However, one can see that none of the

$$\eta \in \left\{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}, \frac{1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k}}{2}\right\}$$

work since there are always two non-zero coefficients of $\mathbf{i}, \mathbf{j}, \mathbf{k}$ except when the unit is ± 1 or $\pm\mathbf{j}$ (which do not work). ■

Exercise 2.5.18*. Let p be a rational prime. Prove that there exist rational integers a and b such that $p \mid 1 + a^2 + b^2$.

Solution

$1 + a^2$ and $-b^2$ both reach $\frac{p+1}{2}$ values modulo p so cannot be disjoint since $\mathbb{F}_p$ only has $p < \frac{p+1}{2} + \frac{p+1}{2}$ elements. ■

2.6 Exercises

Diophantine Equations

Exercise 2.6.2†. Prove that $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ and $\mathcal{O}_{\mathbb{Q}(\sqrt{-2})}$ are Euclidean.

Solution

We proceed exactly as in Proposition 2.3.1. Let $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{\pm 2})} = \mathbb{Z}[\sqrt{\pm 2}]$ be algebraic integers, with $\beta \neq 0$. Write $\alpha/\beta = x + y\sqrt{\pm 2}$. Choose rational integers m, n such that $|x-m|, |y-m| \leq \frac{1}{2}$. Then,

$$|N((x + y\sqrt{\pm 2}) - (m + n\sqrt{\pm 2}))| \leq \left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2 = \frac{3}{4} < 1$$

so that $\tau = \beta - (m + n\sqrt{-2})$ works as the remainder of the Euclidean division of α by β since it has norm less than $|N(\beta)|$. ■

Exercise 2.6.4†. Prove that $\mathcal{O}_{\mathbb{Q}(\sqrt{-7})}$ is Euclidean.

Solution

Let $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{-7})} = \mathbb{Z}\left(\frac{1+\sqrt{-7}}{2}\right)$ be quadratic integers with $\beta \neq 0$. Write $\frac{\alpha}{\beta} = x + y\sqrt{-7}$ with $x, y \in \mathbb{Q}$. Pick a half-integer n such that $|y - m| \leq \frac{1}{4}$, and a half integer $m \equiv n \pmod 1$ such that $|x - n| \leq \frac{1}{2}$. Then,

$$|N((x - m) + (y - n)\sqrt{-7})| \leq \left(\frac{1}{2}\right)^2 + 7\left(\frac{1}{4}\right)^2 = \frac{11}{16} < 1.$$

Thus, the remainder $\tau = \beta(((x - m) + (y - n)\sqrt{-7})$ works since it has norm less than $|N(\beta)|$ by the previous computation and $\alpha = \beta(m + n\sqrt{-7}) + \tau$. ■

Exercise 2.6.6†. Solve the equation $x^2 + 11 = y^3$ over $\mathbb{Z}$.

Solution

First, we prove that $\mathbb{Q}(\sqrt{-11})$ is norm-Euclidean. Let $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{-11})} = \mathbb{Z}\left(\frac{1+\sqrt{-11}}{2}\right)$ be quadratic integers with $\beta \neq 0$. Write $\frac{\alpha}{\beta} = x + y\sqrt{-11}$ with $x, y \in \mathbb{Q}$. Pick a half-integer n such that $|y - m| \leq \frac{1}{4}$, and a half integer $m \equiv n \pmod 1$ such that $|x - n| \leq \frac{1}{2}$. Then,

$$|N((x - m) + (y - n)\sqrt{-11})| \leq \left(\frac{1}{2}\right)^2 + 11\left(\frac{1}{4}\right)^2 = \frac{15}{16} < 1.$$

Thus, the remainder $\tau = \beta(((x - m) + (y - n)\sqrt{-11})$ works since it has norm less than $|N(\beta)|$ by the previous computation and $\alpha = \beta(m + n\sqrt{-11}) + \tau$.

We conclude that $\mathbb{Q}(\sqrt{-11})$ is Euclidean and thus a UFD. It is easy to check that 2 stays prime in $\mathbb{Q}(\sqrt{-11})$. Rewrite the equation $x^2 + 11 = y^3$ as $(x + \sqrt{-11})(x - \sqrt{-11}) = y^3$. Note that, if y is even, then

$$2 \mid \frac{x + \sqrt{-11}}{2} \cdot \frac{x - \sqrt{-11}}{2}$$

which is impossible since 2 is prime and divides neither of these factors. Thus, y is odd, which means that x is even. Let δ be the gcd of $x + \sqrt{-11}$ and $x - \sqrt{-11}$. Since $\delta \mid 2\sqrt{-11}$ and $2x$, we get $\delta = 1$ as $2 \nmid x + \sqrt{-11}$ and $\sqrt{-11} \nmid x + \sqrt{-11}$ (otherwise $11 \mid x, y$ which gives a contradiction modulo 11^2) and $\sqrt{-11}$ is prime (it has prime norm).

We conclude that, since $\mathbb{Q}(\sqrt{-11})$ is a UFD, we have

$$x + \sqrt{-11} = \varepsilon\left(\frac{a + b\sqrt{-11}}{2}\right)^3$$

for some rational integers $a \equiv b \pmod 2$ and ε a unit. Since the units of $\mathbb{Q}(\sqrt{-11})$ are just ± 1 (see Section 7.1), ε is also a cube so we may assume $\varepsilon = 1$.

To conclude, by looking at the real and imaginary parts, we get $8x = a(a^2 - 33b^2)$ and $8 = b(3a^2 - 11b^2)$. Hence, $b \mid 8$.

- If $b = \pm 1$, we get $3a^2 - 11 = \pm 8$, i.e. $b = 1$ and $a = \pm 1$. This yields $(x, y) = (\pm 4, 3)$.
- If $b \equiv \pm 2$, we have $3a^2 - 44 = \pm 4$, i.e. $b = 2$ and $a = \pm 4$. This yields $(x, y) = (\pm 58, 15)$.
- If $4 \mid b$, then, since $a \equiv b \pmod 2$, we get $16 \mid b(3a^2 - 11b^2) = 8$ which is impossible.

■

Exercise 2.6.8†. Let n be a non-negative rational integer. In how many ways can n be written as a sum of two squares of rational integers? (Two ways are considered different if the ordering is different, for instance $2 = 1^2 + (-1)^2$ and $2 = (-1)^2 + 1^2$ are different.)

Solution

Let $n \geq 1$ be an integer. We wish to count in how many ways it is the sum of two squares. First we do the case where $n = \prod_{i=1}^{k} p_i$ is squarefree and all its prime factors are 1 modulo 4. Then, $n = \prod_{i=1}^{k} \pi_i \overline{\pi}_i$ is a product of k Gaussian primes and their conjugate. Expressing it as a sum of two squares is equivalent to writing it as a product of two conjugate Gaussian integer $n = \alpha\overline{\alpha}$, which is equivalent to picking one out of π_i and $\overline{\pi}_i$ for each i and putting it in α. Thus, n is a sum of two squares in 2^k different ways, which turns out to be its number of divisors.

Now, suppose $n = \prod_{i=1}^{k} p_i^{n_i}$ where the p_i are distinct and 1 modulo 4 again. The same approach as before works, except we need to be more careful with where we put repeated prime factors. For instance, for $n = p^2$, $\alpha = \pi\overline{\pi}$ and $\alpha = \overline{\pi}\pi$ are in fact the same. Here is how we do it: we distribute some amount of π_i to α, say π_i^j, and fill the rest with $\overline{\pi}_i^{n_i - j}$. There are $n_i + 1$ ways to do this, so in total n is a sum of two squares in

$$(n_1 + 1) \cdot \ldots \cdot (n_k + 1)$$

ways, which turns out to be again the number of divisors of n.

Finally, we treat the general case, i.e. $n = 2^r \prod_{i=1}^{k} p_i^{n_i} \prod_{i=1}^{\ell} q_i^{2m_i}$, where p_i are distinct primes congruent to 1 modulo 4 and q_i distinct primes congruent to -1 modulo 4 (any sum of two squares has this form by Exercise 2.3.3). Notice that the dyadic valuation of n doesn't change the number of ways to represent it as a sum of two squares, since $2 = -i(1 + i)^2$ so we need to distribute the same prime to α and $\overline{\alpha}$. Thus we may assume $r = 0$. Then, notice that since all q_i are -1 modulo 4, if $n = a^2 + b^2$ then

$$\frac{n}{\prod_{i=1}^{\ell} q_i^{2m_i}} = \left(\frac{a}{\prod_{i=1}^{\ell} q_i^{m_i}}\right)^2 + \left(\frac{a}{\prod_{i=1}^{\ell} q_i^{m_i}}\right)^2$$

so that the numbers of way to represent n as a sum of two squares is the same as the number of ways to represent $\prod_{i=1}^{k} p_i^{n_i}$ as a sum of two squares, i.e. $(n_1 + 1) \cdot \ldots \cdot (n_k + 1)$. Finally, we may in fact summarise all of the above discussion as follows: the number of ways to represent n as a sum of two squares is

$$\sum_{d \mid n} \chi_4(d) = d_1(n) - d_{-1}(n),$$

where $\chi_4(d)$ is 1 if $d \equiv 1 \pmod 4$, -1 if $d \equiv -1 \pmod 4$ and 0 otherwise, d_1 is the number of (positive) divisors congruent to 1 modulo 4, and d_{-1} the number of (positive) divisors congruent to -1 modulo 4. ■

Remark 2.6.1

In fact, the fact that the number of representations as a sum of two squares of n is $\sum_{d|n}\chi_4(d)$ is not at all a coincidence. Let $r_2(n)$ denote the way of representing n as a sum of two squares (of positive rational integers), and s a formal object we will specify later. Then,

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{r_2(n)}{n^s} &= \sum_{a,b\geq 0,(a,b)\neq(0,0)}\frac{1}{(a^2+b^2)^s}\\ &= \sum_{x\neq 0,\Re(x),\Im(x)\geq 0}\frac{1}{N(x)^s}\\ &= \left(\sum_{k=0}^{\infty}\frac{1}{N(1+i)^{ks}}\right)\prod_{p\equiv -1 \pmod 4}\left(\sum_{k=0}^{\infty}\frac{1}{N(p)^{ks}}\right)\\ &\prod_{p\equiv 1 \pmod 4}\left(\sum_{k=0}^{\infty}\frac{1}{N(\pi)^{ks}}\right)\left(\sum_{k=0}^{\infty}\frac{1}{N(\overline{\pi})^{ks}}\right)\\ &= \left(\sum_{k=0}^{\infty}\frac{1}{2^{ks}}\right)\prod_{p\equiv 1 \pmod 4}\left(\sum_{k=0}^{\infty}\frac{1}{p^{ks}}\right)^2\prod_{p\equiv -1 \pmod 4}\left(\sum_{k=0}^{\infty}\frac{1}{p^{2ks}}\right)\\ &= \frac{1}{1-2^{-s}}\prod_{p\equiv 1 \pmod 4}\frac{1}{(1-p^{-s})^2}\prod_{p\equiv -1 \pmod 4}\frac{1}{(1-p^{-2s})}\end{aligned}$$

by uniqueness of the prime factorisation in $\mathbb{Z}[i]$ (we take the sum of $\frac{1}{N(x)}$ over all Gaussian integers except we only choose one associate for each integer, and the product is also taken over all Gaussian primes but with onlyassociate for each prime). This function is called the *Dedekind zeta function* $\zeta_{\mathbb{Q}(i)}$ of $\mathbb{Q}(i)$. Now consider the *Dirichlet L-function of* χ

$$L(s,\chi) := \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}.$$

We claim that $\zeta_{\mathbb{Q}(i)}(s) = \zeta(s)L(s,\chi)$, where ζ is the usual Riemann function $\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$. This is easy: by similar manipulations as before, we have $\zeta(s) = \prod_p \frac{1}{1-p^{-s}}$ and

$$L(s,\chi) = \prod_p \frac{1}{1-\xi(p)p^{-s}} = \prod_{p\equiv 1 \pmod 4}\frac{1}{1-p^{-s}}\prod_{p\equiv -1 \pmod 4}\frac{1}{1+p^{-s}}$$

and thus $\zeta(s)L(s,\chi) = \zeta_{\mathbb{Q}(i)}(s)$ (since $1+p^{-2s} = (1-p^{-s})(1+p^{-s})$). Finally, by regular expansion, we have

$$\zeta(s)L(s,\chi) = \sum_{n\geq 1}\frac{\sum_{d|n}\chi(d)}{n^s}.$$

Since $\zeta_{\mathbb{Q}(i)} = \sum_{n\geq 1}\frac{r_2(n)}{n^s}$, we get the wanted expression for $r_2(n)$ (we do not neeed complex analysis as the above manipulations were purely formal). This solution might seem a lot more complicated than the previous, but it is in fact a lot deeper as this product formula can be generalised to any Galois extension of number fields.

Exercise 2.6.11† (Euler)**.** Let $n \geq 3$ be an integer. Prove that there exist unique positive **odd** rational integers x and y such that $2^n = x^2 + 7y^2$.

Solution

Rewrite this as

$$\frac{x+y\sqrt{-7}}{2}\cdot\frac{x-y\sqrt{-7}}{2}=2^{n-2}.$$

Thus, solving $x^2+7y^2=2^n$ in odd integers amounts to writing 2^n as a product of conjugate odd factors in $\mathbb{Q}(\sqrt{-7})$. We have seen in Exercise 2.6.4† that $\mathbb{Q}(\sqrt{-7})$ is Euclidean, thus we seek the prime factorisation of 2. Since $\frac{1\pm\sqrt{-7}}{2}$ have norm 2 which is a rational prime, the prime factorisation of 2 reads

$$2=\frac{1+\sqrt{-7}}{2}\cdot\frac{1-\sqrt{-7}}{2}=\alpha\beta.$$

Now, write $\frac{x+y\sqrt{-7}}{2}=\alpha^i\beta^j$ with $i+j=n-2$. Since it is not divisible by $2=\alpha\beta$, we have $i=0$ or $j=0$, and which one it is depends on the sign of its $\sqrt{-7}$ part. This shows that there is exactly one pair which works. Indeed, it is also clear that they work since they will have the same parity and thus be both odd as $\alpha^2=\frac{-3+\sqrt{-7}}{2}\equiv\alpha \pmod 2$. ■

Exercise 2.6.12† (Fermat's Last Theorem for $n=4$)**.** Show that the equations $\alpha^4+\beta^4=\gamma^2$ and $\alpha^4-\beta^4=\gamma^2$ have no non-zero solution $\alpha,\beta,\gamma\in\mathbb{Z}[i]$.

Solution

Surprisingly, our solution is very similar to the proof of Theorem 2.4.1. Set $\lambda=1-i$. Any fourth power θ^4 which isn't disivible by λ is congruent to ±1 modulo λ^6: θ is congruent to 1 or i modulo 2, so θ^2 is congruent to ±1 modulo 4, which implies that $\theta^4\equiv1 \pmod 8$ as wanted. Another way to see this is to notice that two factors are of $\theta^4-1=(\theta-1)(\theta+1)(\theta-i)(\theta+i)$ are divisible by λ^2 and the other two by λ.

Now suppose for the sake of a contradiction that $\alpha,\beta,\gamma\in\mathbb{Z}[i]$ are pairwise coprime and non-zero such that $\alpha^4+\beta^4=\gamma^2$. If λ does not divide α nor β, then, the equation becomes $1+1\equiv\gamma^2$ modulo λ^6 by our first remark. In particular, $v_\lambda(\gamma)=1$; set $\gamma=\lambda\delta$. Then, $\lambda^2\delta^2\equiv2=i\lambda^2 \pmod{\lambda^6}$ so $\delta^2\equiv i \pmod{\lambda^4}$ which contradicts our previous observation: $\delta^4\equiv-1\not\equiv1 \pmod{\lambda^6}$.

Hence, λ must divide $\alpha\beta$, say it divides α. We will now, as we did in Theorem 2.4.1, that the more general equation

$$\varepsilon\lambda^{4n}\alpha^4+\beta^4=\gamma^2$$

does not have solutions $\lambda\nmid\alpha,\beta,\gamma\in\mathbb{Z}[i]$ and $\varepsilon\in\mathbb{Z}[i]^\times$ a unit for $n\geq1$. Hence, suppose that $\alpha,\beta,\gamma,\varepsilon$ is a solution with minimal n. We first prove that n must be at least 2. If there were a solution with $n=1$, modulo λ^4 we get $\beta^4\equiv1\equiv\gamma^2$. We will prove that γ^2 is in fact congruent to 1 modulo λ^5, whence $\lambda^5\mid\lambda^{4n}$ which implies $n\geq2$. To prove this notice that γ cannot be congruent to i modulo λ^2 so must be congruent to 1. Set $\gamma=\lambda^2\rho+1$ and notice that

$$\begin{aligned}\gamma^2-1&=(\gamma-1)(\gamma+1)\\ \lambda^2\mu(\lambda^2\rho+2)&\\ &=\lambda^4\rho(\rho+i)\end{aligned}$$

is divisible by λ^5 since one of ρ and $\rho+i$ must be divisible by λ.

Hence, $n\geq2$. We have

$$\varepsilon\lambda^{4n}\alpha^4=(\gamma-\beta^2)(\gamma+\beta^2).$$

We can see that both factors are congruent modulo 2 and that their gcd divides 2, which means that

$$\begin{cases}\gamma\pm\beta^2 & =u\lambda^2x^4\\ \gamma\mp\beta^2=v\lambda^{4n-2}y^4 & \end{cases}$$

for some units u, v and Gaussian integers $\lambda \nmid x, y$. Subtracting the two lines yields the equation

$$2\beta^2 = u\lambda^2 x^4 + v\lambda^{4n-2} y^4,$$

i.e.

$$\mu x^4 + \eta\lambda^{4(n-1)} y^4 = \beta^2$$

where $\mu = -iu$ and $\eta = -iv$ are units. It only remains to prove that $\mu = \pm 1$ to conclude that we have found a solution to the equation corresponding to $n - 1 \geq 1$, thus contradicting its minimality. Indeed, if $\mu = -1$ we get the equation

$$x^4 - \eta\lambda^{4(n-1)} y^4 = (\beta i)^2.$$

For this, consider our equation modulo λ^4 to get $\mu \equiv \pm 1$ as wanted.

We now consider the equation $\alpha^4 - \beta^4 = \gamma^2$. Suppose that (α, β, γ) is a non-zero solution of coprime Gaussian integers. Without loss of generality, suppose as well that $\lambda \nmid \alpha$: if $\lambda \mid \alpha$ then $\lambda \nmid \beta$ and $(\beta, \alpha, i\gamma)$ is a solution. Note that we can assume without we are already done when $\lambda \mid \beta$ because we solved the more general equation

$$\alpha^4 + \varepsilon\lambda^{4n}\beta^4 = \gamma^2.$$

where ε is a unit and $\lambda \geq 1$. Hence, it remains to settle the case where $\lambda \nmid \alpha, \beta$. In that case, rewrite the equation as $\beta^4 = (\alpha^2 - \gamma)(\alpha^2 + \gamma)$. The two factors are coprime since $\lambda \nmid \beta$ so

$$\alpha^2 \pm \gamma = \varepsilon_\pm \delta_\pm^4$$

for some units $\varepsilon_\pm \in \mathbb{Z}[i]$ and Gaussian integers $\lambda \nmid \delta_\pm$. This then yields

$$\varepsilon_- + \delta_-^4 + \varepsilon_+ \delta_+^4 = 2\alpha^2.$$

Modulo λ^2, we get $\varepsilon_- + \varepsilon_+ \equiv 0$. It is easy to see that this implies $\varepsilon_- + \varepsilon_+ = 0$. But then, since we know fourth powers are congruent to 1 modulo λ^6, we get

$$\lambda^6 \mid \varepsilon_- + \delta_-^4 + \varepsilon_+ \delta_+^4 = 2\alpha^2$$

which implies $\lambda \mid \alpha$ and is a contradiction. ■

Exercise 2.6.14†. Prove that $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ is Euclidean.

Solution

Let $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$ be quadratic integers with $\beta \neq 0$. Write $\frac{\alpha}{\beta} = x + y\sqrt{5}$ with $x, y \in \mathbb{Q}$. Pick a half-integer n such that $|y - m| \leq \frac{1}{4}$, and a half integer $m \equiv n \pmod 1$ such that $|x - n| \leq \frac{1}{2}$. Then,

$$|N((x-m) + (y-n)\sqrt{5})| \leq \left(\frac{1}{2}\right)^2 + 5\left(\frac{1}{4}\right)^2 = \frac{9}{16} < 1.$$

Thus, the remainder $\tau = \beta(((x-m) + (y-n)\sqrt{5})$ works since it has norm less than $|N(\beta)|$ by the previous computation and $\alpha = \beta(m + n\sqrt{5}) + \tau$. ■

Hurwitz Integers and Jacobi's Four Square Theorem

Exercise 2.6.15†. Let $\alpha \in H$ be a *primitive* Hurwitz integer, meaning that there does not exist a non-zero $m \in \mathbb{Z}$ such that $\frac{\alpha}{m} \in H$ and let $N(\alpha) = p_1 \cdot \ldots \cdot p_n$ be its prime factorisation. Then, the

factorisation of $\alpha = \pi_1 \cdot \ldots \cdot \pi_n$ for irreducible elements π_i of norm p_i is unique up to *unit-migration*, meaning that if if $\tau_1 \cdot \ldots \cdot \tau_k$ is another such factorisation, then $k = n$ and

$$\begin{cases} \tau_1 & = \pi_1 u_1 \\ \tau_2 & = u_1^{-1} \pi_2 u_2 \\ \ldots & \\ \tau_{n-1} & = u_{n-1}^{-1} \pi_n u_n \\ \tau_n & = u_n^{-1} \pi_n. \end{cases}$$

for some units $u_1, \ldots, u_n$. Deduce that α is irreducible if and only if its norm is a rational prime.

Solution

Let α be a primitive Hurwitz integer. We shall construct its factorisation in irreducible step by step, proving at the same time its uniqueness. We proceed inductively on n. Consider the right-gcd π_1 of p_1 and α, i.e. π_1 such that $p_1 H + \alpha H = \pi_1 H$. This is unique up to multiplication on the right by a unit. Note that this must necessarily be the π_1 we're looking for: if $\alpha = \pi_1' \cdot \ldots \cdot \pi_n'$ and $N(\pi_1') = p_1$, π_1' divides both α and p_1, and, by looking at the norm, must be the right-gcd of p_1 and α. Indeed, if the right-gcd were $\delta = \pi_1' \rho'$ it would have norm p_1^2 since $N(\rho) \mid N(p_1/\pi_1') = p_1$. But then, $\rho \sim p$ so the right-gcd is p which is impossible since $p \nmid \alpha$.

Now, let's prove that this π_1 indeed has norm p. By construction, $\pi_1 \rceil p_1, \alpha$ so there exist ρ and β such that $p_1 = \pi_1 \rho$ and $\alpha = \pi_1 \beta$. In particular, $N(\pi_1) \mid N(p_1) = p_1^2$. We have already proved that there was a problem if $N(\pi_1) = p_1^2$: in that case $p \sim \pi_1$ divides α. It remains to settle the case where $N(\pi_1) = 1$. This would mean that $p_1 H + \alpha H = H$, which is impossible since any element in the LHS has norm divisible by p_0:

$$\begin{aligned} N(p_1 u + \alpha v) &= (p_1 u + \alpha v)(p_1 \overline{u} + \overline{v\alpha}) \\ &\equiv \alpha v \overline{v\alpha} \pmod{p} \\ &= N(\alpha) N(v) \\ &\equiv 0. \end{aligned}$$

Finally, suppose now that α is irreducible. It is then clearly primitive, since we have shown that rational integers were reducible. Factorise its norm as a product of rational primes $p_1 \cdot \ldots \cdot p_k$ and factorise α has $\pi_1 \cdot \ldots \cdot \pi_k$ for irreducible elements π_i of norm p_i. Since α is irreducible, we must have $k = 1$, i.e. its norm $N(\alpha) = p_1$ is prime. ■

Exercise 2.6.16†. Prove that $(1 + \mathbf{i})H = H(1 + \mathbf{i})$[1]. Set $\omega = \frac{1+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}$. We say a Hurwitz integer $\alpha \in H$ is *primary* if it is congruent to 1 or $1 + 2\omega$ modulo $2 + 2\mathbf{i}$.[2] Prove that, for any Hurwitz integer α of odd norm, exactly one of its right-associates is primary.

Solution

As said in the footnote, $1+\mathbf{i}$ and its conjugate $1-\mathbf{i} = -\mathbf{i}(1+\mathbf{i})$ are associates. As a consequence, $1 + \mathbf{i}$ right-divides α if and only if it left-divides $\overline{\alpha}$. In particular, the left and right multiples of $1 + \mathbf{i}$ are the same.

For the second part, note that any Hurwitz integer α can be written in the form $a\omega + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. Modulo 2, α is congruent to 1, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$, or ω. In particular, there is a unit ε such that $\varepsilon\alpha \equiv 1$

[1] This means that we can manipulate congruences modulo $1 + \mathbf{i}$ normally. Note that the choice of $\mathbf{i}$ is not arbitrary at all, since $1 - \mathbf{i} = -\mathbf{i}(1 + \mathbf{i})$ and $1 - \mathbf{j} = (1 - \omega)(1 + \mathbf{i})$ are associates. By $\alpha \equiv \beta \pmod{\gamma}$, we mean that γ divides $\alpha - \beta$ from the left and from the right.

[2] Note that a primary Hurwitz integer is always in $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$.

(mod 2), and this unit is unique up to sign. Then, any Hurwitz integer congruent to 1 modulo 2 is congruent to ± 1 or $\pm(1+2\omega)$ modulo $2+2\mathbf{i}$, so this determines the sign of ε. ■

Exercise 2.6.17†. Let $m \in \mathbb{Z}$ be an odd integer. Prove that the Hurwitz integers modulo m, H/mH, are isomorphic to the algebra of two by two matrices modulo m, $(\mathbb{Z}/m\mathbb{Z})^{2\times 2}$. In addition, prove that the determinant of the image is the norm of the quaternion.

Solution

We shall copy Remark 2.5.2. Our goal is to find matrices with coefficients in $\mathbb{Z}/m\mathbb{Z}$ which square to $-I_2$. We are now going to do something very abusive: we shall define 1 for $I_2 = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, $\mathbf{i}$ for $\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$, $\mathbf{j}$ for $\begin{bmatrix}0 & i\\ i & 0\end{bmatrix}$ and $\mathbf{k}$ for $\begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix}$. Then, we will consider the matrix with integral coefficients $a+b\mathbf{i}+ci\mathbf{j}+di\mathbf{k}$ for $a,b,c,d \in \mathbb{Z}$, where i is the complex number. When we square this, we get

$$a^2 - b^2 + c^2 + d^2 + 2ab\mathbf{i} + 2iac\mathbf{j} + 2iad\mathbf{k},$$

as seen in Exercise 2.5.4. Since we want something linearly independent with 1 and $\mathbf{i}$, we shall assume that $a = b = 0$. Then, if $c = u$ and $d = v$ are such that $u^2 + v^2 \equiv -1 \pmod m$, the matrix

$$\mathbf{j}' := ui\mathbf{j} + vi\mathbf{k} = \begin{bmatrix}-v & -u\\ -u & v\end{bmatrix}$$

squares to -1 modulo m. We still need to find another matrix $\mathbf{k}'$ which squares to -1, and satisfies $\mathbf{i}\mathbf{j}'\mathbf{k}' = -1$, i.e.

$$\mathbf{k}' = -\mathbf{i}\mathbf{j}' = -\mathbf{i}(ui\mathbf{j} + vi\mathbf{k}) = -ui\mathbf{k} + vi\mathbf{j}.$$

Clearly, this also squares to -1. It remains to prove the existence of such u, v. When $m = p$ is prime, this is Exercise 2.5.18*. In fact, our solution to this exercise also works when $m = p^k$ is a prime power: there are $\frac{p^k+1}{2}$ squares since

$$x^2 \equiv y^2 \iff (x+y)(x-y) \equiv 0 \iff x \equiv \pm y$$

since the two factors are coprime so p^k must divide one of them. Thus, there are $\frac{p^k+1}{2}$ elements of the form v^2+1 and $\frac{p^k+1}{2}$ of the form $-u^2$, so two must be equal as wanted. When m is composite, the existence of such u, v follows from the Chinese remainder theorem.

To conclude, we have proven that there exists u, v such that $u^2+v^2 \equiv -1 \pmod m$ and used them to construct an isomorphism from H/mH to $(\mathbb{Z}/m\mathbb{Z})^{2\times 2}$. Explicitely (for the reader which wasn't convinced by our perfectly valid manipulations with very abusive notation), this isomorphism is given by

$$\varphi : a + \mathbf{i} + c\mathbf{j} + d\mathbf{k} \mapsto \begin{bmatrix}a+di & b+ci\\ -b+ci & a-di\end{bmatrix} = a\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} + b\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix} + c\begin{bmatrix}-v & -u\\ -u & v\end{bmatrix} + d\begin{bmatrix}u & -v\\ -v & -u\end{bmatrix}.$$

Actually, so far we have only shown that it is a morphism, but we will prove at the end that it is injective and thus an isomorphism since $|H/mH| = \left|(\mathbb{Z}/m\mathbb{Z})^{2\times 2}\right|$.

Note that $\varphi(\overline{\alpha})$ is the adjugate of $\varphi(\alpha)$, so their product is

$$\begin{aligned} N(\alpha)I_2 &= \varphi(\alpha\overline{\alpha}) \\ &= \varphi(\alpha)\operatorname{adj}\varphi\alpha \\ &= \det(\varphi(\alpha))I_2 \end{aligned}$$

by Proposition C.3.7. Indeed, as we saw in the beginning of Section C.3, the adjugate of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. Since this is additive, it suffices to check that

$$\begin{aligned} \varphi(1) &= \varphi(1) \\ \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} &= \varphi(-\mathbf{i}) = \operatorname{adj}\varphi(\mathbf{i}) \\ \begin{bmatrix} v & u \\ u & -v \end{bmatrix} &= \varphi(-\mathbf{j}) = \operatorname{adj}\varphi(\mathbf{j}) \\ \begin{bmatrix} -u & v \\ v & u \end{bmatrix} &= \varphi(-\mathbf{k}) = \operatorname{adj}\varphi(\mathbf{k}) \end{aligned}$$

which is clearly true.

Finally, φ is injective since its kernel is trivial (see Exercise A.2.13*). Indeed, $\varphi(\alpha) = 0$ implies $\varphi(\overline{\alpha}) = \operatorname{adj}\varphi(\alpha) = 0$. As a consequence, if $\alpha = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$,

$$2\varphi(a) = \varphi(\alpha + \overline{\alpha}) = 0$$

so $a = 0$ since m is odd. The same reasoning used on $\alpha\mathbf{i}$, $\alpha\mathbf{j}$ and $\alpha\mathbf{k}$ shows that $a = b = c = d = 0$. ■

Remark 2.6.2

The step where we assume $a = b = 0$ is completely legitimate: since $a^2 - b^2 + c^2 + d^2 + 2ab\mathbf{i} + 2iac\mathbf{j} + 2iad\mathbf{k}$ must be -1, we need $ab = ac = ad = 0$, i.e. $a = 0$ or $b = c = d = 0$ but the latter clearly doesn't work when there's no square root of -1 in $\mathbb{Z}/m\mathbb{Z}$. Thus, $a = 0$. Similarly, we want

$$\mathbf{k}' := -\mathbf{i}\mathbf{j}' = -\mathbf{i}(w\mathbf{i} + ui\mathbf{j} + vi\mathbf{k}) = w - ui\mathbf{k} + vi\mathbf{j}$$

to square to -1, which implies $w = 0$ for the same reason.

Exercise 2.6.18†. Let m be an odd integer. We say a Hurwitz integer $\alpha = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ is *primitive modulo* n if $\gcd(2a, 2b, 2c, 2d, m) = 1$. Compute the number $\psi(m)$ of primitive Hurwitz integers modulo m with norm zero (modulo m).

Solution

By Exercise 2.6.17†, we need to count the number of two by two primitive modulo m matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with zero determinant, i.e. the number of a, b, c, d such that $ad - bc \equiv 0 \pmod{m}$ and $\gcd(a, b, c, d, m) = 1$. It is immediate from the Chinese remainder theorem that this is multiplicative, i.e. $\psi(mn) = \psi(m)\psi(n)$ when m and n are coprime. Hence, it remains to compute $\psi(p^k)$ for an odd prime p. We shall first prove that $\psi(p^{k+1}) = p^3\psi(p^k)$, thus reducing this computation to the (easy) computation of $\psi(p)$. More precisely, we show that any primitive modulo p^k quadruple (a, b, c, d) such that

$$ad - bc \equiv 0 \pmod{p^k}$$

can be lifted to exactly p^3 primitive modulo p^{k+1} quadruple $(a', b', c', d') \equiv (a, b, c, d) \pmod{p^k}$ such that $a'd' - b'c' \equiv 0 \pmod{p^{k+1}}$. Hence, suppose (a, b, c, d) is such a quadruple and suppose without loss of generality that a is non-zero modulo p. Consider a quadruple $(a', b', c', d') \equiv (a, b, c, d) \pmod{p^k}$. The congruence $a'd' \equiv b'c' \pmod{p^{k+1}}$ is equivalent to

$$d' \equiv b'c'(a')^{-1} \pmod{p^{k+1}}.$$

Thus, for each choice of a', b', c', there is exactly one d' satisfying this equality. Since there are p^3 triplets (a', b', c') modulo p^{k+1} which are congruent to (a, b, c) modulo p^k, this proves the result.

It remains to compute $\psi(p)$. Choose a $t \in \mathbb{Z}/p\mathbb{Z}$ and consider the equation $ad \equiv t \equiv bc \pmod{p}$. If $t \not\equiv 0$, there are $(p-1)^2$ solutions: pick any non-zero a, b, and set $d \equiv ta^{-1}$ and $c \equiv tb^{-1}$. If $t \equiv 0$, there are $2(p-1)+1 = 2p-1$ solutions to $ad \equiv 0$: if $a \equiv 0$, there are $p-1$ non-zero possibilities for d and inversely, and then we count the solution $a \equiv d \equiv 0$. Hence, there are $(2p-1)^2$ solutions to $ad \equiv 0 \equiv bc$, but since we are interested in primitive quadruples, we must remove the solution $(0,0,0,0)$. In total, we have

$$\psi(p) = (p-1) \cdot (p-1)^2 + (2p-1)^2 - 1 = (p^2-1)(p+1).$$

To conclude, if $m = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$, we have

$$\begin{aligned}
\psi(m) &= \prod_{i=1}^{k} \psi(p^k) \\
&= \prod_{i=1}^{k} p^{3(k-1)} \psi(p) \\
&= \prod_{i=1}^{k} p^{3(k-1)} (p^2-1)(p+1) \\
&= m^3 \prod_{p \mid m} \left(1 - \frac{1}{p^2}\right)\left(1 + \frac{1}{p}\right).
\end{aligned}$$

■

Exercise 2.6.19†. Let p be an odd prime. Prove that any non-zero $\alpha \in H/pH$ of zero norm modulo p has a representative of the form $\rho\pi$, where π is a primary element of norm p and $\rho \in H$, and that this π is unique. Conversely, let $\pi \in H$ have norm p. Prove that the equation $\rho\pi \equiv 0 \pmod{p}$ has exactly p^2 solutions $\rho \in H/pH$. Deduce that there are exactly $p+1$ primary irreducible Hurwitz integers with norm p.

Solution

Lift α to a Hurwitz integer β of norm divisible by p. Consider its primitive part γ. Since β isn't divisible by p, the norm of γ is still divisible by p. Hence, by Exercise 2.6.15†, $\gamma = \rho\pi$ for some $\rho \in H$ and some π of norm p. In addition, as we saw in the solution to this exercise, this π is unique up to multiplication by a right-unit since it's the left-gcd of γ and p. However, we still need to justify the step where we went from β to γ, i.e. that $\beta = \delta\pi$ for some $\delta \in H$ and π of norm p implies $\gamma = \rho\pi$ for some $\rho \in H$. Let m be the non-squarefree part of β, i.e. $\beta = m\gamma$. Since $p = \pi\overline{\pi}$ is invertible modulo m, π is too so m must divide δ by Bézout. We are done: $\gamma = (\delta/m)\pi$.

For the second part, by Exercise 2.6.17†, this amounts to counting the solutions (x, y, z, t) to

$$\begin{bmatrix} x & y \\ z & t \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \pmod{p}$$

where $\begin{bmatrix} x & y \\ z & t \end{bmatrix}$ is the matrix corresponding to ρ and $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ the matrix corresponding to π. In

other words, we wish to count the solutions to

$$xa + yc \equiv 0 \tag{2.1}$$
$$xb + yd \equiv 0 \tag{2.2}$$
$$za + tc \equiv 0 \tag{2.3}$$
$$zb + td \equiv 0. \tag{2.4}$$

Note that the condition that π has norm divisible by p translates to $ad - bc \equiv 0$. Since π is non-zero modulo p, at least one of its coordinate is non-zero, say a. Then, (1) becomes $x \equiv -yca^{-1}$ and (3) becomes $z \equiv -tca^{-1}$. Note that the other two equations are then automatically fulfilled since

$$a(xb + yd) = b(xa + yc) - (ad - bc)y$$

and the same goes for z and t. Hence, there are p^2 solutions as claimed: we choose y and t arbitrarily and x and y are then uniquely determined.

We have shown that each of the $\psi(p) = (p^2 - 1)(p + 1)$ non-zero classes of H/pH of zero norm can be written in the form $\rho\pi$ for some unique π of norm p. However, each π has exactly p^2 left-multiples modulo p: $\rho\pi$ takes each value exactly p^2 times and there are p^4 elements $\rho \in H/pH$, π has $p^4/p^2 = p^2$ left-multiples. (This can also be seen more efficiently with the language of group theory: the morphism from H/pH to itself sending ρ to $\rho\pi$ has a kernel of cardinality p^2 so its image has cardinality $|H/pH|/p^2 = p^2$ by the first isomorphism theorem from Exercise A.3.15†.) Thus, each π occurs for exactly $p^2 - 1$ classes, so there are

$$\frac{\psi(p)}{p^2 - 1} = p + 1$$

primary elements of norm p. ■

Exercise 2.6.20† (Jacobi's Four Square Theorem)**.** Let n be a positive rational integer. In how many ways can n be written as a sum of four squares of rational integers. (Two ways are considered different if the ordering is different, for instance $2 = 1^2 + 0^2 + 0^2 + (-1)^2$ and $2 = (-1)^2 + 0^2 + 0^2 + 1^2$ are different.)

Solution

Note that counting the number of ways to write n as a sum of four squares is the same as counting the number of quaternions in $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$ with norm n. We start by counting the number of primary primitive Hurwitz integers of odd norm m, then we will consider the contribution of primary non-primitive integers of norm m, and finally the contribution of their associates too (and treat the even case).

Let m be an odd positive integer and let $p_1^{m_1} \cdot \ldots \cdot p_n^{m_n}$ be its prime factorisation. By Exercise 2.6.15†, each primitive integer of norm m has an expression of the form

$$\prod_{i=1}^{n} \prod_{j=1}^{m_i} \pi_j^{(i)}$$

where $\pi_j^{(i)}$ is an element of norm p_i. Since we are interested in primary integers, we may assume that each $\pi_j^{(i)}$ is primary as well, by migrating the units. Then, this expression becomes unique, and any such expression gives rise to a unique integer of norm m again by Exercise 2.6.15†, provided that it is primitive. We will prove that it is primitive as long as two consecutive factors are not conjugates, which is obviously a necessary condition. (Note that the conjugate of a primary integer is also primary.) Suppose that some rational prime p divides this product. Since the product has norm m, $p = p_k$ for some k. Since every element of norm coprime with p is

invertible modulo p, p must divide

$$\pi_1^{(k)} \cdot \ldots \cdot \pi_{m_k}^{(k)} := \pi_1 \cdot \ldots \cdot \pi_\ell.$$

Consider the greatest i such that p divides $\pi_1 \cdot \ldots \cdot \pi_i$. Then, $\pi_1 \cdot \ldots \cdot \pi_{i-1}$ is not divisible by p so is primitive since its norm is a power of p. We will prove that π_i and π_{i-1} are conjugate. Write $p\rho = \pi_1 \cdot \ldots \cdot \pi_i$ for some $\rho \in H$. This is equivalent to

$$\rho\overline{\pi_i} = \pi_1 \cdot \ldots \cdot \pi_{i-1}.$$

Since these elements are now primitive, Exercise 2.6.15† tells us that $\overline{\pi_i}$ and π_{i-1} are the same up to association, i.e. the same since they are primary.

Hence, the number $f(m)$ of primary and primitive Hurwitz integers of norm m is equal to the number of products of the form

$$\prod_{i=1}^{n} \prod_{j=1}^{m_i} \pi_j^{(i)}$$

where $\pi_j^{(i)}$ is primary of norm p_i and no two consecutive factors are conjugate. In other words, we have $p_1 + 1$ possibilities for $\pi_1^{(1)}$ and then only p_1 for every other $\pi_j^{(1)}$ since we need to avoid the conjugate of $\pi_{j-1}^{(1)}$. The same goes for $p_2, p_3, \ldots, p_n$. Thus,

$$f(m) = \prod_{k=1}^{n} (p_i + 1) p_i^{m_i - 1} = m \prod_{k=1}^{n} \left(1 + \frac{1}{p}\right).$$

Now that we have computed the number of primary primitive integers of norm m, we shall compute the number of primary integers of norm m. This is simply

$$g(m) = \sum_{d^2 | m} f(m^2/d)$$

because a primary integer α of norm m is a primary primitive integer of norm m/d^2, where d is the non-primitive part of m, i.e. the unique positive integer $d \mid \alpha$ such that α/d is primitive. By expanding the following expression, we see that

$$g(m) = \prod_{i=1}^{n} \sum_{k=0}^{m_i/2} f(p_i^{m_i - 2k})$$

because f is multiplicative, i.e. $f(ab) = f(a)f(b)$ when a and b are coprime, and each $d^2 \mid m$ can be written as $p_1^{d_1} \cdot \ldots \cdot p_n^{d_n}$ with $2d_i \leq m_i$ for every i. Now, note that the sum $\sum_{k=0}^{\ell/2} g(p^{\ell-2k})$ is

$$p^{\ell-1}(p+1) + p^{\ell-3}(p+1) + \ldots + (p+1) = p^\ell + \ldots + 1$$

when ℓ is odd, and

$$p^{\ell-1}(p+1) + p^{\ell-3}(p+1) + \ldots + p(p+1) + 1 = p^\ell + \ldots + 1$$

when ℓ is even. Thus, in all cases,

$$g(m) = \prod_{i=1}^{n} \sum_{k=0}^{m_i} p^k = \sum_{d|m} d.$$

Now, only two things remain be done: take in account the contribution of units, and treat the case where m is odd. Let α be a primary integer and let ε be a unit of H. Then, $\alpha\varepsilon$ is in $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$ if and only if $\varepsilon \in \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$. Thus, there are

$$r_4(n) = 8g(n) = 8 \cdot \sum_{d|n} d$$

ways to write n as a sum of four squares when n is odd. Now suppose that n is even and write $n = 2^r m$ with $r = v_2(n)$. We will prove that any element of norm n has the form $(1+i)^r$ times an element of norm m. As a consequence, the number of primary quaternions of norm n will be

$$g(n) = g(m) = \sum_{d|m} d.$$

This time however all units will yield elements in $\mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ since $(1+\mathbf{i})\varepsilon \in \mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$ for any unit ε. Since there are 24 units, we conclude that the numbers of ways to express n as a sum of four squares is

$$r_4(n) = 24g(m) = 24 \cdot \sum_{d|n, d \text{ odd}} d.$$

Hence, it only remains to prove that an element of even norm is divisible by $1+\mathbf{i}$. Indeed, since $1+\mathbf{i}$ has norm 2, iterating this result yields that an element of norm divisible 2^r is divisible by $(1+\mathbf{i})^r$ as wanted. Suppose that $\alpha = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ has even norm. In particular, $(2a)^2 + (2b)^2 + (2c)^2 + (2d)^2$ is divisible by 8. Since odd squares are 1 modulo 8, this implies $2 \mid 2a, 2b, 2c, 2d$, i.e. $\alpha \in \mathbb{Z}[\mathbf{i},\mathbf{j},\mathbf{k}]$. Modulo $1+\mathbf{i}$, α is simply $a+b+c+d$, which is clearly divisible by $1+\mathbf{i}$ since it is divisible by 2. We are done.

To summarise, there are $8 \cdot \sum_{d|n} d$ ways to write n as a sum of two squares when n is odd, and $24 \cdot \sum_{d|n, d \text{ odd}} d$ when n is even. ■

Domains

Miscellaneous

Exercise 2.6.25†. Let $(F_n)_{n\in\mathbb{Z}}$ be the Fibonacci sequence defined by $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for any integer n. Prove that, for any integers m and n, $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.

Solution

Note that $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$, where α, β are the roots of $X^2 - X - 1$ (see Section C.4). Thus, $d \mid F_m, F_n$ if and only if

$$\delta := (\alpha - \beta)d \mid \alpha^m - \beta^m, \alpha^n - \beta^n.$$

Now, note that $\delta = \alpha^{\gcd(m,n)} - \beta^{\gcd(m,n)} = (\alpha - \beta)F_{\gcd(m,n)}$ works since

$$\alpha^{k\gcd(m,n)} \equiv \beta^{k\gcd(m,n)}$$

for any $k \in \mathbb{Z}$. For the converse, let k be the smallest positive integer such that

$$\delta \mid \alpha^k - \beta^k \iff \delta \mid (\alpha/\beta)^k - 1$$

(note that β is a unit since $\alpha\beta = 1$ so we can divide by β like we did). Then, we shall prove that $k \mid m, n$. Write $m = qk + r$ the Euclidean division of m by k. Then,

$$1 \equiv (\alpha/\beta)^m = (\alpha/\beta)^k)^q \cdot (\alpha/\beta)^r \equiv (\alpha/\beta)^r$$

which contradicts the minimality of k, unless $r = 0$. Thus, $k \mid m$, and by symmetry $k \mid n$, which implies that $k \mid \gcd(m,n)$ and $\delta \mid \alpha^{\gcd(m,n)} - \beta^{\gcd(m,n)}$ as wanted. ■

Remark 2.6.3

This is identical to the proof that $\gcd(a^n - b^n, a^m - b^m) = a^{\gcd(m,n)} - b^{\gcd(m,n)}$ for $a, b \in \mathbb{Z}$ using

orders, but in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. See Section 7.2 for more.

Exercise 2.6.27†. Let n be a rational integer. Prove that $(1+\sqrt{2})^n$ is a unit of $\mathbb{Z}[\sqrt{2}]$. Moreover, prove that any unit of $\mathbb{Z}[\sqrt{2}]$ has that form, up to sign.

Solution

Note that $N((1+\sqrt{2})^k) = (-1)^k$ so $(1+\sqrt{2})^k$ is a unit. Now, suppose $a+b\sqrt{2}$ is the smallest unit with $a, b > 0$ which is not a power of $1+\sqrt{2}$. Then,

$$(2b-a)+(a-b)\sqrt{2} = -(a+b\sqrt{2})(1-\sqrt{2}) = \frac{a+b\sqrt{2}}{1+\sqrt{2}} < a+b\sqrt{2}.$$

Thus, if we show that $2b-a>0$ and $a-b>0$, we will reach a contradiction. This is easy: since $a^2-2b^2 = \pm 1$, if $2b \le a$ we have

$$a^2-2b^2 \ge 2b^2 > 1,$$

and if $a \le b$ we have

$$a^2-2b^2 < -b^2 < -1$$

unless $b=1$ but that gives $a+b\sqrt{2} = 1+\sqrt{2}$ which we have ruled out. (See also Section 7.1.)■

Exercise 2.6.28† (IMO 2001)**.** Let $a > b > c > d$ be positive rational integers. Suppose that

$$ac+bd = (b+d+a-c)(b+d-a+c).$$

Prove that $ab+cd$ is not prime.

Solution

We shall first simplify the condition on a, b, c, d:

$$ac+bd = (b+d)^2-(a-c)^2 = b^2+2bd+d^2-a^2+2ac-c^2,$$

i.e. $a^2-ac+c^2 = b^2+bd+d^2$, or in other words, $(a+jc)(a+j^2c) = (b-jd)(b-j^2d)$. This of course suggests working in $\mathbb{Z}[j]$. Set $\alpha = a+jc$ and $\beta = b-jd$. We have $\alpha\overline{\alpha} = \beta\overline{\beta}$. Let ρ be the gcd of α and β and write $\alpha = \gamma\rho$ and $\beta = \delta\rho$. Then,

$$\gamma\overline{\gamma} = \delta\overline{\delta}$$

and $\gcd(\gamma, \delta) = 1$ so $\gamma \mid \overline{\delta}$ and $\delta \mid \overline{\gamma}$, i.e. $\gamma = \varepsilon\delta$ for some unit $\varepsilon \in \mathbb{Z}[j]$. Now, notice that

$$\alpha\beta = (a+jc)(a-jd) = ab+cd+j(bc+cd-ad).$$

However, $\alpha\beta$ is also equal to $\gamma\delta\rho^2$ and $\gamma\delta = \varepsilon N(\gamma)$. Hence, if $ab+cd$ is prime, we have $N(\gamma) \in \{1, ab+cd\}$.

Suppose first that $N(\gamma) = 1$, i.e. γ is a unit. Then, $\beta = \delta\rho$ is a unit times $\gamma\rho = \alpha$, say $\alpha = \eta\beta$. Since the only units of $\mathbb{Z}[j]$ are $\pm j^k$ by Exercise 2.4.2*, we get

$$\pm(a+jc) \in \{b-jd, d+j(b+d), b+d+jb\}.$$

All of these clearly contradict the assumption that $a > b > c > d > 0$. It remains to treat the case where $N(\gamma) = ab+cd$. In that case, we have $ab+cd \mid bc+cd-ad$ since

$$N(\gamma) \mid \alpha\beta = ab+cd+j(bc+cd-ad).$$

Note that $bc + cd - ad$ must be positive or zero for otherwise its absolute value is less than $ad < ab + cd$. However, if it is positive, then $bc + cd - ad \geq ab + cd$ which is impossible since $ab > bc$. Hence, $bc + cd - ad$ must be 0. This implies that

$$\varepsilon\rho^2(ab + cd) = \gamma\delta\rho^2 = ab + cd,$$

i.e. ρ is a unit. Then, $\overline{\beta} = \varepsilon\gamma\overline{\rho}$ is a unit times $\gamma\rho = \alpha$, say $\alpha = \mu\overline{\beta}$. As before, the only units of $\mathbb{Z}[j]$ are $\pm j^k$ so we get

$$\pm(a + jc) \in \{b + d + jd, -d + jb, b + j(b + d)\}.$$

Each of these cases still contradicts $a > b > c > d > 0$. ■

Exercise 2.6.29†. Let $x \in \mathbb{R}$ be a non-zero real number and $m, n \geq 1$ coprime integers. Suppose that $x^m + \frac{1}{x^m}$ and $x^n + \frac{1}{x^n}$ are both rational integers. Prove that $x + \frac{1}{x}$ is also one.

Solution

Let $a = x^m + \frac{1}{x^m}$ and $b = x^n + \frac{1}{x^n}$. Then, $x^m = \frac{a \pm \sqrt{a^2-4}}{2}$ and $x^n = \frac{b \pm \sqrt{a^2-4}}{2}$, i.e. x^m and x^n are units in a quadratic field $\mathbb{Q}(\sqrt{d})$ (it is the same field since $(x^m)^n = (x^n)^m$). Finally, let $u, v \in \mathbb{Z}$ be such that $um + vn = 1$, by Bézout's lemma. Then, $x = x^{um}x^{vn}$ is a unit of $\mathbb{Q}(\sqrt{d})$ too, i.e. $x + \frac{1}{x} \in \mathbb{Z}$ (since $\frac{1}{x}$ is the conjugate of x). ■

Remark 2.6.4

One might be tempted to look at x^{mn}: it is both an mth power and an nth power in $\mathbb{Q}(\sqrt{d})$ so we may want to conclude that it is an mnth power. For UFDs, by looking at the p-adic valuation, we see that it is an mnth power times a unit. Since the only units in real quadratic fields ($\mathbb{Q}(\sqrt{d})$ for $d > 0$) are ± 1 (see Section 7.1), we conclude that it is $\pm$ an mnth power, and by looking at the parity of mn, we can see that in fact it must be an mnth power as wanted. In general, $\mathbb{Q}(\sqrt{d})$ might not be a UFD, but since it has ideal factorisation, there is still a concept of p-adic valuation so the previous solution works too.

Chapter 3

Cyclotomic Polynomials

3.1 Definition

Exercise 3.1.1*. Let ω be an nth root of unity. Prove that its order divides n.

Solution

Let k be the order of ω and let $n = qk + r$ be the Euclidean division of n by k. We have

$$\omega^n = (\omega^k)^q \omega^r = \omega^r$$

so $\omega^r = 1$ but $r < k$ which means that $r = 0$ by minimality of the order. ■

Exercise 3.1.2*. Let p be a rational prime. Prove that $\Phi_p = X^{p-1} + \ldots + 1$.

Solution

We have $\Phi_1 \Phi_p = X^p - 1$ by Proposition 3.1.1 so

$$\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + \ldots + 1.$$

■

Exercise 3.1.3*. Let $n \geq 1$ be an integer. Prove that $\Phi_n(0) = -1$ if $n = 1$ and 1 otherwise.

Solution

By induction on n: true for $n = 1$ and for $n > 1$ we have

$$\Phi_n(0) = \frac{0^n - 1}{\prod_{d|n, d<n} \Phi_d(0)} = \frac{-1}{-1 \cdot 1 \cdot \ldots \cdot 1} = 1.$$

■

Exercise 3.1.4. Let $n > 1$ be an integer. Prove that $\Phi_n(1) = p$ if n is a power of a prime p, and $\Phi_n(1) = 1$ otherwise.

Solution

By induction on n:

$$\prod_{1\neq d|n} \Phi_d = \frac{X^n-1}{X-1} = X^{n-1}+\ldots+1$$

so $\prod_{1\neq d|n} \Phi_d(1) = n$. Note that the function given in the statement satisfies this equation:

$$\prod_{1\neq p^i|n} p = \prod_{p|n} p^{v_p(n)} = n$$

since each factor p appears exactly $v_p(n)$ times. Thus, by induction, $\Phi_n(1)$ is p is n is a power of p and 1 otherwise. ■

Exercise 3.1.5*. Prove the Corollary 3.1.1 by induction.

Solution

By induction on n:

$$\Phi_n = \frac{X^n-1}{\prod_{d|n,d<n}\Phi_d}$$

and this polynomial division has integer coefficients since the divider is monic. ■

Exercise 3.1.6*. Prove that $\Phi_n(1/X) = \Phi_n(X)/X^{\varphi(n)}$ for $n > 1$.

Solution

When $n > 1$, the primitive nth roots of unity come by pairs $\omega, 1/\omega$ so the number of such . Thus,

$$\Phi_n(1/X) = \prod_\omega 1/X - \omega = \prod_\omega \frac{1}{\omega X}(\omega - X) = \Phi_n/X^{\varphi(n)}(-1)^{\varphi(n)}\prod_\omega 1/\omega$$

and $(-1)^{\varphi(n)}\prod_\omega 1/\omega = \Phi_n(0)$ by Vieta's formulas which is 1 by Exercise 3.1.3*. ■

Remark 3.1.1

If $f = \sum_i a_i X^i$ is a polynomial, the fact that $f(X) = X^{\deg f} f(1/X)$ can be seen more visually using its coefficients: this is equivalent to

$$\sum_i a_i X^i = \sum a_i X^{\deg f - i},$$

i.e. $a_i = a_{\deg f - i}$.

Exercise 3.1.7*. Prove that, for $n > 1$, $\Phi_n(X, Y)$ is a two-variable symmetric and homogeneous, i.e. where all monomials have the same degree, polynomial with integer coefficients.

Solution

It is homogeneous because $\Phi_n(X/Y)$ is a homogeneous rational fractions (of degree 0) and $Y^{\varphi(n)}$

is too. It is a polynomial because, if $\Phi_n = \sum_i a_i X^i$ then

$$Y^{\varphi(n)}\Phi_n(X/Y) = \sum_i a_i X^i Y^{\varphi(n)-i}$$

(we can also see it is homogeneous that way). It is symmetric by Exercise 3.1.6*:

$$\Phi_n(Y/X) = (Y/X)^{\varphi(n)}\Phi_n(X/Y) \iff X^{\varphi(n)}\Phi_n(Y/X) = Y^{\varphi(n)}\Phi_n(X/Y).$$

■

Exercise 3.1.8*. Prove that

$$\Phi_n(X,Y) = \prod_{\omega \text{ primitive } n\text{th root}} X - \omega Y.$$

Solution

We have

$$\Phi_n(X,Y) = Y^{\varphi(n)} \prod_\omega X/Y - \omega = \prod_\omega X - Y\omega.$$

■

Exercise 3.1.9*. Prove that, for odd $n > 1$, $\Phi_n(X)\Phi_n(-X) = \Phi_n(X^2)$ and deduce Corollary 3.1.3.

Solution

We have

$$\Phi_n(X)\Phi_n(-X) = \prod_\omega (X-\omega)(-X-\omega) = \prod_\omega -(X^2-\omega^2) = (-1)^{\varphi(n)} \prod_\omega X^2 - \omega^2.$$

Since $n > 2$, $\varphi(n)$ is even, and since n is odd, $\omega \mapsto \omega^2$ is a permutation of the primitive nth roots of unity so this is just $\Phi_n(X^2)$. Since $\Phi_{2n}(X) = \frac{\Phi_n(X^2)}{\Phi_n(X)}$ by Proposition 3.1.2, we get $\Phi_2 n(X) = \Phi_n(-X)$. ■

Exercise 3.1.10. Prove that, for any polynomial f, $f(X)f(-X)$ is a polynomial in X^2.

Solution

We present three proofs: the first work over any ring with the fundamental theorem of symmetric polynomials and by expansion, and one which works over $\mathbb{C}$ (and any algebraically closed field) using the fundamental theorem of algebra A.1.1.

For the first one, note that $f(X)f(-X)$ is symmetric in X and $-X$ so is a polynomial in $-X^2$ and 0.

For the second one, write $f(X)$ as $g(X^2) + Xh(X^2)$ to get

$$f(X)f(-X) = (g(X^2) + Xh(X^2))(g(X^2) - Xh(X^2)) = g(X^2)^2 + X^2 h(X^2)^2.$$

For the last one, note that that the result is true for polynomials of degree 1 as

$$(X-\alpha)(-X-\alpha) = -(X-\alpha)(X+\alpha) = -(X^2-\alpha^2)$$

so is true for any polynomial since any polynomial factorises as a product of a constant polynomial and degree 1 polynomials. ■

Exercise 3.1.11*. Let p be a prime number and $n \geq 1$ an integer. Prove that if $p \mid n$ then $\Phi_{pn}(X,Y) = \Phi_n(X^p, Y^p)$, and that $\Phi_{pn}(X,Y) = \frac{\Phi_n(X^p,Y^p)}{\Phi_n(X,Y)}$ otherwise.

Solution

We have

$$\Phi_{pn}(X,Y) = Y^{\varphi(pn)}\Phi_{pn}(X/Y) = \begin{cases} Y^{p\varphi(n)}\Phi_n(X^p/Y^p) = \Phi_n(X^p,Y^p) & \text{if } p \mid n \\ Y^{p\varphi(n)}/Y^{\varphi(n)}\frac{\Phi_n(X^p/Y^p)}{\Phi_n(X/Y)} = \frac{\Phi_n(X^p,Y^p)}{\Phi_n(X,Y)} & \text{if } p \nmid n \end{cases}$$

by Proposition 3.1.2. ■

Exercise 3.1.12*. Let $k \geq 1$ be an integer. Prove that $\Phi_{2^k} = X^{2^{k-1}} + 1$.

Solution

By induction on n: we have $\Phi_2 = X^{2^0} + 1$ and

$$\Phi_{2\cdot 2^{2^k}} = \Phi_{2^k}(X^2, Y^2) = X^{2^{k-1}} + Y^{2^{k-1}}$$

for $k \geq 1$ by Proposition 3.1.2. ■

3.2 Irreducibility

Exercise 3.2.1*. Let $n \geq 1$ be an integer and ω be a primitive nth root of unity. Prove that any primitive nth root can be written in the form ω^k for some $\gcd(k,n) = 1$.

Solution

Write $\omega = \exp\left(\frac{2mi\pi}{n}\right)$ for some $\gcd(m,n) = 1$. The other primitive roots of unity are $\exp\left(\frac{2ki\pi}{n}\right)$ for $\gcd(k,n) = 1$ and the powers of ω are $\exp\left(\frac{2kmi\pi}{n}\right)$. Since m is coprime with n, it is invertible mod n so $k \mapsto km$ is a bijection of $(\mathbb{Z}/n\mathbb{Z})^\times$ which is equivalent to $\omega \mapsto \omega^k$ being a bijection of primitive nth root as wanted. ■

Exercise 3.2.2*. Let $f = \prod_{k=1}^n X - \alpha_i$ be a polynomial. Prove that, for any $k = 1, \ldots, n$, $f'(\alpha_k) = \prod_{i \neq k} \alpha_k - \alpha_i$.

Solution

By Exercise A.1.8*, we have

$$f' = \sum_i \prod_{j \neq i} X - \alpha_i$$

from which the result follows by evaluating this at α_k. ■

Exercise 3.2.3* (Frobenius Morphism)**.** Prove the following special case of Proposition 4.1.1: for any rational prime p and any polynomial $f \in \mathbb{Z}[X]$, $f(X^p) \equiv f(X)^p \pmod{p}$.

Solution

Note that

$$(f+g)^p = \sum_k \binom{p}{k} f^k g^{p-k} \equiv f^p + g^p \pmod{p}$$

for any $f, g \in \mathbb{Z}[X]$ since $p \mid \binom{p}{k} = \frac{p!}{k!(p-k)!}$ for $0 < k < p$. Thus, by induction, $(\sum f_i)^p \equiv \sum f_i^p$. Taking $f_i = a_i X^i$ and letting $f = \sum_i a_i X^i$, we get

$$f(X)^p = \left(\sum_i a_i X^i\right)^p = \sum_i a_i^p X^{ip} \equiv \sum_i a_i X^{ip} = f(X^p)$$

by Fermat's little theorem. ■

Exercise 3.2.4 (Alternative Proof of Theorem 3.2.1)**.** Let ω be a primitive nth root of unity with minimal polynomial π and let $p \nmid n$ be a rational prime. Suppose τ is the minimal polynomial of $\pi(\omega^p)$. Prove that $p \mid \tau(0)$ and that $\tau(0)$ is bounded when p varies. Deduce that ω^p is a root of π for sufficiently large p, and thus that ω^k is a root of π for any $\gcd(n,k) = 1$.

Solution

$\tau(0)$ is $\pm$ the product of its roots by Vieta's formulas, and since $\pi(\omega^p)$ is a root it is divisible by it. Thus, $p \mid \pi(\omega^p) \mid \tau(0)$. Note that, by the fundamental theorem of symmetric polynomials, each root of τ has the form $\pi(\omega^{kp})$ for some k. In particular, if $\omega_1, \ldots, \omega_m$ are the roots of π (i.e. the conjugates of ω), we have

$$|\pi(\omega^{kp})| = \prod_i |\omega^{kp} - \omega_i| \leq 2^m \leq 2^n$$

by the triangular inequality. Thus, the roots of $\tau(0)$ all have absolute value less than 2^n, and since τ has at most n roots, its constant coefficient $\tau(0)$ is bounded by 2^{n^2}. This shows that for sufficiently large $p > 2^{n^2}$, since $p \mid \tau(0)$, we have $\tau(0) = 0$, i.e. $\tau = X$ and $\pi(\omega^p) = 0$.

To finish, say $p_1, \ldots, p_\ell \nmid n$ are the primes less than 2^{n^2}. Since ω^p is also a primitive nth root of unity for $p \nmid n$, we can repeat our reasoning with this root of unity to show that $\pi(\omega^m) = 0$ for any m whose prime factors are all greater than 2^{n^2}. Pick any k coprime with n. Using the Chinese remainder theorem, pick an $m \equiv k \pmod{n}$ which is congruent to 1 modulo $p_1, \ldots, p_\ell$. Then all prime factors of m are greater than 2^{n^2} so

$$\pi(\omega^k) = \pi(\omega^m) = 0$$

as wanted. ■

Exercise 3.2.5. Let k and $n \geq 1$ be coprime integers. Prove that the conjugates of $\cos\left(\frac{2k\pi}{n}\right)$ are the numbers $\cos\left(\frac{2k'\pi}{n}\right)$ for $\gcd(k', n) = 1$. What is its degree? What about $\sin\left(\frac{2k\pi}{n}\right)$, what are its conjugates and what is its degree?

Solution

Note that

$$2\cos\left(\frac{2k\pi}{n}\right) = \omega + 1/\omega = \omega + \omega^{n-1}$$

where $\omega = \exp\left(\frac{2k\pi}{n}\right)$ is a primitive nth root of unity. In particular, by the fundamental theorem of symmetric polynomials, the conjugates of $2\cos\left(\frac{2k\pi}{n}\right)$ are among $2\cos\left(\frac{2k'\pi}{n}\right)$ for $\gcd(k', n) = 1$ as wanted. For the converse, note that if $f(2\cos\left(\frac{2k\pi}{n}\right)) = 0$ then $f(X + X^k)$ has a root at ω so at all other primitive nth roots of unity as wanted. In particular, for $n \geq 3$, $\cos\left(\frac{2k\pi}{n}\right)$ conjugates since the numbers $\cos\left(\frac{2k'\pi}{n}\right)$ go by pair $\cos\left(\frac{2k'\pi}{n}\right), \cos\left(\frac{-2k'\pi}{n}\right)$. (For $n \leq 2$, it has degree $\varphi(n) = 1$.)

The situation is more complicated for sines. The same argument shows that its conjugates are $\sin\left(\frac{2k'\pi}{n}\right)$ for $\gcd(k', n) = 1$ (or using $\sin(x) = \cos(\pi/2 - x)$), but it is now harder to count its conjugates. Perhaps the simplest way is to transform it into a cosine:

$$\sin\left(\frac{2k\pi}{n}\right) = \cos\left(\frac{\pi}{2} - \frac{2k\pi}{n}\right) = \cos\left(\frac{2\pi(n-4k)}{4n}\right).$$

We need to evaluate $\gcd(n - 4k, 4n)$. Since k and n are coprime, it is clear that the only potential prime factor of this gcd is 2. In particular, if $8 \mid n$, the gcd is 4 so $\sin\left(\frac{2k\pi}{n}\right)$ has degree $\varphi(4n/4)/2 = \varphi(n)/2$.

When $n \equiv 4 \pmod 8$, the numerator is this time divisible by 8 because $n \equiv 4k \pmod 8$. If $n \equiv 4 \pmod{16}$, then the gcd is 16 so $\sin\left(\frac{2k\pi}{n}\right)$ has degree

$$\varphi(4n/16)/2 = \varphi(n)/4.$$

If $n \not\equiv 4 \pmod{16}$, then it has degree $\varphi(4n/8)/2 = \varphi(n)/4$ as well ($\varphi(m) = \varphi(2m)$ when m is odd). Of course, we are assuming that $n \neq 4$ here, so that $n - 4k$ is non-zero. If $n = 4$, it has degree 1.

If $n \equiv 2 \pmod 4$, the gcd of $n - 4k$ and $4n$ is just 2, so $\sin\left(\frac{2k\pi}{n}\right)$ has degree $\varphi(4n/2)/2 = \varphi(n)$. Similarly, if n is odd, the gcd is 1 so it has degree $\varphi(4n)/2 = \varphi(n)$ as well. This time we assumed that n was greater than 2, otherwise it has degree 1. We can summarise our results in the following table.

	degree of $\sin\left(\frac{2k\pi}{n}\right)$
$n \in \{1, 2, 4\}$	1
$n \equiv 0 \pmod 8$	$\varphi(n)/2$
$n \equiv 4 \pmod 8$	$\varphi(n)/4$
$n \equiv 2 \pmod 4$	$\varphi(n)$
$n \equiv 1 \pmod 2$	$\varphi(n)$

■

Remark 3.2.1

The reason why sines turn out to be so unstructured is because of the i in the denominator of $\sin\left(\frac{2k\pi}{n}\right) = \frac{\omega^k - \omega^{-k}}{2i}$. Suppose $k = 1$ without loss of generality, by symmetry between primitive

nth roots of unity. The best way to see this is with Galois theory (see Chapter 6). Because of this i, to consider conjugates of $\sin\left(\frac{2\pi}{n}\right)$ we need to work in $\mathbb{Q}(\omega, i)$. Then, we count the number of automorphisms, i.e. elements of the Galois group over $\mathbb{Q}$, fixing $\sin\left(\frac{2\pi}{n}\right) = \frac{\omega-\omega^{-1}}{2i}$. If there are N such elements, then there are exactly

$$[\mathbb{Q}(\omega, i) : \mathbb{Q}]/N = \varphi(\mathrm{lcm}(4, n))/N$$

conjugates, by Proposition 6.3.1. Normally $N = 2$, i.e. there are only two embeddings fixing $\frac{\omega-\omega^{-1}}{2i}$: the identity and the complex conjugation. However, sometimes there are more. Let's see more closely what's happening: if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega, i)/\mathbb{Q})$ fixes $\frac{\omega-\omega^{-1}}{2i}$, since it sends i to $\pm i$, it must send $\omega - \omega^{-1}$ to $\pm(\omega - \omega^{-1})$. In other words, we consider the potential embeddings

$$\mathrm{id} : \begin{cases} \omega & \mapsto \omega \\ i & \mapsto i \end{cases},$$

$$\tau : \begin{cases} \omega & \mapsto \omega^{-1} \\ i & \mapsto -i \end{cases},$$

$$\varphi : \begin{cases} \omega & \mapsto -\omega \\ i & \mapsto -i \end{cases}$$

and

$$\psi : \begin{cases} \omega & \mapsto -\omega^{-1} \\ i & \mapsto i. \end{cases}$$

The first two always exist: they are the identity and the complex conjugation. The other two are more delicate. First of all, if n is odd or congruent to 2 modulo 4, then $-\omega^{\pm 1}$ is not a conjugate of ω so they do not exist. If $4 \mid n$, since $-\omega^{\pm 1} = \omega^{n/2\pm 1}$ and $\omega^{n/4}$ is i or $-i$, we must have

$$(\omega^{n/4})^{n/2\pm 1} = \pm\omega^{n/4}$$

for these embeddings to exist. This means that $\frac{n}{2} \cdot \frac{n}{4} \equiv \frac{n}{2} \pmod{n}$, i.e $\frac{n}{4}$ is odd, or in other words $n \equiv 4 \pmod 8$.

To conclude, when $8 \mid n$ we have $\varphi(\mathrm{lcm}(4, n))/N = \varphi(n)/2$, when $n \equiv 4 \pmod 8$ we have $\varphi(\mathrm{lcm}(4, n))/N = \varphi(n)/4$, and otherwise we have $\varphi(\mathrm{lcm}(4, n))/N = 2\varphi(n)/2$ as desired. (Obviously, we exclude the exceptions $1, 2, 4$.)

Exercise 3.2.6. Find all quadratic cosines.

Solution

The degree of $\cos\left(\frac{2k\pi}{n}\right)$ is 1 for $n = 1, 2$ and $\varphi(n)/2$ for $n > 2$. Indeed, when $n > 2$, the cosines $\cos\left(\frac{2k\pi}{n}\right)$ for $\gcd(k, n) = 1$ come into pairs

$$\cos\left(\frac{2k\pi}{n}\right) = \cos\left(\frac{2(n-k)\pi}{n}\right)$$

so $\cos\left(\frac{2k\pi}{n}\right)$ has half as many conjugates as the number of $\gcd(k, n) = 1$, i.e. $\varphi(n)/2$. Thus, the quadratic cosines are $\cos\left(\frac{2k\pi}{n}\right)$ for $\gcd(k, n) = 1$ and $\varphi(n)/2 \leq 2$, i.e. $n \in \{1, 2, 3, 4, 5, 6, 8\}$. ■

3.3 Orders

Exercise 3.3.1*. Let p be a rational prime and a a rational integer. Prove that, for any $n \geq 1$, $p \mid \Phi_n(a)$ if and only if $p \mid \Phi_{pn}(a)$.

Solution

It suffices to note that $\Phi_{pn}(X) \equiv \Phi_n(X)^p$ or $\Phi_n(X)^{p-1}$ modulo p by Proposition 3.1.2. ■

Exercise 3.3.2*. Let p be a rational prime. Prove that there always exists a *primitive root* or *generator* modulo p, i.e. an integer g such that g^k generates all integers $p \nmid m$ modulo p.

Solution

Primitive roots are the elements of order $p-1$, i.e. the roots of Φ_{p-1} modulo p. Since

$$\Phi_{p-1} \mid X^{p-1} - 1 = (X-1) \cdot \ldots \cdot (X-(p-1))$$

it splits in $\mathbb{F}_p$ and in particular has a root. ■

Exercise 3.3.3*. Let p be a rational prime and a, b two rational integers. Prove that $p \mid \Phi_n(a,b)$ if and only if $p \mid a, b$ or $\frac{n}{p^{v_p(n)}}$ is the order of ab^{-1} modulo p.

Solution

If $p \nmid a, b$, $\Phi_n(a,b)$ is zero modulo p if and only if $\Phi_n(ab^{-1})$ is. ■

Exercise 3.3.4*. Let p be a rational prime and a an integer of order n modulo p. Prove that $a^k \equiv 1 \pmod{p}$ if and only if $n \mid k$. Deduce that n divides $p-1$.[1]

Solution

Let $k = qn + r$ be the Euclidean division of k by n. We have

$$a^k = (a^n)^q a^r \equiv a^r$$

so $a^r \equiv 1$ but $r < n$ which means that $r = 0$ by minimality of the order. Since $a^{p-1} \equiv 1$ by Fermat's little theorem, we get $n \mid p-1$. ■

Exercise 3.3.5*. Let p be a rational prime and a, b two rational integers. Suppose that $p \mid \Phi_n(a,b)$. Prove that $p \mid a, b$, $p \equiv 1 \pmod{n}$ or p is the greatest prime factor of n.

Solution

If $p \nmid a, b$ then $\Phi_n(ab^{-1}) \equiv 0 \pmod{p}$. ■

Exercise 3.3.6*. Let p be a rational prime and a an integer. Suppose $p \mid \Phi_n(a), \Phi_m(a)$ and $n \neq m$. Prove that $\frac{m}{n}$ is a power of p.

[1] This is the mod p version of Exercise 3.1.1*. In fact the proof should be the same as it works in any *group* (see Section A.2 and Theorem 6.3.2).

Solution

a has both order $\frac{n}{p^{v_p(n)}}$ and $\frac{m}{p^{v_p(m)}}$ modulo p so $\frac{m}{n} = p^{v_p(m)-v_p(n)}$ is a power of p as wanted. ■

Exercise 3.3.7. Prove the following strengthening of Problem 3.1.1: for any integer $n \geq 0$, the number $2^{2^{n+1}} + 2^{2^n} + 1$ has at least $n+1$ **distinct** prime factors.

Solution

We have

$$2^{2^{n+1}} + 2^{2^n} + 1 = \prod_{k=0}^{n} \Phi_{3\cdot 2^k}(2)$$

and 2 is not the greatest prime factor of $3 \cdot 2^k$ neither is it congruent to 1 modulo $3 \cdot 2^k$ so can't divide $\Phi_{3\cdot 2^k}(2)$ by Corollary 3.3.1. Since $\frac{3\cdot 2^k}{3\cdot 2^{k'}}$ is a power of 2, the only possible common prime factor of $\Phi_{3\cdot 2^k}(2)$ and $\Phi_{3\cdot 2^{k'}}(2)$ is 2 but we have already shown that they were odd. Thus, each factor contributes to at least one prime factor and we have in total at least $n+1$ prime factors as wanted (we have shown in Problem 3.1.1 that they were non-trivial). ■

Remark 3.3.1

This can also be seen as a corollary of the Zsigmondy theorem: each $\Phi_{3\cdot 2^k}(2)$ brings a primitive prime factor except when $k = 1$ but $3 = \Phi_6(2)$ is still primitive compared to $7 = \Phi_3(2)$.

Exercise 3.3.8*. Let $n \geq 1$ be an integer. Prove that there exist infinitely many rational primes $p \equiv 1 \pmod{n}$.

Solution

Suppose that there were only finitely many primes $p_1, \ldots, p_k$ congruent to 1 modulo n. Consider the number $\Phi_n(np_1 \cdot \ldots \cdot p_k)$. It is congruent to ± 1 modulo $np_1 \cdot \ldots \cdot p_k$ by Exercise 3.1.3* so any prime factor of it must be congruent to 1 modulo n by Theorem 3.3.1 and distinct from $p_1, \ldots, p_k$. Since it is greater than 1 by the triangular inequality, it has a prime factor which is a contradiction. ■

3.4 Zsigmondy's Theorem

Exercise 3.4.1*. Check that the exceptions stated in Theorem 3.4.1 are indeed exceptions.

Solution

When $n = 2$ and $a + b$ is a power of 2, all prime factors of $a^2 - b^2 = (a-b)(a+b)$ either divide $a - b$ or are equal to 2 which also divide $a - b$. For $a = 2$, $b = 1$, and $n = 6$, we see that all prime factors of $2^6 - 1 = 9 \cdot 7$ divide $2^3 - 1 = 7$ and $2^2 - 1 = 3$. ■

Exercise 3.4.2*. Prove that $a^2 - b^2$ has no primitive prime factor if and only if $a + b$ is $\pm$ a power of 2.

Solution

We have already shown that $a^2 - b^2$ has no primitive prime factor if $a + b$ is a power of 2. For the converse, note that any common prime factor of $a + b$ and $a - b$ must divide $2a$ and $2b$ so must be 2 since a and b are coprime. ■

Exercise 3.4.3. Let $n \geq 3$ be an integer. Prove that Φ_n is positive on $\mathbb{R}$.

Solution

Since $\Phi_n(0) = 1 > 0$ by Exercise 3.1.3*, if $\Phi_n(x)$ were nonpositive for some real x, Φ_n would have a real root by the intermediate value theorem which would imply $n = 1$ or $n = 2$ since the only real roots of unity are 1 and -1. ■

Exercise 3.4.4. Prove that $2^{m-1} > m$ for any integer $m \geq 3$ and $2^m - 1 > 3m$ for any integer $m \geq 4$.

Solution

It suffices to prove the second inequality since, if $2^m > 3m + 1$ then $2^{m-1} > m + \frac{m+1}{2} \geq m + 1$ and we already have $2^2 > 3$. We use the binomial expansion:

$$2^m = (1+1)^m > \binom{m}{m-1} + \binom{m}{2} + \binom{m}{1} = 2m + \frac{m(m-1)}{2} > 3m + 1$$

since $m \geq 4$. ■

3.5 Exercises

Diophantine Equations

Exercise 3.5.2† (USA TST 2008)**.** Let n be a rational integer. Prove that $n^7 + 7$ is not a perfect square.

Solution

Suppose that $n^7 + 7 = m^2$. Then, by adding $121 = 11^2$ to both sides, we get $n^7 + 2^7 = m^2 + 11^2$, i.e.

$$\Phi_1(n, -2)\Phi_7(n, -2) = \Phi_4(m, 11).$$

In particular, any prime factor of the RHS must be equal to 11 or congruent to 1 modulo 4. First suppose that $11 \nmid m$. Then, we must have $n + 2 = \Phi_1(n, -2) \equiv 1 \pmod 4$, i.e. $n \equiv -1 \pmod 4$. However, we then have $n^7 + 2^7 \equiv -1 \pmod 4$ which is impossible.

Thus, 11 must divide m. Since 11 is not equal to 2 or 7 nor congruent to 1 modulo 7, it can't divide $\Phi_7(n, -2)$. Hence, it must divide $n + 2 = \Phi_1(n, -2)$. Since $v_{11}(\Phi_4(m, 11)) = 2$, we also have $v_{11}(n + 2) = 2$. But then, $n + 2$ is still congruent to 1 modulo 4, since all its prime factors are congruent to 1 modulo 4 except 11, and its v_{11} is even. Hence, we get the same contradiction as before which shows that our equation does not have any solution. ■

Exercise 3.5.5† (French TST 1 2017). Determine all positive integers a for which there exists positive integers m and n as well as positive integers $k_1, \ldots, k_m, \ell_1, \ldots, \ell_n$ such that

$$(a^{k_1} - 1) \cdot \ldots \cdot (a^{k_m} - 1) = (a^{\ell_1} + 1) \cdot \ldots \cdot (a^{\ell_n} + 1).$$

Solution

If we multiply both sides by $(a^{\ell_1} - 1) \cdot \ldots \cdot (a^{\ell_n} - 1)$, we get

$$(a^{k_1} - 1) \cdot \ldots \cdot (a^{k_m} - 1)(a^{\ell_1} - 1) \cdot \ldots \cdot (a^{\ell_n} - 1) = (a^{2\ell_1} - 1) \cdot \ldots \cdot (a^{2\ell_n} - 1).$$

If we eliminate common factors, we get an equality of the form $(a^{u_1} - 1) \cdot \ldots \cdot (a^{u_r} - 1) = (a^{v_1} - 1) \cdot \ldots \cdot (a^{v_s} - 1)$ with even v_i and disjoint $\{u_1, \ldots, u_r\}$ and $\{v_1, \ldots, v_s\}$. Now, consider $a^{\max_{i,j}(u_i, v_j)} - 1$. By the Zsigmondy theorem, unless $a = 2$ or $\max_{i,j}(u_i, v_j) \leq 2$, this has a primitive prime factor which is a contradiction since this implies that some prime divides one side of the equality but not the other. Conversely, it is easy to see that $a = 2$ works: $(2^2 - 1)^2 = 2^3 + 1$.

Now suppose that $\max_{i,j}(u_i, v_j) \leq 2$. It cannot be 1 since the u_i and v_j are disjoint. Hence, it must be 2. Since the v_j are even, this implies $u_1 = \ldots = u_r = 1$ and $v_1 = \ldots = v_s = 2$. We conclude that $(a-1)^r = (a^2 - 1)^s$, i.e. $(a-1)^{r-s} = (a+1)^s$. The gcd of $a+1$ and $a-1$ divides 2, so we must have $a - 1$ and $a + 1$ must both be powers of 2. This gives us $a = 3$. Conversely, we have $(3 - 1)^2 = (3 + 1)$.

We conclude that the only solutions are $a = 2$ and $a = 3$. ■

Divisibility Relations

Exercise 3.5.7†**.** Find all coprime positive integers a and b for which there exist infinitely many integers $n \geq 1$ such that

$$n^2 \mid a^n + b^n.$$

Solution

We shall prove that a and b work if and only if $a + b$ is not a power of 2 and $\{a, b\} \neq \{1, 2\}$. Suppose that $n^2 \mid a^n + b^n$. Let p be the smallest prime factor of n. Then, the order of ab^{-1} divides $2n$ and $p - 1$ so must be 2 by assumption, i.e. $p \mid a + b$. If $a + b$ was a power of 2, then 4 would not divide $a^n + b^n$ which would be a contradiction. Thus, $a + b$ is not a power of 2.

Now suppose $a = 2$ and $b = 1$. The previous reasoning shows that the smallest prime factor of n is 3. Let q be the second smallest prime factor (distinct from 3). Then, the order of 2 divides $2n$ and $q - 1$ so must divide 6, i.e. $q = 7$. This is impossible since the order of 2 modulo 7 is odd so 7 never divides $2^k + 1$. Thus, n has only one prime factor, i.e. it is a power of3. Clearly, n is odd, as otherwise $3 \nmid 2^n + 1$. The lifting the exponent lemma gives $v_3(2^n + 1) = v_3(n) + 1$ so that $v_3(n) \leq 1$, i.e. $n \in \{1, 3\}$. There are finitely many such integers.

Finally, suppose $a + b$ is not a power of 2 and $\{a, b\} \neq \{1, 2\}$. We shall proceed by induction on k to find an odd n that works with exactly k prime factors. We start with the solution $n = 1$ corresponding $k = 0$. Then, Zsigmondy tells us that $a^n + b^n = \frac{a^{2n} - b^{2n}}{a^n - b^n}$ has an odd prime factor p which doesn't divide n, since a prime factor $q \mid n$ divides $a^{q-1} - b^{q-1}$ (the exception was with $\{a, b\} = \{2, 1\}$ which we have ruled out). We claim that pn is also a solution:

$$n^2 \mid a^n + b^n \mid a^{np} + b^{np}$$

since p is odd, and by the lifting the exponent lemma $v_p(a^{np}+b^{np}) = 1 + v_p(a^n+b^n) \geq 2$ so p^2 divides $a^{np}+b^{np}$ as well. Since p and n are coprime, we have $(np)^2 \mid a^{np}+b^{np}$ as desired. ■

Prime Factors

Exercise 3.5.11† (ISL 2002)**.** Let $p_1, \ldots, p_n > 3$ be distinct rational primes. Prove that the number

$$2^{p_1 \cdot \ldots \cdot p_n} + 1$$

has at least 2^{2^n} distinct prime factors.

Solution

Consider the 2^n divisors of $p_1 \cdot \ldots \cdot p_n$ and order them $d_1 < \ldots < d_{2^n}$. Then, each $2^{d_i}+1 \mid 2^{p_1 \cdot \ldots \cdot p_n}+1$ gives a primitive prime factor by Zsigmondy's theorem (no exception since $p_i > 3$), so there are at least 2^n prime factors in total and thus at least 2^{2^n} divisors. ■

Exercise 3.5.12† (Problems from the Book)**.** Let $a \geq 2$ be a rational integer. Prove that there exist infinitely many integers $n \geq 1$ such that the greatest prime factor of $a^n - 1$ is greater than $n \log_a n$.

Solution

We choose $n = a^k$, so that $n \log_a n = ka^k$. We consider prime factors of $\Phi_{a^k}(a) \mid a^{a^k} - 1$. They are all congruent to 1 modulo a^k, and suppose for the sake of a contradiction that they are all less than ka^k (which is the same as being at most ka^k since they are congruent to 1 modulo a^k). Since $\Phi_{a^k}(a) < a^{a^k}$, it has at most $\frac{a^k}{k}$ prime factors since they are all greater than a^k. Let these prime factors be $k_1 a^k + 1, \ldots, k_m a^k + 1$. The key claim is that $\Phi_{a^k}(a) \equiv 1 \pmod{a^{2k}}$, but

$$\prod_{i=1}^{m} k_i a^k + 1 \equiv 1 + a^k \sum_{i=1}^{m} k_i \pmod{a^{2k}}$$

and $\sum_{i=1}^{m} k_i < km < a^k$ since each k_i is less than k and m is less than $\frac{a^k}{k}$. Thus, it remains to prove that $\Phi_{a^k}(a) \equiv 1 \pmod{a^k}$. We shall prove that this holds modulo p^{vk} for any prime power p^v which divides a.

By Proposition 3.1.2, we have

$$\Phi_{a^k}(a) = \Phi_{p(a/p^v)^k}(a^{p^{kv-1}}).$$

Since $p^{kv-1} \geq 2kv$ for sufficiently large k (in fact $k \geq 3$), modulo p^{2kv} we get

$$\Phi_{p(a/p^v)^k}(0) \equiv 1$$

as wanted. ■

Exercise 3.5.13† (Inspired by IMO 2003)**.** Let $m \geq 1$ be an integer. Prove that there is some rational prime p such that $p \nmid n^m - m$ for any rational integer n.

Solution

In fact, we prove more: if p is a prime factor of m and $k = v_p(m)$, there is some prime q such that m is not a p^kth power modulo q. For didactic purposes, we shall first do the case $k = 1$ (this whole paragraph will be about motivation, and the following paragraph will have the real proof). By Exercise 4.6.19†, m is a pth power modulo q if and only if

$$m^{\frac{q-1}{\gcd(p,q-1)}} \equiv 1 \pmod{q}.$$

In particular, we must have $q \equiv 1 \pmod{p}$, otherwise this is always true. Hence, we want to have $m^{\frac{q-1}{p}} \not\equiv 1$, i.e. the order r of m modulo q doesn't divide $\frac{q-1}{p}$, or in other words $v_p(m) = v_p(q-1)$. This suggests to try, for instance, $m = p$ and $q \not\equiv 1 \pmod{p^2}$. Hence, we want to pick a prime factor q of $\Phi_p(m)$ which is not congruent to 1 modulo p^2. If there was no such prime, we would have $\Phi_p(m)equiv1 \pmod{p^2}$ which is impossible since $\Phi_p(m) \equiv m+1 \pmod{p^2}$ and $p^2 \nmid m$.

Now, let's do the general case. The proof is almost identical: we find a prime q for which m has order p modulo q, and such that $q \not\equiv 1 \pmod{p^{k+1}}$. That way, $\frac{q-1}{\gcd(q-1,p^k)}$ is not divisible by p. Hence, if m were congruent to a $\gcd(q-1,p^k)$th power $n^{\gcd(q-1,p^k)}$ modulo p, we would have

$$m^{\frac{q-1}{\gcd(q-1,p^k)}} \equiv n^{q-1} \equiv 1$$

but the order of m doesn't divide $\frac{q-1}{\gcd(q-1,p^k)}$. To find such a prime q, consider $\Phi_p(m)$ as before. If all its prime divisors were congruent to 1 modulo p^{k+1}, we woudl have $\Phi_p(m) \equiv 1 \pmod{p^{k+1}}$ which is impossible since it is congruent to $1+m$. ■

Remark 3.5.1

This is also a consequence of (a corollary of) the Chebotarev density theorem: as said in Remark 4.6.3, it there were no such prime, m would be an $m/2$th power if $8 \mid m$, which is impossible since $2^{m/2} > m$ for $m \geq 8$, or an mth power if $8 \nmid m$, which is also impossible since $2^m > m$ for $m \geq 1$.

Exercise 3.5.14†. Prove that $\varphi(n)/n$ can get arbitrarily small. Deduce that $\pi(n)/n \to 0$, where $\pi(n)$ denotes the number of primes at most n.

Solution

We take $n = p_1 \cdot \ldots \cdot p_k$, where $p_1, \ldots, p_k$ are the first k primes. We need to prove that

$$\varphi(n) = \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) \to 0,$$

i.e.

$$\prod_p \left(1 - \frac{1}{p}\right) = 0.$$

This follows from the following equality:

$$\prod_p \frac{1}{1-p^{-1}} = \sum_{n=1}^{\infty} \frac{1}{n} = \infty.$$

To deduce that $\pi(n) = o(n)$, one can notice that there are $\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) n + o(n)$ numbers less than n which are not divisible by any of $p_1, \ldots, p_k$. ■

Exercise 3.5.15†. Let $P(n)$ denote the greatest prime factor of any rational integer $n \geq 1$ ($P(1) = 0$). Let $\varepsilon > 0$ be a real number. Prove that there exist infinitely many rational integers $n \geq 2$ such that

$$P(n-1), P(n), P(n+1) < n^{\varepsilon}.$$

Solution

We choose $n = 2^{p_1 \cdot \ldots \cdot p_k}$, where $p_1 \cdot \ldots \cdot p_k$ are the first k odd primes. It is clear that $P(n) = n^{o(1)}$. By factorisating the other two sides in cyclotomic polynomials, we get that $P(n)$ is at most

$$\max_{d \mid p_1 \cdot \ldots \cdot p_k} (\Phi_d(2), \Phi_d(-2)) \leq 3^{\varphi(p_1 \cdot \ldots \cdot p_k)} = 2^{o(p_1 \cdot \ldots \cdot p_k)}$$

since $\frac{\varphi(p_1 \cdot \ldots \cdot p_k)}{p_1 \cdot \ldots \cdot p_k} \to 0$ by Exercise 3.5.14†. ■

Exercise 3.5.16† (Brazilian Mathematical Olympiad 1995)**.** Let $P(n)$ denote the greatest prime factor of any rational integer $n \geq 1$. Prove that there exist infinitely many rational integers $n \geq 2$ such that

$$P(n-1) < P(n) < P(n+1).$$

Solution

Let p be an odd prime. Let $k \geq 0$ be the smallest integer such that $P(p^{2^k} + 1) > p$, there exists one $P(p^{2^k} + 1) \to \infty$ by Zsigmondy (one may also note that two numbers of the form $p^{2^k} + 1$ have gcd 2). Note that $k \geq 1$ since $P(p+1) < p$. We claim that $n = p^{2^k}$ works. Indeed, we have $P(p^{2^k} + 1) > p = P(p^{2^k})$ by assumption, and

$$P(p^{2^k} - 1) = P\left((p-1)\prod_{i=1}^{k-1} p^{2^i} + 1\right) < p$$

by minimality of k. ■

Exercise 3.5.18† (Structure of units of $\mathbb{Z}/n\mathbb{Z}$)**.** Let p be an odd rational prime and $n \geq 1$ and integer. Prove that there is a primitive root modulo p^n, i.e. a number g which generates all the numbers coprime with p modulo p^n. Moreover, show that there doesn't exist a primitive root mod 2^n for $n \geq 3$, but that, in that case, there exist a rational integer g and a rational integer a such that each rational integer is congruent to either g^k for some k or ag^k modulo 2^n.[2]

Solution

Let $g \in \mathbb{Z}$ be a primitive root modulo p. Then, if $g^{p-1} \not\equiv 1 \pmod{p^2}$, we have $v_p(g^{n(p-1)} - 1) = 1 + v_p(n)$ by LTE which shows that g is a primitive root modulo p^n for any n. If $g^{p-1} \not\equiv 1 \pmod{p^2}$, then $g + p$ is also a primitive root modulo p and

$$(g+p)^{p-1} \equiv g^{p-1} + p(p-1)g^{p-2} \not\equiv 1 \pmod{p^2}$$

so our previous argument shows that g is a primitive root modulo any power of p.

[2] In group-theoretic terms, this says that $(\mathbb{Z}/p^n\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(p^n)\mathbb{Z}$ and that $(\mathbb{Z}/2\mathbb{Z})^n \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z})$ for $n \geq 2$. The Chinese remainder theorem then yields

$$(\mathbb{Z}/2^n p_1^{n_1} \cdots p_m^{n_m}\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z}) \times (\mathbb{Z}/\varphi(p_1^{n_1})\mathbb{Z}) \times \ldots \times (\mathbb{Z}/\varphi(p_m^{n_m})\mathbb{Z}).$$

For $p = 2$, we have $v_p(g^n - 1) = v_p(n) + v_p(g^2 - 1) - 1 \geq v_p(n) + 2$ for even n since $8 \mid g^2 - 1$, so the order of any odd integer modulo 2^n divides $2^{n-2} < \varphi(2^n)$. However, the same argument as before shows that, if $g^2 \not\equiv 1 \pmod{16}$ (e.g $g = 3$), then g has exactly order 2^{n-2}. Then, note that powers of g are all congruent to 1 or g modulo 8, and since there are exactly 2^{n-2} such elements modulo 2^n, this means that it goes through all of them. Thus, if $a \not\equiv 1, g \pmod 8$ is odd, every element of $\mathbb{Z}/2^n\mathbb{Z}$ can be represented in exactly one way as either g^n or ag^n as wanted. ■

Coefficients of Cyclotomic Polynomials

Exercise 3.5.20†. Let $m \geq 0$ be an integer. Prove that the coefficient of X^m of Φ_n is bounded when n varies.

Solution

This follows from the formula $\Phi_n = \prod_{d|n}(X^d - 1)^{\mu(n/d)}$ of Exercise 3.5.19. Indeed, modulo X^{m+1}, all terms with $d > m$ vanish (possibly changing the sign also) and we are left with a finite number of cases. ($(X^d - 1)^{-1}$ is too be interpreted as the inverse of $X^d - 1$ modulo X^m.) ■

Remark 3.5.2

In fact, if we define $\mu(x)$ to be 0 when x is not an integer, we get

$$\Phi_n = \prod_{d=1}^{\infty}(1 - X^d)^{\mu(n/d)}$$

since the total number of times $\mu(n/d)$ is ± 1 is even, for it is 2^r where r is the number of prime factors of n. This can be used to give explicit formulas for the coefficients of Φ_n, since the coefficient $a_n(k)$ of X^k depends on the finite product

$$\prod_{d=1}^{k}(1 - X^d)^{\mu(n/d)},$$

which we can expand as

$$\prod_{d=1}^{k}\sum_{i}(-X)^{di}\binom{\mu(n/d)}{i}$$

(this is an equality of formal power series) and then extract the coefficient of X^k of this expression. For instance, we get the formulas

$$\begin{aligned} a_n(1) &= -\mu(n) \\ a_n(2) &= \frac{\mu(n)(\mu(n) - 1)}{2} - \mu(n/2) \\ a_n(3) &= \frac{\mu(n)(\mu(n) - 1)}{2} + \mu(n/2)\mu(n) - \mu(n/3). \end{aligned}$$

Exercise 3.5.21†. Let $\psi(x) = \sum_{p^\alpha \leq x} \log p$. By noticing that

$$\exp(\psi(2n + 1)) \int_0^1 x^n(1 - x)^n \, \mathrm{d}x \leq \frac{\exp(\psi(2n + 1))}{4^n},$$

prove that $\pi(n)$, the number of primes at most n, is greater than $Cn/\log n$ for some constant $C > 0$.

Solution

We have $x(1-x) \leq \frac{1}{4}$ for $x \in [0,1]$ so

$$\int_0^1 x^n(1-x)^n \, \mathrm{d}x \leq \int_0^1 \frac{1}{4^n} \, \mathrm{d}x = \frac{1}{4^n}.$$

However, since $\exp(\psi(2n+1)) = \operatorname{lcm}(1,\ldots,2n+1)$, $\exp(\psi(2n+1)) \int_0^1 x^n(1-x)^n$ is a positive integer, since if $X^n(1-X)^n = \sum_i a_i X^i$ we get

$$\int_0^1 x^n(1-x)^n \, \mathrm{d}x = \sum_i \frac{a_i}{i+1}.$$

Hence, $\exp(\psi(2n+1)) \geq 4^n$ which implies $\psi(2n+1) \geq 2n \log 2$. In particular, $\psi(2n) \geq 2(n-1)\log 2$ so $\psi(n) \geq (n-2)\log 2$ for all n. Since

$$\psi(n) = \sum_{p \leq n} \lfloor \log_p(n) \rfloor \log p = \sum_{p \leq n} \left\lfloor \frac{\log n}{\log p} \right\rfloor \log p \leq \log n \pi(n),$$

we get $\pi(n) \geq \frac{(n-2)\log 2}{\log n}$ as wanted. ■

Exercise 3.5.22†. Let $m \geq 3$ be an odd integer and suppose that $p_1 < \ldots < p_m = p$ are rational primes such that $p_1 + p_2 > p_m$ and let $n = p_1 \cdot \ldots \cdot p_m$. What are the coefficient of X^p and X^{p-2} of Φ_n? Deduce that any rational integer arises as a coefficient of a cyclotomic polynomial.[3]

Solution

By Exercise 3.5.19, we have $\Phi_n = \prod_{d|n}(X^d-1)^{\mu(n/d)}$. Modulo X^{p+1}, if $d > p+1$, $(X^d-1)^{\mu(n/d)}$ becomes -1, since n/d is always squarefree. Hence,

$$\Phi_n = \prod_{d|n}(X^d-1)^{\mu(n/d)} \equiv \frac{(X^{p_1}-1)\cdot\ldots\cdot(X^{p_m})}{X-1}$$

since we removed $2^t - (t+1)$ factors, which is even by assumption, so the sign doesn't change. Moreover, since $p_i + p_j \geq p+1$ for any i,j, we have

$$\begin{aligned}\Phi_n &= \frac{X^p-1}{X-1}(1-X^{p_1})\cdot\ldots\cdot(1-X^{p_{m-1}}) \\ &= (1+X+\ldots+X^{p-1})(1-X^{p_1}-X^{p_2}-\ldots-X^{p_{m-1}})\end{aligned}$$

so the coefficient of X^p is $-m+1$ since each monomial of the second factor has a contribution of -1 except the first one, which has no contribution since the degree of the first factor is less than p. Similarly, the coefficient of X^{p-2} is $-m+2$ since now the first monomial of the second factor has a contribution of 1 since the degree of the first factor is large enough.

Suppose for the sake of a contradiction that there are no odd primes $p_1 < \ldots < p_m = p$ such that $p_1 + p_2 > p$. In particular, if $p_1 < \ldots < p_m$, we have $p_m > 2p_1$. Hence, the number of primes between 2^k and 2^{k+1} is always less than m. As a consequence, the number of primes less than 2^k, $\pi(2^k)$, is less than kt. This contradicts Exercise 3.5.21†. This shows that any negative coefficient can be represented, and for the positive coefficients (we can trivially get 0, e.g. $\Phi_9 = X^6+X^3+1$) simply consider Φ_{2n} which is $\Phi_n(-X)$ for odd n: this negates our coefficients since p and $p-2$ are odd. ■

[3] This may come off as a bit surprising considering that all the cyclotomic polynomials we saw had only ± 1 and 0 coefficients.

Exercise 3.5.23†. Let p and q be two rational primes. Prove that the coefficients of Φ_{pq} are in $\{-1,0,1\}$.

Solution

Let a and b be positive rational integers such that $ap+bq=\varphi(pq)$, there exists scuh integers by **??**. We claim that

$$\Phi_{pq}=\left(\sum_{i=0}^{a}X^{pi}\right)\left(\sum_{j=0}^{b}X^{qj}\right)-X^{-pq}\left(\sum_{i=a+1}^{q-1}X^{pi}\right)\left(\sum_{j=b+1}^{p-1}X^{qj}\right).$$

Note that this is monic and has degree $ap+bq=\varphi(pq)$ so it suffices to show that it is zero at any primitive pqth root of unity ω. Here is a hint of motivation for this formula (which I don't find extremely convincing, if anyone has something better please contact me): we start with the equations

$$\Phi_p(\omega^q)=\sum_{i=0}^{p-1}\omega^{qi}=0$$

and

$$\Phi_q(\omega^p)=\sum_{j=0}^{q-1}\omega^{pi}=0.$$

To construct a polynomial vanishing at ω, we can consider polynomials in $\Phi_p(X^q)$ and $\Phi_q(X^p)$, but it is easy to see that this will have a degree which is too high. Then, we try splitting the sum $\Phi_p(\omega^p)$, but it is again easy to see that the degree will be too high, unless we factorise one of the parts by powers of ω. However, for this to work, we need to factorise by exactly X^{pq} (the exponent must be a multiple of pq since ω has order pq, and the higher the exponent the more cancellation is needed so the best guess is X^{pq}).

Back to the problem, it is trivial to show that our polynomial is zero at ω: we have $\sum_{i=0}^{a}\omega^{pi}=-\sum_{i=a+1}^{q-1}\omega^{pi}$ and $\sum_{j=0}^{b}\omega^{qi}=-\sum_{j=b+1}^{p-1}\omega^{qi}$ so

$$\left(\sum_{i=0}^{a}\omega^{pi}\right)\left(\sum_{j=0}^{b}\omega^{qi}\right)=\left(\sum_{i=a+1}^{q-1}\omega^{pi}\right)\left(\sum_{j=b+1}^{p-1}\omega^{qi}\right)$$

as wanted.

Finally, let us return to the original problem. Showing that Φ_{pq} has coefficients in $\{-1,0,1\}$ is now equivalent to showing that that there is at most one way to write any integer n in the form $pi+qj$ for $i\in[\![0,a]\!]$ and $j\in[\![0,b]\!]$ or in the form $pi+qj-pq$ for $i\in[\![a+1.q-1]\!]$ and $j\in[\![b+1,p-1]\!]$.

For this, note that n can be written in two ways if and only if there are distinct pairs (i,j) and (i',j') with $i,i'\in[\![0,q-1]\!]$ and $j,j'\in[\![0,p-1]\!]$ such that

$$pi+qj\equiv pi'+qj'\pmod{pq}.$$

(It is clear that two such expressions give us an equality of this form, and the converse follows from $|pi+qj-(pi'+qj')|<2pq$, although it is techncially not needed in our case.) This is equivalent to $p(i-i')\equiv q(j'-j)\pmod{pq}$, which implies that $p\mid j'-j$ so $j'=j$ and $q\mid i-i'$ so $i=i'$. This contradicts the assumption that $(i,j)\neq(i',j')$. (In fact, this a special case of the Chinese remainder theorem: the map $\psi:\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}\to\mathbb{Z}/pq\mathbb{Z}$ given by $(i,j)\mapsto pi+qj$ is bijective.) ■

Cyclotomic Fields and Fermat's Last Theorem

Exercise 3.5.24† (Sophie-Germain's Theorem)**.** Let p be a *Sophie-Germain prime*, i.e. a rational prime such that $2p+1$ is also prime. Prove that the equation $a^p + b^p = c^p$ does not have rational integer solutions $p \nmid abc$.

Solution

Suppose that $a^p + b^p = c^p$ for some coprime rational integers a, b, c such that $p \nmid abc$. Modulo $q = 2p+1$, pth powers are congruent to ± 1 or 0, so $q \mid abc$, say $q \mid c$. We have

$$\Phi_2(a,b)\Phi_{2p}(a,b) = c^p$$

and the gcd of $\Phi_2(a,b)$ and Φ_{2p} divides p by LTE and Theorem 3.3.1. Since $p \nmid c$ by assumption, the two factors are coprime and hence are both pth powers. Modulo q, this implies that $a+b$ is congruent to 0 or ± 1. The same goes for $a-c$ and $b-c$ by symmetry. Since

$$0 \equiv 2c = (a+b) - (a-c) - (b-c) \pmod{q},$$

one of $a+b$, $a-c$ and $b-c$ must be divisible by q. If it is $a-c$ or $b-c$, then $q \mid a, b, c$ contradicting the hypothesis that they are coprime. Thus, $q \mid a+b$. Since $a - c \equiv a$ and $b - c \equiv b$ are also congruent to ± 1 or 0 modulo q, we get $a \equiv -b \equiv \pm 1$, i.e. $a \equiv 1$ and $b \equiv -1$ without loss of generality. But then,

$$\Phi_{2p}(a,b) = \sum_{k=0}^{p-1} a^k(-b)^{p-1-k} \equiv p$$

which is not a pth power modulo q. This is a contradiction. ■

Exercise 3.5.25†**.** Let ω be an nth root of unity. Define $\mathbb{Q}(\omega)$ as $\mathbb{Q} + \omega\mathbb{Q} + \ldots + \omega^{n-1}\mathbb{Q}$. Prove that

$$\mathbb{Q}(\omega) \cap \mathbb{R} = \mathbb{Q}(\omega + \omega^{-1})$$

where $\mathbb{Q}(\omega + \omega^{-1}) = \mathbb{Q} + (\omega + \omega^{-1})\mathbb{Q} + \ldots + (\omega + \omega^{-1})^{n-1}\mathbb{Q}$.

Solution

Let $f(\omega) = \sum_i a_i \omega^k$ be a real element of $\mathbb{Q}(\omega)$. Note that

$$2f(\omega) = f(\omega) + f(\omega^{-1}) = \sum_i a_i(\omega^i + \omega^{-i}) \in \mathbb{Q}(\omega + \omega^{-1})$$

since $X^i + \frac{1}{X^i}$ is a polynomial with rational coefficients in $X + \frac{1}{X}$ by induction on i or by the fundamental theorem of symmetric polynomials: $X^i + \frac{1}{X^i}$ is symmetric in X and $\frac{1}{X}$ so it is a polynomial in $X + \frac{1}{X}$ and $X \cdot \frac{1}{X} = 1$. ■

Exercise 3.5.26†**.** Let ω be a primitive pth root of unity, where p is prime. Prove that the ring of integers of $\mathbb{Q}(\omega)$, $\mathcal{O}_{\mathbb{Q}(\omega)} := \mathbb{Q}(\omega) \cap \overline{\mathbb{Z}}$ is

$$\mathbb{Z}[\omega] := \mathbb{Z} + \omega\mathbb{Z} + \ldots + \omega^{n-1}\mathbb{Z}.$$

(In fact this holds for any nth root of unity but it is harder to prove.)

Solution

Suppose that $\sum_{i=0}^{p-2} a_i\omega^i = \alpha \in \overline{\mathbb{Z}}$ for some rational numbers $a_0, \dots, a_{p-2}$. Then, the same is true for its conjugates $\sum_{i=0}^{p-1} a_i\omega^{ki} = \alpha_k$. If we consider this as a system of equations, we know from Proposition C.3.7 that a_i times the determinant of $\Omega = (\omega^{ij})_{i,j\in[p-2]}$ is an algebraic integer for all i. Since this is is the Vandermonde determinant $\prod_{1\leq i<j\leq p-2} \omega^i - \omega^j$, we get

$$a_i \prod_{0\leq i\neq j\leq p-1} \omega^i - \omega^j \in \mathbb{Z}.$$

Finally, as we saw in Theorem 3.2.1, the product $\prod_{i\neq j} \omega^i - \omega^j$ is $\pm p^p$ by Exercise 3.2.2* which means that the denominator of the a_i is a power of p. To conclude, we shall prove that if $\sum_{j=0}^{p-2} b_i\omega^i$ is divisible by p, then all b_i are divisible by p, thus showing that the denominator of the a_i is in fact not divisible by p, i.e. $a_i \in \mathbb{Z}$ as desired.

Hence, suppose that $\sum_{i=0}^{p-2} b_i\omega^i \equiv 0 \pmod p$. The same is true for its conjugates, and summing them we get $(p-1)b_0 \equiv 0$, i.e. $p \mid b_0$. Since ω is invertible ($\omega^p = 1$), we can simply remove b_0, divide by ω and repeat this process to get $p \mid b_i$ for all i. ■

Exercise 3.5.27†. Let ω be a primitive pth root of unity, where p is prime. Prove that $p = u(1-\omega)^{p-1}$, where $u \in \overline{\mathbb{Z}}$ is a unit of $\overline{\mathbb{Z}}$, i.e. $1/u$ is also an algebraic integer. Deduce that $1-\omega$ is prime in $\mathbb{Q}(\omega)$.

Solution

We have

$$p = \Phi_p(1) = \prod_{k=1}^{p-1} 1 - \omega^k$$

so we want to prove that $\frac{1-\omega^k}{1-\omega}$ is a unit for every $p \nmid k$. Note that this already shows that $1-\omega$ is prime since it has prime norm (the norm of $f(\omega)$ is defined as $\prod_{k=1}^{p-1} f(\omega^k)$ and this is clearly multiplicative). We wish to show that $\frac{1-\omega}{1-\omega^k}$ is also an algebraic integer, which is true by symmetry between primitive roots of unity: if $\zeta = \omega^k$ and $\omega = \zeta^\ell$ then this is just $\frac{1-\zeta^\ell}{1-\zeta}$. ■

Exercise 3.5.28† (Kummer)**.** Let ω be a root of unity of odd prime order p and suppose ε is a unit of $\mathbb{Q}(\omega)$. Prove that $\varepsilon = \eta\omega^n$ for some $n \in \mathbb{Z}$ and $\eta \in \mathbb{R}$.

Solution

Let $\varepsilon = f(\omega)$ be a unit of $\mathbb{Q}(\omega)$. Consider $\theta = \varepsilon/\overline{\varepsilon} = f(\omega)/f(\omega^{-1})$. Then, its conjugates are $f(\omega^k)/f(\omega^{-k})$ which all have module 1, so θ is a root of unity by Kronecker's theorem 1.5.27†. We shall now analyze the roots of unity of $\mathbb{Q}(\omega)$: by Bézout, if $\zeta \in \mathbb{Q}(\omega)$ is a primitive mth root of unity, then $\xi \in \mathbb{Q}(\omega)$ where ξ is a primitive $\operatorname{lcm}(m,p)$th root of unity. Indeed,

$$\exp\left(\frac{2i\pi}{m}\right)^a \exp\left(\frac{2i\pi}{p}\right)^b = \exp\left(\frac{2i\pi}{\operatorname{lcm}(p,m)}\right)$$

where $ap + bm = \gcd(m,n)$ by Bézout's lemma. However, the degree of a primitive kpth root of unity is $\varphi(kp)$ which is always greater than $\varphi(p)$ (which is the maximum degree of an element of $\mathbb{Q}(\omega)$ by the fundamental theorem of symmetric polynomials), except when $k \leq 2$. Thus, the root of unity of $\mathbb{Q}(\omega)$ have the form $\pm\omega^k$, and this means that $\theta = \pm\omega^n$ for some n.

Without loss of generality, we may assume that n is even (by replacing it by $n+p$ if necessary). Then, consider $\eta = \varepsilon\omega^{-n/2}$. We wish to prove that it is real. By definition, $\eta/\overline{\eta} = \pm 1$, so it is

either real or purely imaginary: we want to rule the second case out. Thus, suppose that $\eta = -\overline{\eta}$. We claim that η is divisible by $1-\omega$, and thus not a unit by Exercise 3.5.27†. Since $1-\omega \mid p$, 2 is invertible modulo $1-\omega$ so it suffices to show that $2\eta = \eta - \overline{\eta}$ is divisible by $1-\omega$. Finally, if $\eta = \sum_i a_i\omega^i$ then

$$\eta - \overline{\eta} = \sum_i a_i(\omega^i - \omega^{-i})$$

which is divisible by $1-\omega$ since $1-\omega \mid 1-\omega^{2i} = \omega^i(\omega^{-i}+\omega^i)$. ■

Exercise 3.5.29†. Let $\alpha \in \mathbb{Z}[\omega]$, where ω is a primitive pth root of unity. Prove that α^p is congruent to a rational integer modulo p.

Solution

Note that

$$(a_0 + a_1\omega + \ldots + a_{p-1}\omega^{p-1})^p \equiv a_0^p + a_1^p\omega^p + \ldots + a_{p-1}^p\omega^{p(p-1)} \equiv a_1 + \ldots + a_{p-1} \pmod{p}$$

by Frobenius. ■

Exercise 3.5.30† (Kummer)**.** Let p be an odd prime and ω a primitive pth root of unity. Suppose that $\mathbb{Z}[\omega]$ is a UFD.[4] Prove that there do not exist non-zero rational integers $a, b, c \in \mathbb{Z}$ such that

$$a^p + b^p + c^p = 0.$$

(You may assume that, if a unit of $\mathbb{Z}[\omega]$ is congruent to a rational integer modulo p, it is a pth power of a unit. This is known as "Kummer's lemma". See Borevich-Shafarevich [6] or Conrad [10] for a $(1-\omega)$-adic proof of this.)

Solution

Suppose that there are non-zero coprime $a, b, c \in \mathbb{Z}$ such that $a^p + b^p = c^p$ and, without loss of generality, $p \nmid a, b$. Working in $\mathbb{Z}[\omega]$, this gives us

$$(a+b)(a+\omega p)\cdot\ldots\cdot(a+\omega^{p-1} = c^p.$$

The gcd of two factors divides $(\omega^i - 1)b$ and $(\omega^j - 1)a$ for some $p \nmid i, j$. Since $\frac{\omega^k-1}{\omega-1}$ is a unit whenever $k \nmid p$ by Exercise 3.5.27†, the gcd of two factors divides $(\omega-1)a$ and $(\omega-1)b$ so divides $\omega - 1$. Since $\omega - 1$ is prime by the same exercise, either all factors are divisible by $1-\omega$ (since $a + b\omega^k \equiv a + b \pmod{1-\omega}$) or none of them are. We will distinguish these two cases.

First, suppose that $1-\omega \nmid a+b$. This corresponds to $p \nmid c$. Then, by unique factorisation, there are units $\varepsilon_k \in \mathbb{Z}[\omega]^\times$ and elements $c_k \in \mathbb{Z}[\omega]$ such that $a + b\omega^k = \varepsilon_k c_k^p$. Consider $k = 1$ and set $\varepsilon = \varepsilon_1$ and $\overline{\varepsilon} = \omega^m\overline{\varepsilon}$ by Exercise 3.5.28†. Then, since $c_1^p \equiv \overline{c}_1^p \pmod{p}$ by Exercise 3.5.29†, we

[4] Sadly, it has been proven that $\mathbb{Z}[\omega]$ is only a UFD when $p \in \{3, 5, 7, 11, 13, 17, 19, 23\}$. This approach works however almost verbatim when the *class number* h of $\mathbb{Q}(\omega)$ is not divisible by p. The case $h = 1$ corresponds to $\mathbb{Z}[\omega]$ being a UFD. That said, it has not been proven that there exist infinitely many p such that $p \nmid h$ (but it has been conjectured to be the case), while it has been proven that there exist infinitely many p such that $p \mid h$.

have

$$\begin{aligned} a+b\omega &= \varepsilon c_1^p \\ &\equiv \varepsilon \overline{c_1^p} \\ &= \omega^m \overline{\varepsilon} \overline{c_1^p} \\ &= \omega^m \overline{a+b\omega} \\ &= a\omega^m + b\omega^{m-1}. \end{aligned}$$

Hence, $p \mid a+b\omega-a\omega^m-b\omega^{m-1}$. If $m \neq 1, 0$, then the coefficient of ω^m of this expression is a and this is not divisible by p so the expression isn't either by Exercise 3.5.26†. Similarly, when $m \neq 1, 2$, the coefficient of ω^{m+1} is b which isn't divisible by p. Thus, $m = 1$, which yields $a \equiv b \pmod{p}$. But then, by symmetry, we must also have $a \equiv -c \pmod{p}$. This implies that $0 = a^p + b^p - c^p \equiv 3a^p$ which forces $p = 3$. It is however easy to see that $a^3 + b^3 = c^3$ has no solution $3 \nmid abc$ by working modulo 9, which finishes the first case.

Now, we consider the second case. As in our proof of Theorem 2.4.1, we consider the more general equation

$$\alpha^p + \beta^p = \varepsilon(1-\omega)^{pn}\gamma^p$$

with coprime $1-\omega \nmid \alpha, \beta, \gamma \in \mathbb{Z}[\omega]$, $\varepsilon \in \mathbb{Z}[\omega]^\times$ a unit, and $n \geq 1$. Suppose that α, β, γ is a non-trivial solution with minimal n. As we saw before, the gcd of two numbers of the form $\alpha + \beta\omega^k$ is $1-\omega$. First, we prove that there are no solutions when $n = 1$. In that case, $v_{1-\omega}(\alpha+\beta\omega^k)$ must be 1 for all k, which implies that the numbers $\alpha + \beta\omega^k$ are non-zero multiplies of $1-\omega$ modulo $(1-\omega)^2$. Since there are only $p-1$ such multiples as $|\mathbb{Z}[\omega]/(1-\omega)\mathbb{Z}[\omega]^\times| = p-1$, two of them must be equal which is impossible as we saw previously. Hence, $n \geq 2$.

By replacing β by $\beta\omega^m$ for some m, we may assume that $v_{1-\omega}(\alpha+\beta\omega^k) = 1$ for all $p \nmid k$ and $v_{1-\omega}(\alpha+\beta) = p(n-1)+1$.By unique factorisation, set $\alpha + \beta\omega = \eta(1-\omega)\rho^p$ and $\alpha + \beta = \mu(1-\omega)^{p(n-1)+1}\tau^p$ for some units η, μ. Then, since

$$(\alpha+\beta\omega) + \omega(\alpha+\beta\omega^{-1}) = (\omega+1)(\alpha+\beta),$$

we get

$$\eta\rho^p + \omega\overline{\eta}\overline{\rho^p} = (\omega+1)\mu(1-\omega)^{p(n-1)}\tau^p.$$

Dividing by η and noticing that $\omega + 1 = \frac{\omega^2+1}{\omega-1}$ is a unit, this gives us an equation of the form $x^p + uy^p = v(1-\omega)^{p(n-1)}z^p$ for $1-\omega \nmid x, y, z$ and u, v units. We wish to prove that u is a pth power. This is where we use this fundamental lemma of Kummer: modulo p, u is congruent to the pth power $(-x/y)^p$ so is a pth power itself. This contradicts the minimality since $n-1 \geq 1$, so we are done. ■

Exercise 3.5.31† (Fleck's Congruences)**.** Let $n \geq 1$ be an integer, p a prime number and $q = \left\lfloor \frac{n-1}{p-1} \right\rfloor$. Prove that, for any rational integer m,

$$p^q \mid \sum_{k \equiv m \pmod{p}} (-1)^k \binom{n}{k}.$$

Solution

Let ω be a primitive pth root of unity. We use a unity root filter on the polynomial $X^{-m \pmod p}(X-1)^n$ (see Exercise A.3.9†):

$$S := \sum_{k \equiv m \pmod{p}} (-1)^k \binom{n}{k} = \frac{\sum_k \omega^{-km}(1-\omega^k)^n}{p}.$$

Now, note that the numerator is divisible by $(1-\omega)^n$. This means that $v_{1-\omega}(S) \geq n-(p-1)$ since $v_{1-\omega}(p) = p-1$ by Exercise 3.5.27† (and $1-\omega$ is prime in $\mathbb{Q}(\omega)$). Thus,

$$v_p(S) \geq \frac{v_{1-\omega}(S)}{p-1} \geq \frac{n}{p-1} - 1$$

which implies that $v_p(S) \geq \left\lceil \frac{n}{p-1} - 1 \right\rceil = \left\lfloor \frac{n-1}{p-1} \right\rfloor$ as wanted. ■

Miscellaneous

Exercise 3.5.33† (Korea Winter Program Practice Test 1 2019)**.** Find all non-zero polynomials $f \in \mathbb{Z}[X]$ such that, for any prime number p and any integer n, if $p \nmid n$, $f(n)$, the order of $f(n)$ modulo p is at most the order of n modulo p.

Solution

Let's see what the condition means: it says that, if n is a mth root of unity in $\mathbb{F}_p$, then $f(n)$ is either zero or a root of unity of order $\leq m$ in $\mathbb{F}_p$. Thus, if we remember Proposition 1.3.1, we might try to prove that the same holds over $\mathbb{C}$. In fact we only need an assertion a lot weaker than this to finish with Exercise A.3.23†, but since we can prove the general result directly with cyclotomic polynomials let's do it.

Let $k \geq 1$ be an integer and ω a complex primitive mth root of unity. Let $p \equiv 1 \pmod{m}$ be a rational prime and $z \in \mathbb{F}_p$ an element of order m. Then, $f(z)$ has order at most m (or is zero). There are infinitely many such primes, so let m' be such that for infinitely many $p \equiv 1 \pmod{k}$, $f(z)$ has order m' (or is zero). Then,

$$\prod_{\gcd(k,m')=1} f(\omega^k)\Phi_{m'}(f(\omega^k)) \equiv \prod_{\gcd(k,m')} f(z^k)\Phi_{m'}(f(z^k)) \equiv 0 \pmod{p}$$

is divisible by infinitely many primes so must be zero, i.e. $f(\omega^k) = 0$ or $\Phi_{m'}(f(\omega^k)) = 0$ for some k. We have shown our claim: $f(\omega)$ is zero or a root of unity of order $m' \leq m$.

Finally, we can use Exercise A.3.23†: its assumption is a bit weaker than what we have, but we can see that it works for any polynomial which sends infinitely many points on the unit circle to itself, which is clearly the case here. Thus, $f = \pm X^k$ for some k since real numbers of the unit circles are ± 1, and it is easily seen that $-X^k$ does not work as $f(1)$ is a root of unity of order at most 1. Conversely, it is easy to that X^k works. ■

Exercise 3.5.34† (Korea Mathematical Olympiad Final Round 2019)**.** Show that there exist infinitely many positive integers k such that the sequence $(a_n)_{n\geq 0}$ defined by $a_0 = 1$, $a_1 = k+1$ and

$$a_{n+2} = ka_{n+1} - a_n$$

for $n \geq 0$ contains no prime number.

Solution

Using Theorem C.4.1, we can see that $a_n = \frac{\alpha^n(1+\alpha)-\beta^n(1+\beta)}{\alpha-\beta}$, where α and β are the roots of the characteristic polynomial $X^2 - kX + 1$. Indeed, we have $a_0 = 1$ and $a_1 = \alpha+\beta+1 = k+1$.

Let's express this formula in a more convenient form:

$$\begin{aligned} a_n &= \frac{\alpha^n(1+\alpha) - \beta^n(1+\beta)}{\alpha - \beta} \\ &= \frac{\alpha^n(1+\alpha) - \left(\frac{1}{\alpha}\right)^n \left(1+\frac{1}{\alpha}\right)}{\alpha - \frac{1}{\alpha}} \\ &= \frac{\alpha^n(1+\alpha) - \left(\frac{1}{\alpha}\right)^n \cdot \frac{1+\alpha}{\alpha}}{\frac{(1+\alpha)(1-\alpha)}{\alpha}} \\ &= \frac{1}{\alpha^n} \cdot \frac{\alpha^{2n+1}-1}{\alpha - 1}. \end{aligned}$$

These manipulations might seem a bit random at first, but they are very simple and motivated: we have simply replaced β by $\frac{1}{\alpha}$ and simplified it as much as possible. We can now see where cyclotomic polynomials appear:

$$\frac{\alpha^{2n+1}-1}{\alpha-1} = \prod_{d|2n+1, d>1} \Phi_d(\alpha)$$

is a product of cyclotomic polynomials! Note however that this product is trivial when $2n+1=p$ is prime, and that it is a product of cyclotomic polynomials evaluated at quadratic integers, so we need to be a bit careful, but this is still a good sign. How could we transform this into a non-trivial product even when $2n+1=p$ is prime? If $\alpha = \gamma^m$ was an mth power, we would have

$$\frac{\alpha^{2n+1}-1}{\alpha-1} = \frac{\gamma^{m(2n+1)}}{\gamma^m - 1} = \prod_{d|m(2n+1), d\nmid m} \Phi_d(\gamma).$$

In particular, for $m=2$, this product is always non-trivial. Note that given a quadratic integer of norm 1 γ, we can always construct a sequence a_n associated with $\alpha = \gamma^m$, since α is also a quadratic integer of norm 1, and quadratic integers of norm 1 are exactly the roots of polynomials of the form $X^2 - kX + 1$. Now let's show that all these α work.

To show this, we take the norm of $\Phi_d(\gamma)$: if δ is the conjugate of γ, we have

$$a_n^2 = \frac{\gamma^{m(2n+1)}-1}{\gamma^m - 1} \cdot \frac{\delta^{m(2n+1)}-1}{\delta^m - 1} = \prod_{d|m(2n+1), d\nmid m} \Phi_d(\gamma)\Phi_d(\delta)$$

and $\Phi_d(\gamma)\Phi_d(\delta)$ is now a rational integer. First, we will prove that these factors are non-trivial, and then that they cannot be all equal to a rational prime, thus establishing that a_n^2 has at least two distinct prime factors so that a_n isn't prime as wanted. (Note that this last step isn't needed if we had chosen, say, $m=4$, but we prefer to give the smallest possible m.)

Without loss of generality suppose that $\gamma > \delta$. Since $\Phi_d(\delta) = \Phi_d(\gamma)/\gamma^{\varphi(n)}$, we want to have

$$\Phi_d(\gamma)^2 > \gamma^{\varphi(n)}.$$

Since $\Phi_d(\gamma) > (\gamma-1)^{\varphi(n)}$, this is true for $(\gamma-1)^2 \geq \gamma$, i.e. when $\gamma^2 + 1 = k\gamma \geq 3\gamma$. (This is not a bad result at all: for $k<3$, the roots of $X^2 - kX + 1$ are either rational or non-real so it is normal that the situation gets weirder there. In general, it is very hard to estimate the size of linear recurrences with non-real roots. For instance, that's why we have this condition on a^2-4b in Exercise 4.6.33†. See also Theorem 8.5.1.)

Now suppose that

$$\Phi_{2n+1}(\gamma)\Phi_{2n+1}(\delta) = p = \Phi_{2(2n+1)}(\gamma)\Phi_{2(2n+1)}(\delta).$$

If we were dealing with rational integers, we could say that this is impossible since $\frac{2(2n+1)}{2n+1}$ must be a power of p but $p>2$ by our previous inequalities. We are dealing with quadratic

integers instead, but it is not that different: we just use higher finite fields instead of only $\mathbb{F}_p$ (see Chapter 4). If $\eta \in \mathbb{F}_{p^2}$ is a root of $\pi_\gamma = X^2 - kX + 1$, we get

$$\Phi_{2n+1}(\eta) = \Phi_{2(2n+1)}(\eta) = 0$$

so η has order both $\frac{2n+1}{p^{v_p(2n+1)}}$ and $\frac{2(2n+1)}{p^{v_p(2(2n+1))}}$ which implies that $p = 2$ as wanted. ■

Remark 3.5.3

If $\alpha \in \mathbb{R}$ and we choose γ to be the fundamental unit of $\mathbb{Q}(\alpha)$ (which may have norm -1, see Chapter 7), the same reasoning shows that if $\alpha = \gamma^m$ and m is not an odd prime p, a_n is composite except finitely many times (if $m = p^r$ the factorisation of $a_{\frac{p^s-1}{2}}$ for $s \leq r$ is trivial). In particular, if the fundamental unit has norm -1, any α works since it has norm 1 so $2 \mid m$. Conversely, we can conjecture that, for $m = p$ an odd prime, a_n is prime infinitely many times. This is an anlogue of the conjecture that there exists infinitely many Mersenne primes.

Exercise 3.5.35[†] (Iran Mathematical Olympiad 3rd round 2018)**.** Let a and b be positive rational integers distinct from $\pm 1, 0$. Prove that there are infinitely rational primes p such that a and b have the same order modulo p. (You may assume Dirichlet's theorem.)

Solution

Without loss of generality, suppose that $a \neq b$. Note that, modulo p, if $\gcd(q, p-1) = 1$, a and a^q always have the same order. Hence, we pick a prime q and look at primes factors p of $a^q - b$. Our goal is to prove that there are infinitely many ones which is not congruent to 1 modulo q. Note that if they were all congruent to 1 modulo q, then $a^q - b$ would be congruent to 1 modulo q too so $q \mid a - b$, which is easy to avoid. The idea will be to control the (for the sake of a contradiction) finitely many primes not congruent to 1 modulo q to reach the same contradiction.

Say these primes are $p_1, \ldots, p_k$. We allow q to vary here: these are the primes p which divide at least one term of the form $a^q - b$ without being congruent to 1 modulo q. We wish to bound the p-adic valuation of $a^q - b$: for each i, depending on whether p_i divides a or not, set $m_i = v_p(a-b)+1$ in the former case and $m_i = v_p(b)+1$ in the latter. Now consider $N = \varphi(p_1^{m_1}) \cdot \ldots \cdot \varphi(p_k^{m_k})$ and a prime $q \equiv -1 \pmod{N}$ (there exists one by Dirichlet's theorem, or by Theorem 4.4.1). We have

$$a^q - b = \begin{cases} -b \pmod{p_i^{m_i}} \text{ if } p_i \mid a \\ \frac{1}{a} - b \equiv \frac{1-ab}{a} \pmod{p_i^{m_i}} \text{ otherwise.} \end{cases}$$

We have successfuly evaluated the contribution of our primes p_i: if $p = p_i \mid a$, then $v_p(a^q - b) = v_p(b)$, otherwise $v_p(a^q - b) = v_p(ab - 1)$. If all other prime factors of $a^q - b$ were congruent to 1 modulo q, we would thus have

$$a - b \equiv a^q - b \equiv \prod_{p_i \mid a} p_i^{v_p(b)} \prod_{p_i \nmid a} p_i^{v_p(ab-1)}.$$

In particular, for large q,

$$\prod_{p_i \mid a} p_i^{v_p(b)} \prod_{p_i \nmid a} p_i^{v_p(ab-1} = a - b.$$

Now, note that the only property of the p_i we have used is that every other prime factor of $a^q - b$ is congruent to 1 modulo q. Hence, we may assume that the prime factors of $ab - 1$ are among them. Since any $p \mid ab - 1$ doesn't divide a, this yields $v_p(ab-1) = v_p(a-b)$ for every $p \mid ab - 1$. Hence, $ab - 1 \mid a - b$. This is clearly impossible since $a \neq b$ and $a, b > 1$ so $|ab-1| > |a-b| > 0$.■

Remark 3.5.4

It is more natural to try this approach with $q \equiv 1 \pmod N$ at first. However, this only gives us the equality

$$a - b \equiv a^q - b \equiv \prod_{p_i | a} p_i^{v_p(b)} \prod_{p_i \nmid a} p_i^{v_p(a-b)}$$

which provides almost no information: it only yields $v_p(a-b) = v_p(b)$ for $p \mid a$ (it implies $v_p(a) \geq v_p(b)$, and by symmetry $v_p(a) = v_p(b)$, but since this is only for $p \mid \gcd(a,b)$ it is not sufficient to finish). Thus, we need to try with $q \equiv r \pmod N$. Since q is prime, r needs to be coprime with N and this can give complicated choices of r such as the smallest prime which doesn't divide N. Then, we need to evaluate $v_p(a^r - b)$, if it is larger than $v_p(a-b)$ we are done by the equality $a - b = \prod_{p_i|a} p_i^{v_p(b)} \prod_{p_i \nmid a} p_i^{v_p(a^r-b)}$, and by the same equality we are done if it smaller. Then, we can vary r so that $v_p(a^r - b) < v_p(a-b)$ but this is complicated since we need to take in account the prime factors of N and choose an r coprime. Finally, we can realise that in fact there is a very natural choice of r coprime with N apart from 1, and that is -1. This is also very good in the sense that a and $\frac{1}{a}$ are the powers of a which are the most likely to be distinct modulo p: if they aren't, we have $a \equiv a^r$ for any odd r so all other choices of r aren't better. These considerations give the above solution.

Exercise 3.5.37† (IMC 2010)**.** Let $f : \mathbb{R} \to \mathbb{R}$ be a function and $a < b$ two real numbers. Suppose that f is zero on $[a,b]$, and

$$\sum_{k=0}^{p-1} f\left(x + \frac{k}{p}\right) = 0$$

for any $x \in \mathbb{R}$ and any rational prime p. Prove that f is zero everywhere.

Solution

Let N be a positive integer that we will choose later. Define $I \subseteq \mathbb{R}[X]$ as the set of polynomials $a_n X^n + \ldots + a_0$ such that the function

$$x \mapsto \sum_{k=0}^{n} a_k f\left(x + \frac{k}{N}\right)$$

is identically zero. We claim that I is an *ideal* of $\mathbb{R}[X]$, meaning that it is closed under addition and closed under multiplication by any polynomial. The former is clear, for the latter note that multiplication by X^k corresponds to a translation (and that multiplication by constants obviously doesn't change anything to the condition). The key point about ideals is that we can take the gcd of two polynomials: indeed, if u, v are elements of I, by Bézout's lemma there exist polynomials $r, s \in \mathbb{R}[X]$ such that $ru + sv = \gcd(u,v)$, and since I is an ideal, $ru + sv \in I$.

Now, we use the second condition of the statement. This gives us that, for any rational prime $p \mid N$, the polynomial

$$u_p = 1 + X^{N/p} + X^{2N/p} \ldots + X^{(p-1)N/p} = \frac{X^N - 1}{X^{N/p} - 1}$$

is in I. Let's compute the gcd of these polynomials when p ranges through the prime factors of N: the roots of u_p are Nth roots of unity with order not dividing N/p. Thus, the gcd of the u_p is exactly the polynomials whose roots are primitive Nth roots of unity, i.e. Φ_N.

Now, since $\varphi(N)/N$ can be arbitrarily small by Exercise 3.5.14†, choose N so that $\varphi(N)/N \leq b - a$. Let x be an element of $\left[a - \frac{1}{N}, b\right]$. By definition of I, since $\Phi_N = \sum_i \phi_i X^i \in I$, we have

$$\sum_{k=0}^{\varphi(n)} \phi_i f\left(x + \frac{k}{N}\right) = 0.$$

Note that all terms in this sum are in $[a, b]$ except the first one, since

$$a \leq x + \frac{k}{N} \leq x + \frac{\varphi(N)}{N} \leq a + (b - a) = b$$

for $1 \leq k \leq \varphi(n)$. Thus, we also have $f(x) = \phi_0 f(x) = 0$, i.e. f is identically zero on $\left[a - \frac{1}{N}, b\right]$. Similarly, f is identically zero on $\left[a, b + \frac{1}{N}\right]$. By induction, f is identically zero on $\left[a - \frac{k}{N}, b + \frac{k}{N}\right]$ for any $k \in N$, i.e. f is zero on $\mathbb{R}$ as wanted. ■

Exercise 3.5.40†. Let $n \geq 1$ be an integer. Prove that $\Phi_n(x) \geq (x-1)x^{\varphi(n)-1}$ with equality if and only if $n = 1$.[5]

Solution

We clearly have equality when $n = 1$, thus assume that $n \geq 2$. We present ABCDE's solution on AoPS, see https://artofproblemsolving.com/community/c6h1596694p9917603. Write

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)},$$

by Exercise 3.5.19. We wish to prove that this product is greater than $(x-1)x^{\varphi(n)-1}$, i.e., by dividing by $x^{\varphi(n)}$, that

$$\prod_{d|n} (1 - x^{-d})^{\mu(n/d)} \geq 1 - x^{-1}.$$

Now, take the logarithm to get

$$\sum_{d|n} \mu(n/d) \log(1 - x^{-d}) \geq \log(1 - x^{-1}).$$

Recall the Taylor series of the logarithm:

$$\log(1 - y) = -\sum_{k=1}^{\infty} \frac{y^k}{k},$$

valid for $|y| < 1$. Thus, we wish to prove that

$$\sum_{k=1}^{\infty} \frac{1}{k} \sum_{d|n} \mu(n/d) x^{-kd} = \sum_{d|n} \mu(n/d) \sum_{k=1}^{\infty} \frac{x^{-kd}}{k} \leq \sum_{k=1}^{\infty} \frac{x^k}{k}.$$

Note that we exchanged the two sums thanks to absolute convergence. Finally, to show this, we will prove that each term on the left is less than the term on the right, i.e. that

$$\sum_{d|n} \mu(n/d) x^{-kd} \leq x^{-k}.$$

More specifically, we will prove that $\sum_{d|n} \mu(n/d) y^{-d} \leq y^{-1}$ for all $y \geq 2$. We distinguish a few cases.

1. n is squarefree and has an even number of prime factors, i.e. $\mu(n) = 1$. This is the most interesting case, and the one where the inequality is the sharpest. Since $\mu(n) = 1$,

$$\sum_{d|n} \mu(n/d) y^{-d} = y^{-1} - y^{-p} + \ldots,$$

[5] In particular, $\Phi_n(2) \geq 2^{\varphi(n)-1}$.

where p is the smallest prime factor of n. Now, notice that the dots have absolute value less than

$$\sum_{d=p+1}^{\infty} y^{-d} = y^{-(p+1)} \frac{1}{1-y^{-1}} \leq y^{-p}$$

since $\frac{1}{1-y} \leq 2 \leq y$. Thus, $\ldots < y^{-p}$, i.e.

$$\sum_{d|n} \mu(n/d) y^{-d} = y^{-1} - (y^{-p} + \ldots) \leq y^{-1}$$

as wanted.

2. n is squarefree and has an odd number of prime factors, i.e. $\mu(n) = -1$. In that case, we have

$$\sum_{d|n} \mu(n/d) y^{-d} = -y^{-1} + \ldots,$$

where the dots have absolute value less than

$$\sum_{d=2}^{\infty} y^{-d} = x^{-2} \frac{1}{1-y^{-1}} \leq y^{-1}$$

so

$$\sum_{d|n} \mu(n/d) y^{-d} = -y^{-1} + \ldots < 0 < y^{-1}.$$

3. n is not squarefree, i.e. $\mu(n) = 0$. In that case, we have

$$\sum_{d|n} \mu(n/d) y^{-d} \leq \sum_{d=2}^{\infty} y^{-d} = y^{-2} \frac{1-y^{-1}}{\leq} y^{-1}.$$

■

Chapter 4

Finite Fields

Exercise 4.0.1. Suppose K is a field of *characteristic zero*, i.e.

$$\underbrace{1+\ldots+1}_{n \text{ times}}$$

(where 1 is the multiplicative identity) is never zero for any $n \geq 1$. Prove that K contains (up to relabelling of the elements) $\mathbb{Q}$.[1]

Solution

We consider the following injective morphisme $\mathbb{Q} \to K$; its image will be the copy of $\mathbb{Q}$ inside K. Send $n \in \mathbb{N}$ to

$$\xi(n) = \underbrace{1+\ldots+1}_{n \text{ times}}$$

where 1 is the multiplicative identity of K. Then send $-n$ to the additive inverse $-\xi(n)$ of $\xi(n)$. Finally, send a/b to $\xi(a)/\xi(b)$. It is clear that this is a well defined morphism, and this is injective since K has characteristic zero. Indeed, by expanding we get $\xi(mn) = \xi(m)\xi(n)$ for any $m, n \in \mathbb{N}$, which means it's true for $m, n \in \mathbb{Z}$ too by adding signs where needed. In particular, if $a/b = c/d$ then $\xi(a)/\xi(b) = \xi(c)/\xi(d)$, which shows that it is well-defined. To show that it is multiplicative on all of $\mathbb{Q}$ and thus a morphism, we see that, for $a, b, c, d \in \mathbb{Z}$ with $b, d \neq 0$, we have

$$\xi(ac/bd) = \xi(a/b)\xi(c/d) \iff \frac{\xi(ac)}{\xi(bd)} = \frac{\xi(a)\xi(c)}{\xi(b)\xi(d)}$$

which is true since ξ is multiplicative on $\mathbb{Z}$. ■

Exercise 4.0.2*. Let p be a rational prime. Prove that there exists a unique field with p elements (it's $\mathbb{Z}/p\mathbb{Z}$).

Solution

First we prove that F has characteristic p. For this, we shall prove that the characteristic of a finite ring divides its cardinality, thus proving that F has characteristic 1 or p but the former is impossible since it is non-trivial. Let m be the characateristic of a ring R. Partition R into sets of the form $\{a, a+1, \ldots, a+m-1\}$. These sets either coincide or are pairwise disjointe: if $a+i = b+j$ then $\{a, \ldots, a+m-1\} = \{b, \ldots, b+m-1\}$. Thus the cardinality of R is divisible

[1] Technically, it will usually not contain $\mathbb{Q}$ because $\mathbb{Q}$ is a very specific object. Indeed, the definition of a field is extremely sensitive: if you change the set K (relabel its elements) but keep everything else the same you get a different field. In that case we say the new field is *isomorphic* to the old one. So you must prove that K contains a field isomorphic to $\mathbb{Q}$, i.e. $\mathbb{Q}$ up to relabeling of its elements.

by m since each such set has cardinality m.

Now, identify $n \in \mathbb{F}_p$ with

$$\underbrace{1 + \ldots + 1}_{n \text{ times}}.$$

This is well defined because $\mathbb{F}_p$ and F have the same characateristic, thus yields a morphism (it is clearly multiplicative and additive) between $\mathbb{F}_p$ and F, which is clearly injective. Since F and $\mathbb{F}_p$ have the same cardinality, this is an isomorphism. ■

Remark 4.0.1

What we did can be summarised as follow: use Lagrange's theorem on the additive group of F to prove that F has characteristic p, then conclude with Exercise A.2.3* that F contains a copy of $\mathbb{F}_p$ which mean that they are isomorphic since they have the same cardinality.

Exercise 4.0.3*. Prove that $F_3(i) := F_3 + iF_3$ is a field (with 9 elements). (The hard part is to prove that each element has an inverse.)

Solution

The inverse of $a + i_3 b$ is given by $\frac{a - i_3 b}{a^2 + b^2}$ since $(a + i_3 b)(a - i_3 b) = a^2 + b^2$. Note that this is well defined since $a^2 + b^2 = 0$ iff $a = b = 0$, as the polynomial $X^2 + 1$ has no root in $\mathbb{F}_3$. ■

4.1 Frobenius Morphism

Exercise 4.1.1. Why is commutativity (of R) needed?

Solution

We need R to be commutative for the binomial expansion to work: for instance, $(a + b)^2 = a^2 + ab + ba + b^2$ which is $ab + ba$ if and only if a and b commute. ■

Exercise 4.1.2*. Prove that $a_n = \alpha^n + \beta^n + \gamma^n$.

Solution

We have $1 + 1 + 1 = 3 = u_1$, $\alpha + \beta + \gamma = 0 = u_1$ by Vieta's formulas, and

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) = 2 = u_2$$

by Vieta's formulas. ■

4.2 Existence and Uniqueness

Exercise 4.2.1*. Let K be a field and $f \in K[X]$ an irreducible polynomial of degree n. Prove that

$$K(\alpha) := K + \alpha K + \ldots + \alpha^{n-1} K$$

is a field, where α is defined as a formal root of f, i.e. an object satisfying $f(\alpha) = 0$.

Solution

It is clear that $K(\alpha)$ is a commutative ring, since α^n is a linear combination of $1, \dots, \alpha^{n-1}$ by definition ($f(\alpha) = 0$) so it is closed under multiplication (the other ring axioms are obvious). Thus the tricky part is to prove that every non-zero element has an inverse. Note that this is not necessarily true if f is reducible: if $f = gh$ we have $g(\alpha)h(\alpha) = 0$ and the $g(\alpha), h(\alpha)$ could be both non-zero (keep in mind that α is just a formal object satisfying $f(\alpha) = 0$).

Let $g(\alpha)$ be a non-zero element of $K(\alpha)$, i.e. $f \nmid g$. We use Bézout's lemma in $K[X]$ ($K[X]$ is Euclidean for the degree map so Bézout too): since f is irreducible, it is coprime with g so there exist $r, s \in K[X]$ such that

$$rf + sg = 1.$$

Evaluation at α yields $s(\alpha)g(\alpha) = 1$ as wanted. ■

Remark 4.2.1

In fact, if α is a root of f, we have $K(\alpha) \sim K[X]/(f)$, where $K[X]/(f)$ means $K[X]$ modulo f. This gives a more abstract way of constructing a field extension of K where f has a root. Indeed, the element $X \in K[X]/(f)$ is a root of f: $f(X)$ is divisible by f. (Note that we treat f as an element of $K[X]/(f)[Y]$ here, i.e. a polynomial in Y with coefficients in $K[X]/(f)$ (in fact its coefficients are simply in K).)

4.3 Properties

Exercise 4.3.1*. Let a and b be positive integers and K a field. Prove that $X^a - 1$ divides $X^b - 1$ in K if and only if $a \mid b$. Similarly, if $x \geq 2$ is a rational integer, prove that $x^a - 1$ divides $x^b - 1$ in $\mathbb{Z}$ if and only if $a \mid b$.

Solution

Note that the roots of $X^a - 1$ are ath roots of unity and that these are all bth roots of unity if and only if $a \mid b$ (for instance by considering a primitive ath root of unity). Thus $X^a - 1 \mid X^b - 1$ if and only if $a \mid b$.

$x^a - 1 \mid x^b - 1$ if and only if the order of x modulo $x^a - 1$ divides b. Since x has order a modulo $x^a - 1$, this means $a \mid b$. ■

Exercise 4.3.2*. Let $f \in \mathbb{F}_p[X]$ be a polynomial of degree n. Prove that f splits over $\mathbb{F}_{p^{n!}}$.

Solution

It suffices to prove that an irreducible polynomial g of degree at most n has its roots in $\mathbb{F}_{p^{n!}}$, since any polynomial of degree n is a product of such polynomials. This is true because Corollary 4.3.3: $\deg g$ is at most n and thus divides $n!$. ■

4.4 Cyclotomic Polynomials

Exercise 4.4.1*. Prove Proposition 4.4.1.

Solution

The formula for Φ_m follows from Vieta's formulas. The formula from Φ_n follows from Proposition 3.1.2 by induction on $n/m = p^k$. ■

Exercise 4.4.2*. Let $p \nmid m$ be a positive integer. Prove that Φ_m has a root in $\mathbb{F}_{p^n}$ if and only if $m \mid p^n - 1$.

Solution

Since the order of any element of $\mathbb{F}_{p^n}$ divides $p^n - 1$ by Theorem 4.2.1, if Φ_m has a root in $\mathbb{F}_{p^n}$, since this root has order m we get $m \mid p^n - 1$. For the converse, if $m \mid p^n - 1$ then

$$\Phi_m \mid X^{p^n-1} - 1 = \prod_{a \in \mathbb{F}_{p^n}^\times} X - a.$$

The RHS splits in $\mathbb{F}_{p^n}$ so the LHS too and in particular has at least one root there. ■

Exercise 4.4.3. Prove that $p^2 \equiv 1 \pmod 9$ if and only if $p \equiv \pm 1 \pmod 9$.

Solution

$p^2 \equiv 1 \pmod 9$ iff $9 \mid p^2 - 1 = (p-1)(p+1)$. The two factors have gcd dividing 2 so are coprime with 9, so 9 divides $p^2 - 1$ iff 9 divides $p - 1$ or $p + 1$, i.e. iff $p \equiv \pm 1 \pmod 9$. ■

Exercise 4.4.4. Compute $\Psi_1, \ldots, \Psi_8$.

Solution

We have $\Psi_1 = X - 2$, $\Psi_2 = X + 2$,

$$\Psi_3\left(X + \frac{1}{X}\right) = \frac{\Phi_3}{X} = X + 1 + \frac{1}{X}$$

so $\Psi_3 = X + 1$,

$$\Psi_4\left(X + \frac{1}{X}\right) = \frac{\Phi_4}{X} = \left(X + \frac{1}{X}\right)$$

so $\Psi_4 = X$,

$$\begin{aligned}\Psi_5\left(X + \frac{1}{X}\right) &= \frac{\Phi_5}{X}^2 \\ &= X^2 + X + 1 + \frac{1}{X} + \frac{1}{X^2} \\ &= \left(X + \frac{1}{X}\right)^2 + \left(X + \frac{1}{X}\right) - 1\end{aligned}$$

so $\Psi_5 = X^2 + X - 1$,

$$\Psi_6\left(X + \frac{1}{X}\right) = \frac{\Phi_6}{X} = X - 1 + \frac{1}{X}$$

so $\Psi_6 = X - 1$,

$$\begin{aligned}\Psi_7\left(X + \frac{1}{X}\right) &= \frac{\Phi_7}{X^3} \\ &= X^3 + X^2 + X + 1 + \frac{1}{X} + \frac{1}{X^2} + \frac{1}{X^3} \\ &= \left(X + \frac{1}{X}\right)^3 + \left(X + \frac{1}{X}\right)^2 - 2\left(X + \frac{1}{X}\right) - 1\end{aligned}$$

so $\Psi_7 = X^3 + X^2 - 2X - 1$, and finally

$$\Psi_8\left(X + \frac{1}{X}\right) = \frac{\Phi_8}{X^2} = X^2 + \frac{1}{X}^2 = \left(X + \frac{1}{X}\right)^2 - 2$$

so $\Psi_8 = X^2 - 2$. ■

Exercise 4.4.5*. Let $p \neq 0$ be an integer. Prove that the numbers m/p^k with $m \in \mathbb{Z}$ and $k \in \mathbb{N}$ are dense in $\mathbb{R}$.

Solution

Let $x \in \mathbb{R}$ be a real number. Write it in base p: $x = \sum_{i=-\infty}^{N} a_i p^i$ with $a_i \in \{0, \ldots, p-1\}$. Let $\alpha = \sum_{i=-(M-1)}^{N} a_i p^i$, which is a fraction with denominator a power of p. Then,

$$\left| x - \sum_{i=-(M-1)}^{N} a_i p^i \right| < \sum_{i=-\infty}^{-M} \frac{p-1}{p^i} = \frac{p-1}{p^M} \sum_{i=-\infty}^{0} \frac{1}{p^i} = \frac{1}{p^M} \cdot \frac{p-1}{1 - \frac{1}{p}}$$

which goes to zero as $M \to \infty$, thus showing the wanted density. ■

Exercise 4.4.6*. Prove that the leading coefficient of Ψ_n is 1.

Solution

$\Psi_1 = X - 2, \Psi_2 = X + 2$ are clearly monic so assume $n > 2$. Let a be the leading coefficient of Ψ_n. Then, the leading coefficient of $\Phi_n / X^{\varphi(n)/2} = \Psi_n(X + 1/X)$ comes from $(X + 1/X)^{\varphi(n)/2}$ and is thus $aX^{\varphi(n)/2}$. Since Φ_n is monic, Ψ_n is too. ■

4.5 Quadratic Reciprocity

Exercise 4.5.1*. Prove Proposition 4.5.1.

Solution

Let g be a primitive root modulo p. a is a square modulo p if and only if it has the form g^{2k} for some k, which is exactly equivalent to $a^{\frac{p-1}{2}} = g^{k(p-1)} = 1$.

Without primitive roots, one can also do a bit of elementary counting: there are exactly $\frac{p-1}{2}$ quadratic residues (they come by pairs $x^2, (-x)^2$, since $x^2 = y^2 \iff x = \pm y$) and all quadratic

residues are roots of $X^{\frac{p-1}{2}} - 1$ by Fermat's little theorem. The quadratic non-residues must therefore be roots of

$$\frac{X^{p-1}-1}{X^{\frac{p-1}{2}}-1} = X^{\frac{p-1}{2}} + 1.$$

■

Exercise 4.5.2. Compute $\left(\frac{77}{101}\right)$.

Solution

We have

$$\begin{aligned}\left(\frac{77}{101}\right) &= \left(\frac{7}{101}\right)\left(\frac{11}{101}\right)\\ &= \left(\frac{101}{7}\right)\left(\frac{101}{1}\right)1\\ &= \left(\frac{3}{7}\right)\left(\frac{2}{11}\right)\\ &= \left(\frac{7}{3}\right)\\ &= 1.\end{aligned}$$

■

Exercise 4.5.3. Prove that $\Psi_8 = X^2 - 2$ and that $(-1)^{\frac{p^2-1}{8}} = 1$ if and only if $p \equiv \pm 1 \pmod 8$.

Solution

We have already computed Ψ_8 in Exercise 4.4.4. ■

Exercise 4.5.4*. Prove that, for any $\ell \in \mathbb{F}_q$, $g_\ell = \left(\frac{\ell}{q}\right) g$.

Solution

If $\ell = 0$ then both sides are 0. Otherwise, ℓ is invertible so

$$\left(\frac{\ell}{q}\right) g_\ell = \sum_{k \in \mathbb{F}_q} \left(\frac{k\ell}{q}\right) \omega^{k\ell} = g$$

which yields $g_\ell = \left(\frac{\ell}{q}\right) g$ since $\left(\frac{\ell}{q}\right)^2 = 1$. ■

Exercise 4.5.5*. Prove without computing g^2 that g has exactly 2 conjugates, i.e. is a quadratic number.

Solution

$\prod_i X - g_i$ has rational coefficients by the fundamental theorem of symmetric polynomials so the conjugates of g are among g and $-g$. Conversely, g and $-g$ are conjugates of g since if

$$f\left(\sum_i \left(\frac{i}{p}\right) X^i\right)$$

has a root at ω it also has a root at ω^k for $p \nmid k$. Thus, if $f(g) = 0$ then $f(g_i) = 0$ too. ■

4.6 Exercises

Dirichlet Convolutions

Exercise 4.6.1† (Dirichlet Convolution)**.** A function f from $\mathbb{N}^*$ to $\mathbb{C}$ is said to be an *arithmetic function*. Define the *Dirichlet convolution*[2] $f * g$ of two arithmetic functions f and g as

$$n \mapsto \sum_{d|n} f(d)g(n/d) = \sum_{ab=n} f(a)g(b).$$

Prove that the Dirichlet convolution is associative. In addition, prove that if f and g are *multiplicative*[3], meaning that $f(mn) = f(m)f(n)$ and $g(mn) = g(m)g(n)$ for all **coprime** $m, n \in \mathbb{N}$, then so is $f * g$.

Solution

Let f, g, h be three arithmetic functions and let $n \in \mathbb{N}^*$. Then,

$$\begin{aligned}((f*g)*h)(n) &= \sum_{cd=n} (f*g)(d)h(c) \\ &= \sum_{cd=n, ab=d} f(a)g(b)h(c) \\ &= \sum_{abc=n} f(a)g(b)h(c).\end{aligned}$$

Similarly,

$$\begin{aligned}(f*(g*h))(n) &= \sum_{ad=n} f(a)(g*h)(d) \\ &= \sum_{ad=n, bc=d} f(a)g(b)h(c) \\ &= \sum_{abc=n} f(a)g(b)h(c)\end{aligned}$$

which shows that the Dirichlet convolution is associative. Now, suppose that f and g are multiplicative and let m, n be two coprime positive integers. We have

$$(f*g)(mn) = \sum_{d|n} f(d)g\left(\frac{mn}{d}\right) \sum_{a|m, b|n} f(ab)g\left(\frac{mn}{ab}\right)$$

[2]The Dirichlet convolution appears naturally in the study of *Dirichlet series*: the product of two Dirichlet series $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ and $\sum_{n=1}^{\infty} \frac{g(n)}{n^s}$ is the Dirichlet series corresponding to the convolution of the coefficients $\sum_{n=1}^{\infty} \frac{(f*g)(n)}{n^s}$.

[3]This terminology has conflicting meanings: in algebra, it means that $f(xy) = f(x)f(y)$ for all x, y, while for arithmetic functions, it only means that $f(xy) = f(x)f(y)$ for coprime x, y.

because m and n are coprime, so each divisor of mn is a divisor of m times a divisor of n. By multiplicativity of f and g, this is

$$\sum_{a|m,b|n} f(a)f(b)g(m/a)g(n/d) = \left(\sum_{a|m} f(a)g(m/a)\right)\left(\sum_{b|n} f(b)g(m/d)\right) = (f*g)(m)(f*g)(n)$$

so $f*g$ is also multiplicative. ■

Exercise 4.6.2† (Möbius Inversion)**.** Define the *Möbius function* $\mu : \mathbb{Z}_{\geq 1} \to \{-1, 0, 1\}$ by $\mu(n) = (-1)^k$ where k is the number of prime factors of n if n is squarefree, and $\mu(n) = 0$ otherwise. Define also δ as the function mapping 1 to 1 and everything else to 0. Prove that δ is the identity element for the Dirichlet convolution: $f*\delta = \delta*f = f$ for all arithmetic functions f. In addition, prove that μ is the inverse of 1 for the Dirichlet convolution, meaning that $\mu*1 = 1*\mu = \delta$ where 1 is the function $n \mapsto 1$.[4]

Solution

The first claim is very easy: for any $n \in \mathbb{N}^*$,

$$(f*\delta)(n) = \sum_{d|n} \delta(d)f(n/d) = f(n).$$

For the second claim, note that the Möbius function is multiplicative. Hence, by Exercise 4.6.1†, $\mu*1$ is as well. This means that, to prove that $\mu*1$ is zero everywhere except at 1, we just need to prove that it's zero on prime powers. Thus, let $p^m \neq 1$ be a prime power. We have

$$(\mu*1)(p^m) = \sum_{d|p^m} \mu(d) = \mu(1) + \mu(p) = 1 - 1 = 0$$

since $\mu(p^m) = 0$ when $m \geq 2$. To finish, we also have $(\mu*1)(1) = \mu(1) = 1 = \delta(1)$. ■

Exercise 4.6.3† (Prime Number Theorem in Function Fields)**.** Prove that the number of irreducible polynomials in $\mathbb{F}_p[X]$ of degree n is

$$N_n = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

and show that this is asymptotically equivalent to $\frac{p^n}{\log_p(p^n)}$.

Solution

The fact that μ is the inverse of 1 means that the equalities $g = 1*f$ and $f = \mu*g$ are equivalent. Now, consider the number $f(n)$ of elements of $\overline{\mathbb{F}}_p$ of degree n. This is n times the number of irreducible polynomials of degree n, by grouping them by minimal polynomial. However, we also have

$$\sum_{d|n} f(d) = p^n$$

since this is the number of elements of $\mathbb{F}_{p^n}$. In other words, $f*1 = n \mapsto p^n$. This means that $f = (n \mapsto p^n)*\mu$, i.e.

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

[4] This also explains how we found the formula for Φ_n from Exercise 3.5.19

Division by n yields the formula for the number of irreducible polynomials of degree n. Now, observe that

$$\frac{p^n}{n} - N_n = \frac{1}{n} \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) p^d$$

is at most

$$\frac{1}{n} \sum_{k=1}^{\lfloor n/2 \rfloor} p^k = \frac{p^{\lfloor n/2 \rfloor + 1} - 1}{n(p-1)} = O\left(\frac{p^{n/2}}{n}\right)$$

in absolute value since the greatest strict divisor of n is at most $n/2$. We conclude that

$$N_n = \frac{p^n}{n} + O\left(\frac{p^{n/2}}{n}\right) \sim \frac{p^n}{n}.$$

■

Linear Recurrences

Exercise 4.6.4† (China TST 2008)**.** Define the sequence $(x_n)_{n \geq 1}$ by $x_1 = 2$, $x_2 = 12$ and $x_{n+2} = 6x_{n+1} - x_n$ for $n \geq 0$. Suppose p and q are rational primes such that $q \mid x_p$. Prove that, if $q \neq 2, 3$, then $q \geq 2p - 1$.

Solution

Without loss of generality, suppose that p is odd. It is easy to see that $x_n = 2 \cdot \frac{\alpha^n - \beta^n}{\alpha - \beta}$ where α and β are the roots of $X^2 - 6X + 1$. From now on we will assume α and β to be the roots of $X^2 - 6X + 1$ in $\overline{\mathbb{F}}_q$, since we are working modulo q. We have $\alpha, \beta \in \mathbb{F}_{q^2}$ and $\Phi_p(\alpha, \beta)$ by assumption. Thus, either α/β has order p unless $p = q$. If $p = q$, $x_p \equiv x_1 = 2$ so $q = 2$. Otherwise, since the order of α/β divides $q^2 - 1$, we have $p \mid q^2 - 1$, i.e. $q \equiv \pm 1 \pmod{p}$ so $q \geq 2p - 1$ as wanted since $p \pm 1$ is even. ■

Exercise 4.6.6†**.** Let $p \neq 2, 5$ be a prime number. Prove that $p \mid \mathbb{F}_{p - \varepsilon}$ where $\varepsilon = \left(\frac{5}{p}\right)$.

Solution

Let $\alpha \in \mathbb{F}_{p^2}$ be a square root of 5. The key point is that $\left(\frac{1 \pm \alpha}{2}\right)^{p - \varepsilon} = 1$. Indeed, $\left(\frac{1 \pm \alpha}{2}\right)^{\varepsilon} = \frac{1 \pm \varepsilon\alpha}{2}$ since this is clearly true when $\varepsilon = 1$, and when $\varepsilon = -1$ it's also true since $\frac{1 \pm \alpha}{2}$ times its conjugate is 1 (root of $X^2 - X - 1$). Thus,

$$F_{p - \varepsilon} \equiv \frac{\left(\frac{1+\alpha}{2}\right)^{p-\varepsilon} - \left(\frac{1-\alpha}{2}\right)^{p-\varepsilon}}{\alpha} = 0$$

as wanted. ■

Exercise 4.6.7†**.** Let $p \neq 2, 5$ be a rational prime. Prove that $p \mid F_p - \left(\frac{5}{p}\right)$.

Solution

Let $\alpha \in \mathbb{F}_{p^2}$ be a square root of 5. Then,

$$F_p \equiv \frac{(1+\alpha)^p - (1-\alpha)^p}{2^p \alpha} = \frac{(1+\alpha^p) - (1-\alpha^p)}{2\alpha} = \alpha^{p-1}$$

which is $\left(\frac{5}{p}\right)$ as $\alpha^{p-1} = 5^{\frac{p-1}{2}}$. ■

Exercise 4.6.8†. Let $m \geq 1$ be an integer and p a rational prime. Find the maximal possible period modulo $p \geq m$ of a sequence satisfying a linear recurrence of order m.

Solution

We prove that the maximum possible is $p^m - 1$. Here is a construction: let $\alpha \in \overline{\mathbb{F}}_p$ be an element of order $p^m - 1$ with conjugates $\alpha_1, \ldots, \alpha_m$, i.e. a primitive root of $\mathbb{F}_{p^m}$. Consider the sequence

$$a_n := \sum_{i=1}^{m} \alpha_i^n,$$

which takes values in $\mathbb{F}_p$ by the fundamental theorem of symmetric polynomials (and is a linear recurrence of order m). Suppose that is has period t, i.e.

$$a_{n+t} = a_n, \ a_{n+t+1} = a_{n+1}, \ldots, \quad a_{n+t+m-1} = a_{n+m-1}$$

for some m. Then, the Vandermonde determinant gives that $\alpha_i^t = \alpha_i$, by considering this as system of equations with coefficients α_i^j and solution $\alpha_i^{n+t} = \alpha_i^n$. This shows that the period is $p^m - 1$.

Now, let $\sum_{i=1}^{r} f_i(n)\alpha_i^n$ be a linear recurrence of order m (the α_i are not necessarily conjugates anymore). Suppose first that all f_i are constant. Group the α_i by their degrees $k_1, \ldots, k_s$. Since the period is at most the product of the orders of the α_i, and the order of an element of degree k divides $p^k - 1$, the period is at most

$$(p^{k_1} - 1) \cdot \ldots \cdot (p^{k_r} - 1)$$

which is at most $p^m - 1$ since $\sum_{i=1}^{s} k_i \leq m$ (there might be repeated roots so we don't necessarily have equality).

Finally, if one of the f_i is not constant anymore, then we group the α_i by their degrees as before. The difference is that, now $\sum_{i=1}^{s} k_i \leq m - 1$ (there is at least one repeated root). Since all polynomials have period dividing p, the period is at most

$$p(p^{k_1} - 1) \cdot \ldots \cdot (p^{k_r} - 1) < p^m - 1.$$

■

Remark 4.6.1

It is interesting to note that this proof also characterises the linear recurrences with maximal period. Indeed, their characteristic polynomial must be the minimal polynomial of a primitive root of $\mathbb{F}_{p^m}$ by what we have seen, and, conversely, Vandermonde shows that all such sequences have period $p^m - 1$.

Exercise 4.6.9†. Let $f \in \mathbb{Z}[X]$ be a polynomial and $(a_n)_{n\geq 0}$ be a linear recurrence of rational integers. Suppose that $f(n) \mid a_n$ for any rational integer $n \geq 0$. Prove that $\left(\frac{a_n}{f(n)}\right)$ is also a linear recurrence.[5]

Solution

Write $a_n = \sum_{i=1}^{m} f_i(n)\alpha_i^n$. We shall prove that $f \mid f_i$ for every i, thus showing the wanted result. Choose some n and a large prime p such that $p \mid f(n)$ using Theorem 5.2.1. Then consider $a_n,\ a_{n+p}, \ldots, a_{n+(m-1)p}$. These are all zero modulo p since $f(k) \mid a_k$. However, the Vandermonde determinant shows that this implies that either $f_i(n) \equiv 0$ for all i, or the determinant of α_i^{jp} is zero, i.e. $\alpha_i^p \equiv \alpha_j^p$ for some $i \neq j$. This is clearly impossible for large p since this implies

$$p \mid \prod_{i\neq j} \alpha_i\alpha_j,$$

as $\alpha_i^p - \alpha_j^p \equiv (\alpha_i - \alpha_j)^p$ by Frobenius. Thus, we get $p \mid f(n) \implies p \mid f_i(n)$ for large p. We can then use Corollary 5.4.2 (it is clear that the proof also works for $f, g \notin \mathbb{Z}[X]$) to deduce that all irreducible factors of f divide f_i for every i. Simply divide f and all f_i by these irreducible factors, and repeat the argument. ■

Polynomials and Elements of $\overline{\mathbb{F}}_p$

Exercise 4.6.11†. Let $a \in \mathbb{F}_p$ be non-zero. Prove that $X^{p^n} - X - a$ is irreducible over $\mathbb{F}_p$ if and only if $n = 1$, or $n = p = 2$.

Solution

■

Exercise 4.6.12† (ISL 2003)**.** Let $(a_n)_{n\geq 0}$ be a sequence of rational integers such that $a_{n+1} = a_n^2 - 2$. Suppose an odd rational prime p divides a_n. Prove that $p \equiv \pm 1 \pmod{2^{n+2}}$.

Solution

We prove that $f = X^2 - 2$ iterated nth times is $\Psi_{2^{n+2}}$. This means that $f^n\left(X + \frac{1}{X}\right) = \Phi_{2^{n+2}}/X^{2^n} = X^{2^n} + \frac{1}{X^{2^n}}$. Note that $f\left(X + \frac{1}{X}\right) = X^2 + \frac{1}{X^2}$ so this follows by induction. ■

Exercise 4.6.14†. Let $f \in \mathbb{F}_p[X]$ be an irreducible polynomial of odd degree. Prove that its discriminant is a square in $\mathbb{F}_p$.

Solution

The square root of the discriminant $\Delta = \left(\prod_{i<j} \alpha_i - \alpha_j\right)^2$ of a polynomial $f = \prod_{i=1}^{n} X - \alpha_i$ is

$$\sqrt{\Delta} = \pm \prod_{i<j} \alpha_i - \alpha_j.$$

[5] In fact, the Hadamard quotient theorem states that if a linear recurrence b_n always divides another linear recurrence a_n then $\left(\frac{a_n}{b_n}\right)$ is also a linear recurrence.

Thus, if this was not in $\mathbb{F}_p$, $\mathbb{F}_{p^n}$ would contain $\mathbb{F}_p(\sqrt{\Delta}) = \mathbb{F}_{p^2}$ which is impossible since $2 \nmid n$. ■

Remark 4.6.2

In particular, for $n = 3$, $\sqrt{\Delta} \in \mathbb{F}_p$ if and only if f is irreducible or splits in K.

Exercise 4.6.15† (Chevalley-Warning Theorem)**.** Let $f_1, \ldots, f_m \in \mathbb{F}_{p^k}[X_1, \ldots, X_n]$ be polynomials such that $d_1 + \ldots + d_m < n$, where d_i is the degree of f_i. Prove that, if $f_1, \ldots, f_m$ have a common root in $\mathbb{F}_{p^k}$, then they have another one.

Solution

We shall prove more strongly that the number of common roots is divisible by p. This follows from the following result: we have $\sum_{x \in \mathbb{F}_p} x^k = 0$ for $k < p - 1$ by Exercise A.3.11†, so the sum over $\mathbb{F}_p^n$ of $f(x)$ for any polynomial $f \in \mathbb{F}_p[X_1, \ldots, X_n]$ of degree less than $n(p-1)$ also vanish (since one variable must have degree less than $p - 1$). This yields our claim when applied to the polynomial

$$f = (1 - f_1^{p-1}) \cdot \ldots \cdot (1 - f_m^{p-1})$$

(the powers mean exponentiation and not iteration). Indeed, this has degree less than $n(p-1)$ by assumption, and $f(x)$ is 1 if x is a common root of $f_1, \ldots, f_m$ and 0 otherwise. ■

Squares and the Law of Quadratic Reciprocity

Exercise 4.6.19†**.** Let q be a prime power, $a \in \mathbb{F}_q^\times$ and $m \geq 1$ an integer. Prove that a is an mth power in $\mathbb{F}_q$ if and only if $a^{\frac{p-1}{\gcd(p-1,m)}} = 1$.

Solution

Let g be a primitive root of $\mathbb{F}_p^\times$. Let k be such that $a = g^k$. Then, a is an mth power if and only if there is an n such that $g^k = g^{mn}$, i.e. $k \equiv mn \pmod{p-1}$ which is equivalent to $\gcd(p-1, m) \mid k$. Finally, this is itself equivalent to $a^{\frac{p-1}{\gcd(p-1,m)}} = 1$. ■

Exercise 4.6.20†**.** Let a be a rational integer. Suppose a is quadratic residue modulo every rational prime $p \nmid a$. Prove that a is a perfect square.

Solution

Without loss of generality, suppose that $a = \varepsilon 2^n p_1 \cdot \ldots \cdot p_k$ is squarefree, where $\varepsilon = \pm 1$, $n \in \{0, 1\}$ and $p_1, \ldots, p_k$ are distinct odd primes. Suppose for the sake of a contradiction that $p_k \geq 1$. Let r be a quadratic non-residue modulo p_1. Pick a prime $p \equiv 1 \pmod{8p_2 \cdot \ldots \cdot p_k}$ and $p \equiv r \pmod{p_1}$, using Dirichlet's theorem. Then, since $p \equiv 1 \pmod 4$ we have $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ by the law of quadratic

reciprocity for any odd prime $q \neq p$, and since $p \equiv 1 \pmod 8$ we have $\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right) = 1$. Thus,

$$\begin{aligned}\left(\frac{a}{p}\right) &= \left(\frac{\varepsilon}{p}\right)\left(\frac{2}{p}\right)\left(\frac{p_1}{p}\right)\cdot\ldots\cdot\left(\frac{p_k}{p}\right)\\ &= \left(\frac{p}{p_1}\right)\cdot\ldots\cdot\left(\frac{p}{p_k}\right)\\ &= \left(\frac{r}{p_1}\right)\left(\frac{1}{p_2}\right)\cdot\ldots\cdot\left(\frac{1}{p_k}\right)\\ &= (-1)\cdot 1\cdot\ldots\cdot 1\\ &= -1\end{aligned}$$

which is a contradiction. This means that $a \in \{\pm 1, \pm 2\}$; we could simply give counterexamples to $-1, \pm 2$, but we construct arbitrarily large ones so that the problem still holds with the slightly weaker assumption that a is quadratic resideu modulo sufficiently large primes. For $a = -1$, simply pick any prime congruent to -1 modulo 4. For $a = 2$, pick a prime congruent to 3 modulo 8, and for $a = -2$, pick a prime congruent to -1 modulo 8.

Finally, we give some ways to avoid the use od Dirichlet's theorem on primes in arithmetic progressions. Instead of picking a prime $p \equiv 1 \pmod{8p_2\cdot\ldots\cdot p_k}$ and $p \equiv r \pmod{p_1}$, we could simply choose p to be such an integer with sufficiently large prime factors, and replace Legendre symbols by Jacobi symbols. ■

Remark 4.6.3

This result illustrates the celebrated Chebotarev density theorem, which implies that the set of primes p such that the polynomial $X^2 - a$ splits over $\mathbb{F}_p$ has density $\frac{1}{2}$ when it is irreducible (and of course 1 otherwise). (This can also be seen from a more careful observation of the quadratic reciprocity law and our solution of the exercise.) This theorem also implies that, if a is an nth power modulo all sufficiently primes, then it is an nth power if $8 \nmid n$, and an $\frac{n}{2}$th power otherwise (which is sharp, as shown by Exercise 4.6.21†). A note on this theorem: it does **not** imply that the density of primes p such that an irreducible polynomial f of degree n splits over $\mathbb{F}_p$ has density $\frac{1}{n}$; this depends on its Galois group (see Chapter 6).

Exercise 4.6.21†. Prove that 16 is an eighth power modulo every prime but not an eighth power in $\mathbb{Q}$.

Solution

Notice that $X^8 - 16 = (X^2 - 2)(X^2 + 2)(X^4 + 4)$. Thus, it has a root in $\mathbb{F}_p$ of 2 or -2 is a quadratic residue. Otherwise, $p \equiv 5 \pmod 8$ which implies that -4 is a fourth power in $\mathbb{F}_p$ so it has a root as well. Indeed,

$$(-1)^{\frac{p-1}{4}} = -1 = 2^{\frac{p-1}{2}} = 4^{\frac{p-1}{4}}$$

so $(-4)^{\frac{p-1}{4}} = 1$ which means that -4 is a fourth power by Exercise 4.6.19†. ■

Exercise 4.6.22†. Prove that, if a polynomial $f \in \mathbb{Z}[X]$ of degree 2 has a root in $\mathbb{F}_p$ for any rational prime p, then it has a rational root. However, show that there exists polynomials of degree 5 and 6 that have a root in $\mathbb{F}_p$ for every prime p but no rational root.[6]

[6]The Chebotarev density theorem implies that such a polynomial must be reducible. In fact it even characterises polynomials which have a root in $\mathbb{F}_p$ for every rational prime p based on the Galois groups of their splitting field (see Chapter 6). In particular, it shows that 5 and 6 are minimal.

Solution

For odd p, a quadratic polynomial $f \in \mathbb{Z}[X]$ has a root in $\mathbb{F}_p$ if and only if its discriminant Δ is a square in $\mathbb{F}_p$. Hence, Δ is a square modulo sufficiently large primes, so it is a square by Exercise 4.6.20†, i.e. f has rational roots.

For $n = 6$, the following polynomial works: $(X^2+1)(X^2+2)(X^2-2)$. Indeed, for any odd prime p, if both 2 and -1 are quadratic non-residues, then -2 is a quadratic residue (and 1 is a quadratic residue modulo 2). For $n = 5$, the following works: $(X^2 + X + 1)(X^3 - 2)$. Indeed, if $p \equiv 1 \pmod 3$ then Φ_3 has a root modulo p, and otherwise 2 is a cube modulo p by Exercise 4.6.19†.■

Exercise 4.6.23† (Jacobi Reciprocity)**.** Define the *Jacobi symbol* $\left(\frac{\cdot}{n}\right)$ of an odd positive integer n as the product

$$\left(\frac{\cdot}{p_1^{n_1}}\right) \cdot \ldots \cdot \left(\frac{\cdot}{p_k^{n_k}}\right)$$

where $n = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$ is the prime factorisation of n. Prove the following statements: for any odd m, n

- $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$.
- $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$.
- $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.

(The Jacobi symbol $\left(\frac{m}{n}\right)$ is 1 if m is quadratic residue modulo n but may also be 1 if m isn't.)

Solution

Let $m = \prod_i p_i$ (not necessarily distinct) and $n = \prod_i q_i$. Then,

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_i \left(\frac{p_i}{q_i}\right)\left(\frac{q_i}{p_i}\right) = \prod_i (-1)^{\frac{p_i-1}{2}\cdot\frac{q_i-1}{2}} = (-1)^{\sum_i \frac{p_i-1}{2}\cdot\frac{q_i-1}{2}}.$$

Thus, we want to show that $\frac{a-1}{2} + \frac{b-1}{2} = \frac{ab-1}{2} \pmod 2$ for any odd a and b, since this this implies that

$$\sum_i \frac{p_i-1}{2}\cdot\frac{q_i-1}{2} \equiv \frac{\prod_i p_i - 1}{2}\cdot\frac{\prod_i q_i - 1}{2} = \frac{m-1}{2}\cdot\frac{n-1}{2}$$

as wanted. This is equivalent to $a - 1 + b - 1 \equiv ab - 1 \pmod 4$, i.e. $4 \mid (a-1)(b-1)$ which is clearly true. Similarly, we have

$$\left(\frac{-1}{m}\right) = \prod_i \left(\frac{-1}{p_i}\right) = \prod_i (-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_i \frac{p_i-1}{2}}$$

which is $(-1)^{\frac{m-1}{2}}$ by the previous computation. Finally,

$$\left(\frac{2}{m}\right) = \prod_i \left(\frac{2}{p_i}\right) = \prod_i (-1)^{\frac{p_i^2-1}{8}} = (-1)^{\sum_i \frac{p_i^2-1}{8}}$$

so we want to show that $\frac{a^2-1}{8} + \frac{b^2-1}{8} = \frac{(ab)^2-1}{8} \pmod 2$, i.e. $16 \mid (a^2-1)(b^2-1)$ which is true.■

Exercise 4.6.24†. Suppose $a_1, \ldots, a_n$ are distinct squarefree rational integers such that

$$\sum_{i=1}^{n} b_i\sqrt{a_i} = 0$$

for some rational numbers $b_1, \ldots, b_n$. Prove that $b_1 = \ldots = b_n = 0$.

Solution

Let $p_1, \ldots, p_k$ the prime factors of the a_i. We proceed by induction on k. Write $\sum_{i=1}^{n} b_i\sqrt{a_i}$ as

$$A + B\sqrt{p_k} := A(\sqrt{p_1}, \ldots, \sqrt{p_{k-1}}) + B(\sqrt{p_1}, \ldots, \sqrt{p_{k-1}})\sqrt{p_k}$$

, where A and B are linear combinations of square roots of integers with prime factors among $p_1, \ldots, p_{k-1}$. The key point is that quadratic reciprocity gives us infinitely many primes p such that all p_i for $i < k$ are quadratic residues, while p_k isn't. This implies that $p \mid B$, and for sufficiently large p we get $B = 0$. We can then remove it and repeat the argument. Note that $A + B\sqrt{p_k}$ does not directly make sense modulo p, but if we consider square roots α_i of p_i we get that (by symmetric polynomials), for some choice of ± 1,

$$A(\pm\alpha_1, \ldots, \pm\alpha_{k-1}) + B(\pm\alpha_1, \ldots, \pm\alpha_{k-1})\alpha_k \in \mathbb{F}_p$$

(for sufficiently large p so there's no problem with the denominators of the coefficients). For the p mentioned earlier, we get that $B(\pm\alpha_1, \ldots, \pm\alpha_{k-1}) = 0$ otherwise this sum is in $\mathbb{F}_{p^2}$ and not $\mathbb{F}_p$. This implies that $B = 0$ (we see that infinitely many primes divide its norm, i.e. the product of its conjugates).

Now, we prove this key claim. The proof is the same as the solution of Exercise 4.6.20†. Pick a quadratic non-residue r and a large prime $p \equiv r \pmod{p_k}$, $p \equiv 1 \pmod{8p_1 \cdot \ldots \cdot p_k}$ (if $p_k \neq 2$, otherwise this simply corresponds to the irrationality of $\sqrt{2}$; or we can pick a prime $p \equiv 5 \pmod 8$ instead of $1 \pmod 8$). As in Exercise 4.6.20†, we can substitue our use of the quadratic reciprocity law by the Jacobi reciprocity law, although we need adapt it slightly because we used the convenient formalism of field theory (when p isn't prime, $\mathbb{Z}/p\mathbb{Z}$ is not a field, however the fundamental theorem of symmetric polynomials works in any ring). ■

Exercise 4.6.25†. Let $n \geq 2$ be an integer and p a prime factor of $2^{2^n} + 1$. Prove that $p \equiv 1 \pmod{2^{n+2}}$.

Solution

Note that, since $p \mid \Phi_{2^{n+1}}(2)$ and $n \geq 2$, $p \equiv 1 \pmod 8$ which implies that 2 is q qudratic residue modulo p. Thus, we have $2^{2^n} \equiv -1 \pmod p$ but $2^{\frac{p-1}{2}} \equiv 1 \pmod p$ which implies that $v_2\left(\frac{p-1}{2}\right) < n$, i.e. $p \equiv 1 \pmod{2^{n+2}}$. ■

Exercise 4.6.26† (USA TST 2014)**.** Find all functions $f : \mathbb{Z} \to \mathbb{Z}$ such that $(m-n)(f(m)-f(n))$ is a perfect square for all $m, n \in \mathbb{Z}$.

Solution

We shall prove that, for any prime p, if $f(a) \equiv f(b) \pmod p$ for some $a \not\equiv b \pmod b$, then f is constant modulo p. Since $(f(a)-f(b))(a-b)$ is a square, we also get that $f(a) \equiv f(b) \pmod{p^2}$. Then, since $(f(n)-f(b))(n-b)$ and $(f(n)-f(a))(n-a)$ are square, we get that, in fact, f is constant modulo p^2, by looking at the v_p. Thus, we can divide f by p^2 and give rise to another solution with a smaller value of $f(1)$. Hence, assuming we have shown this, we can assume that $f(a) \equiv f(b) \pmod p \implies a \equiv b \pmod p$. Now, suppose we are working under this assumption. Then, $f(n+1) - f(n)$ has no prime factor so must be ± 1. Moreover, since f is injective, it must be always 1 or always -1 but since $f(n+1) - f(n)$ is square, it must be always 1. Thus, $f(n) = n + c$, and if we remove the assumption that $f(1)$ was minimal, we get that all solutions have the form $f(n) = a^2(n + c)$ (and clearly these work).

Hence, suppose that $f(a) \equiv f(b) \pmod{p}$ for some $a \not\equiv b \pmod{p}$. We need to show that f is constant modulo p. Without loss of generality, suppose that $f(a) \equiv 0$ be translating f, and that $b = 0$ by translating f inside (replace f by $x \mapsto f(x+b)$). Let S be the set of integers s such that $f(s) \equiv 0 \pmod{p}$. Note that, if $f(x) \not\equiv 0$ for some $x \not\equiv 0, a$, then $xf(x)$ and $f(x)(x-a)$ are quadratic residues modulo p, and thus

$$\frac{x-a}{x}$$

too. Hence, if we choose x such that $\frac{x-a}{x} = t \iff x = \frac{a}{1-t}$ where t is a quadratic non-residue, then $f(x) \equiv 0$, since $x \equiv 0$ or a is impossible in that case. Now, note the only condition on $a \in S$ is $a \not\equiv 0$, so we can replace it by $\frac{a}{1-t}$ where t is a quadratic non-residue. This gives that $\frac{\frac{a}{1-t}}{1-t}\frac{a}{(1-t)^2}$ also satisfies these conditions, Iterating this process, we get that $\frac{a}{(1-t)^k}$ is in S for any integer k. In particular, for $k = p-2$, we have $a(1-t) \in S$. Hence, $\frac{a(1-t)}{1-\frac{1}{t}} = -at \in S$ too, since $\frac{1}{t}$ is also a quadratic non-residue. Thus, $att' = -(-at)t' \in S$ for any quadratic non-residues t, t', i.e. $ar \in S$ for any quadratic residue r.

It remains to get $ar \in S$ for quadratic non-residues r. For this, note that if we have a $b \in S$ such that $\left(\frac{b}{p}\right) = -\left(\frac{a}{p}\right)$ then we can get br for quadratic residues r and this corresponds to ar for quadratic non-residues r. If there was no such b, since $\frac{a}{1-t} \in S$, we would have $\left(\frac{1-t}{p}\right) = 1$ for any quadratic non-residue t, i.e. the set of quadratic residues would be 1 minus the set of quadratic non-residues. This is impossible since 1 is never reached by $1-t$. Thus, we have $f(x) \equiv 0$ for any $x \not\equiv 0, a$.

Finally, if $p \geq 3$, by replacing a by a $b \not\equiv 0, a$, we also get $f(x) \equiv 0$ for any $x \not\equiv 0, b$ and thus for all $x \equiv a$. Similarly, by replacing 0 by $b \not\equiv 0$, we get $f(x) \equiv 0$ for all $x \equiv 0$. If $p = 2$, by translating f (on the inside) if necessary, it suffices to show that $f(n)$ is even when n is (to also show that $f(n)$ is odd when n is). Since $nf(n)$ is a square, we have $f(n) \equiv 0$ for $n \equiv 2 \pmod{4}$. Then, since $(n-2)(f(n) - f(2))$ is a square, we get $f(n) \equiv 0 \pmod{4}$ for $n \equiv 0 \pmod{4}$. ■

Sums and Products

Exercise 4.6.27† (Tuymaada 2012)**.** Let p be an odd prime. Prove that

$$\frac{1}{0^2+1} + \frac{1}{1^2+1} + \ldots + \frac{1}{(p-1)^2+1} \equiv \frac{(-1)^{\frac{p+1}{2}}}{2} \pmod{p}$$

where the sum is taken over the k for which $k^2 + 1 \not\equiv 0$.

Solution

Note that we have the following partial fractions decomposition in $\mathbb{F}_{p^2}$:

$$\frac{1}{k^2+1} = \frac{1}{(k-i)(k+i)} = \frac{i}{2}\left(\frac{1}{k+i} - \frac{1}{k-i}\right)$$

where $i \in \mathbb{F}_{p^2}$ satisfies $i^2 = -1$. First, we treat the case $p \equiv 1 \pmod{4}$, i.e. $i \in \mathbb{F}_p$. Then, the sum is telescopic: $\frac{1}{k+i}$ cancels out with $\frac{1}{(k+2i)-i}$, except when $k = -i$. Thus, the only terms that don't cancel are $\frac{1}{2i}$ and $-\frac{1}{-2i}$, i.e. the sum is

$$\frac{i}{2} \cdot \frac{1}{i} = \frac{-1}{2}$$

as wanted.

Now, suppose $p \equiv -1 \pmod 4$. By Exercise A.3.26† and Fermat's little theorem, we have

$$\sum_{k\in\mathbb{F}_p} \frac{1}{X-k} = \frac{(X^p-X)'}{X^p-X} = -\frac{1}{X^p-X}.$$

Evaluating this at i, we get

$$\sum_{k\in\mathbb{F}_p} \frac{1}{i-k} = \frac{1}{2i}$$

since i^p is the conjugate of i, i.e. $-i$. We finally conclude that

$$\begin{aligned}\sum_{k\in\mathbb{F}_p} \frac{1}{k^2+1} &= \frac{i}{2}\left(\sum_{k\in\mathbb{F}_p} \frac{1}{k+i} - \sum_{k\in\mathbb{F}_p} \frac{1}{k-i}\right)\\ &= \frac{i}{2}\left(\frac{1}{2i} - \frac{1}{-2i}\right)\\ &= \frac{1}{2}.\end{aligned}$$

■

Remark 4.6.4

This argument can be adapted to compute

$$\sum_{k\in\mathbb{F}_p} \frac{1}{f(k)},$$

where $f \in \mathbb{F}_p[X]$ is a monic polynomial which irreducible over $\mathbb{F}_p$. Indeed, it must have distinct roots since it is irreducible: $\gcd(f, f')$ must be 1 or f, and the only way it could have a common root with its derivative at the same time is if $f' = 0$, i.e. $f = \sum_i a_i X^{pi} = \left(\sum_i a_i X^i\right)^p$ which is not irreducible. Thus,

$$\frac{1}{f} = \sum_{f(\alpha)=0} \frac{1}{f'(\alpha)(X-\alpha)}.$$

This is called the *partial fractions decomposition* of f (see also Remark C.4.1). Indeed, it is equivalent to

$$\sum_{f(\alpha)} \frac{f}{f'(\alpha)(X-\alpha)} = 1$$

which is true, since by evaluating at α we get 1 as desired by Exercise 3.2.2*, so this is a polynomial of less than $\deg f$ taking $\deg f$ times the value 1. (If this seems unmotivated, notice that there must exist such a partial fractions decomposition since the polynomials $\frac{f}{X-\alpha}$ are linearly independent, as can be seen by evaluating a linear combination at α, and then we get the precise coefficients by also evaluating at α).

This implies that

$$\begin{aligned}\sum_{k\in\mathbb{F}_p} \frac{1}{f(k)} &= \sum_{f(\alpha)=0} \frac{1}{f'(\alpha)} \sum_{k\in\mathbb{F}_p} \frac{1}{k-\alpha}\\ &= -\sum_{f(\alpha)=0} \frac{1}{f'(\alpha)(\alpha^p-\alpha)}.\end{aligned}$$

Exercise 4.6.30†. Let $n \geq 1$ be an integer. Prove that, for any rational prime p,

$$\prod_{k=1}^{p-1} \Phi_n(k) \equiv \Phi_{n/\gcd(n,p-1)}(1)^{\frac{\varphi(n)}{\varphi(n/\gcd(n,p-1))}} \pmod{p}.$$

Solution

First, notice that when we replace n by np both sides of the equality are raised to the pth or $(p-1)$th power (depending on whether $p \mid n$ or not). Thus, we may assume without loss of generality that $p \nmid n$. We have $\Phi_n = \prod_\omega X - \omega$ where the product is over the elements of order n of $\overline{\mathbb{F}}_p$. Thus,

$$\begin{aligned}\prod_{k\in\mathbb{F}_p^\times} \Phi_n(k) &= \prod_{k\in\mathbb{F}_p^\times} \prod_\omega k - \omega \\ &= \prod_\omega \prod_{k\in\mathbb{F}_p^\times} \omega - k \\ &= \prod_\omega \omega^{p-1} - 1\end{aligned}$$

since $X^{p-1}-1 = \prod_{k\in\mathbb{F}_p^\times} X-k$ (we exchanged $k-\omega$ with $\omega-k$ since this multiplies everything by $(-1)^{p-1}=1$ when p is odd and $-1=1$ when $p=2$). To conclude, we claim that each primitive $n/\gcd(n,p-1)$th root is represented exactly $\frac{\varphi(n)}{\varphi(n/\gcd(n,p-1))}$ times by ω^{p-1}, thus yielding the wanted result (when $n>2$ we can replace $\omega^{p-1}-1$ by $1-\omega^{p-1}$ since this multiplies the product by $(-1)^{\varphi(n)}=1$, and when $n \leq 2$ the product is zero).

Let $m = n/\gcd(n,p-1)$. Note that, if we fix an element of order n and write the others as power of it, this becomes equivalent to the set of elements coprime with n modulo n restricting to $\frac{\varphi(n)}{\varphi(m)}$ copies of the set of elements coprime with m modulo m. Note that the cardinalities agree:

$$\varphi(n) = \frac{\varphi(n)}{\varphi(m)} \cdot \varphi(m).$$

Thus, we only need to check that each element of $(\mathbb{Z}/mZ)^\times$ (the subset of $\mathbb{Z}/m\mathbb{Z}$ with invertible elements) is reached as many times by evaluating elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ modulo m. This is easy: if $a_1 \equiv \ldots \equiv a_k \equiv a \pmod{m}$, then $ca_1 \equiv \ldots \equiv ca_k \equiv b \pmod{m}$ for any $b \in (\mathbb{Z}/m\mathbb{Z})^\times$, where c is any element of $(\mathbb{Z}/n\mathbb{Z})^\times$ congruent to ba^{-1} modulo m. ■

Miscellaneous

Exercise 4.6.32† (Lucas's Theorem)**.** Let p be a prime number and

$$n = p^m n_m + \ldots + pn_1 + n_0$$

and

$$k = p^m k_m + \ldots + pk_1 + k_0$$

be the base p expansion of rational integers $k, n \geq 0$ (n_i and k_i can be zero). Prove that

$$\binom{n}{k} \equiv \prod_{i=0}^{m} \binom{n_i}{k_i}.$$

Solution

We have

$$(X+1)^n = \prod_{i=0}^{m}(X+1)^{n_i p^i} \equiv \prod_{i=0}^{m}(X^{p^i}+1)^{n_i}$$

and considering the coefficient of X^k yields the desired result. ■

Exercise 4.6.33† (Carmichael's Theorem)**.** Let a, b be two coprime integers such that $a^2 - 4b > 0$, and let $(u_n)_{n\geq 1}$ denote the linear recurrence defined by $u_0 = 0$, $u_1 = 1$, and

$$u_{n+2} = aU_{n+1} - bU_n.$$

Prove that for $n \neq 1, 2, 6$, u_n always have a primitive prime factor, except when $n = 12$ and $a = b = \pm 1$ (corresponding to the Fibonacci sequence).

Solution

Notice that $u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ where α and β are the roots of $X^2 - aX + b$, which are real by assumption. Thus, Carmichael's theorem is an analogue of Zsigmondy's theorem for real conjugate quadratic integers. We proceed as in the case of $\mathbb{Z}$. Note that $\Phi_n(\alpha, \beta)$ is a rational integer since it is its own conjugate has. Suppose that p is a non-primitive prime factor of $\Phi_n(\alpha, \beta)$. Since p is not primitive, p also divides $\Phi_m(\alpha, \beta)$ for some $m < n$. Consider temporarily α and β as elements of $\mathbb{F}_{p^2}$. If one of them is zero, i.e. $p \mid b$, the other must be too since

$$\Phi_m(\alpha, \beta) = \alpha^{\varphi(m)} + \beta^{\varphi(m)} + \alpha\beta(\cdots).$$

This is impossible since $p \nmid a \equiv \alpha + \beta$ as a and b are coprime. Hence, α/β is well-defined and has both order $m/p^{v_p(m)}$ and $n/p^{v_p(n)}$ which implies that $p \mid n$. Since $n/p^{v_p(n)} \mid p^2 - 1$, we conclude that p is either the greatest prime factor of n or the second greatest, since if $p < q, r \mid n$, we get $n/p^{v_p(n)} \geq qr > p^2$. This means that there are at most two non-primitive prime factors not dividing b.

The second step of the proof is to bound the p-adic valuations of $\Phi_n(\alpha, \beta)$. When p is odd, the same proof as the usual LTE works since $p \mid \Phi_{n/p}(\alpha, \beta) \mid \alpha^{n/p} - \beta^{n/p}$ so we prove the same way that

$$\frac{\alpha^n - \beta^n}{\alpha^{n/p} - \beta^{n/p}} \equiv p\alpha^n \pmod{p^2}.$$

When $p = 2$, things get trickier. Since $n/p^{v_p(n)} \mid p^2 - 1 = 3$, we need to consider the cases $n = 2^k$ and $n = 3 \cdot 2^k$. In fact, we will only consider the cases $n = 4$ and $n = 12$ since $\Phi_{2m\cdot 2^k}(\alpha, \beta) = \Phi_{2m}(\alpha^{2^k}, \beta^{2^k})$ and the coefficients of the $(X - \alpha^{2^k})(X + \beta^{2^k})$ are also coprime. Indeed, the coefficients of α^2 and β^2 are $a^2 - 2b$ and b^2 and we conclude by induction. (This also follows from ideal factorisation: if α and β are coprime, so are α^{2^k} and β^{2^k}).

We first do the easy case, $n = 4$. We wish to show that $\alpha^2 + \beta^2$ cannot be a power of 2. If we write $\alpha = u + v\sqrt{d}$ and $\beta = u - v\sqrt{d}$ with positive d, we have

$$\Phi_4(\alpha, \beta) = \alpha^2 + \beta^2 = 2(u^2 + dv^2).$$

Since $a = 2u$ and $b = u^2 - dv^2$ are coprime, either $u, v \in \mathbb{Z}$ and and $u^2 - dv^2$ is odd, so $u^2 + dv^2$ is too and can't be a power of 2 (it's greater than 1), or $2u, 2v$ are odd integers and $u^2 + dv^2 = 2u^2 - b$ is a half integer so $2(u^2 + dv^2)$ is odd and can't be a power of 2 (it's greater than 1).

Now, we treat the case where $n = 12$. We write $\alpha, \beta = u \pm v\sqrt{d}$ again. We need to determine when

$$\Phi_{12}(\alpha, \beta) = \alpha^4 - (\alpha\beta)^2 + \beta^4 = 2(u^4 + 14u^2v^2d + v^4d^2)$$

is a power of 2 or 3 times a power of 2. Since $a = 2u$ and $b = u^2 - dv^2$ are coprime, if $u, v \in \mathbb{Z}$ then $u^2 - dv^2$ but then so is $u^4 + 14u^2v^2d + v^4d^2$ so it can't be a power of 2. Hence, let $u = 2r$, $v = 2s$ with odd r, s. Then, an *absolutely miraculous* (computer) computation shows that $r^4 + 14r^2s^2d + s^4d^2$ can never be divisible by 64 for odd r, s, d. Since $d \equiv 1 \pmod 4$, it is greater than $1 + 5 \cdot 14 + 5^2 = 96$ so must be exactly 96 since this is the only integer of the form 2^k or $3 \cdot 2^k$ for some $k \leq 6$ which is greater than 70. This yields $|r| = |s| = 1$ and $d = 5$, i.e. $\{\alpha, \beta\} = \pm\left\{\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right\}$ corresponding to $a = b = \pm 1$ as desired.

To conclude, if $\Phi_n(\alpha, \beta)$ doesn't have a primitive prime factor and n is not a power of 2 or 3 times a power of 2 (we have already covered these cases), then $\Phi_n(\alpha, \beta) = p$ for some prime $p \mid n$ or $\Phi_n(\alpha, \beta) = pq$ for some distinct primes $p, q \mid n$. By Proposition 3.4.1, we have

$$pq \geq \Phi_n(\alpha, \beta) > |\alpha - \beta|^{\varphi(n)}$$

(set $q = 1$ if $\Phi_n(\alpha, \beta)$ is prime). Since $\varphi(p) = p - 1 > p/2$ and $\varphi(pq) = (p-1)(q-1) \geq pq/2$, we conclude that

$$pq > |\alpha - \beta|^{pq/2},$$

i.e. $C^N < N^2$ where $C = |\alpha - \beta|$ and $N = pq$. However, it is easy to see that, when $C > 2.2$, $C^N > N^2$ for any positive integer N.Indeed, this is true for $N \leq 4$, and for $N \geq 5$ we have

$$2^N = (1+1)^N \geq 2\binom{N}{2} + \binom{N}{1} = N^2.$$

Hence, we must have $|\alpha - \beta| \leq 2.2$. Now, notice that $|\alpha - \beta| = \sqrt{a^2 - 4b}$ so that $0 \leq a^2 - 4b \leq 2.2^2 < 5$. Since $a^2 - 4b$ is congruent to 0 or 1 modulo 4, it must be equal to 0, 1, or 4. In all these cases α and β are rational integers and we have already proven the Zsigmondy theorem for rational integers so we are done. ■

Exercise 4.6.34†. Suppose $p \equiv 2$ or $p \equiv 5 \pmod 9$ is a rational prime. Prove that the equation

$$\alpha^3 + \beta^3 + \varepsilon a\gamma^3 = 0$$

where $\varepsilon \in \mathbb{Z}[j]$ is a unit and $2 \neq a \in \{p, p^2\}$ does not have solutions in $\mathbb{Z}[j]$.

Solution

Note that $p \equiv 2 \pmod 3$ so p is prime in $\mathbb{Z}[j]$. Suppose that there is a solution $\alpha, \beta, \gamma \neq 0$, and pick one which minimises $|N(\alpha\beta\gamma)|$. In particular, α, β, γ are coprime. Rewrite the equation as

$$(\alpha + \beta)(\alpha + j\beta)(\alpha + j^2\beta) = -\varepsilon a\gamma^3.$$

Consider the numbers $x = \alpha + \beta$, $y = j\alpha + j^2\beta$ and $z = j^2\alpha + j\beta$. By assumption, $xyz = -\varepsilon a\gamma^3$. Since p^3 does not the divide the RHS, exactly one of x, y, z is divisible by a and the other ones are not divisible by p, by unique factorisation. By replacing α and β by $j^k\alpha$ and $j^k\beta$ for some k if necessary, suppose without loss of generality that it is z. Let d be the gcd of x, y, z and consider the numbers

$$\begin{cases} x/d &= \varepsilon_1 u^3 \\ y/d &= \varepsilon_2 v^3 \\ z/d &= \varepsilon_3 a w^3 \end{cases}$$

by unique factorisation. Since $x + y + z = 0$, we have

$$\varepsilon_1 u^3 + \varepsilon_2 v^3 + \varepsilon_3 a w^3 = 0,$$

i.e.

$$u^3 + \mu v^3 + \eta a w^3 = 0$$

for some units μ, η. Suppose for a moment that we manage to prove $\mu = \pm 1$. Then, we get the smaller solution

$$u^3 + (\pm v)^3 + \eta a w^3 = 0$$

for non-zero u, v, w. This implies, by assumption, that

$$\begin{aligned} |N(\alpha\beta\gamma)|^3 &\geq |N(uvw)|^3 \\ &= \left|N\left(\frac{xyz}{d^3 a}\right)\right| \\ &= \left|N\left(\frac{\gamma}{d}\right)\right|^3 \end{aligned}$$

which implies that $|N(d\alpha\beta)| \leq 1$: α and β are units. This yields the equation $\pm 1 \pm 1 + \varepsilon a \gamma^3 = 0$, which is clearly impossible since $a \nmid \pm 1 \pm 1$ as $a > 2$.

It remains to prove that $\mu = \pm 1$ from the equation $u^3 + \mu v^3 + \eta a w^3 = 0$. What else can we do to prove this apart from considering the equation modulo p? This gives us that μ is congruent to a cube modulo p. You might be wondering what the link between this problem and the theory of finite fields is. Here is the answer: since $p \equiv 2 \pmod 3$ is prime, $\mathbb{Z}[j]/p\mathbb{Z}[j] \simeq \mathbb{F}_{p^2}$ is a field with p^2 elements. Since $p \not\equiv -1 \pmod 9$, there is no primitive ninth root of unity as $9 \nmid p^2 - 1$. Hence, if μ were a primitive cube root of unity, it could not be a cube modulo p since a cube root of μ would be a primitive ninth root of unity modulo p. This implies that $\mu = \pm 1$ as wanted. ■

Exercise 4.6.35† (Class Equation of a Group Action and Wedderburn's Theorem)**.** Let G be a finite group, S a finite set, and $\cdot$ a *group action* of G on S.[7] Given an element $s \in S$, let $\mathrm{Stab}(s)$ and $\mathrm{Fix}(G)$ denote the set of elements of G fixing s and the elements of S fixed by all of G respectivelly. Finally, let $\mathcal{O}_i = Gs_i$ be the (disjoint) orbits of size greater than 1. Prove the class equation:

$$|S| = |\operatorname{Fix}(G)| + \sum_{|\mathcal{O}_i|>1} \frac{|G|}{|\operatorname{Stab}(s_i)|}.$$

Deduce Wedderburn's theorem: any finite skew field is a field.

Solution

For the first part, notice that an orbit $\mathcal{O} = Gs$ has size 1 if and only if s is fixed by all of G, i.e. is in $|\operatorname{Fix}(G)|$, and that

$$|\mathcal{O}| = |Gs| = |G/\operatorname{Stab}(s)| = \frac{|G|}{\operatorname{Stab}(s)}$$

for any s. Indeed, the map $G/\operatorname{Stab}(s) \to Gs$ sending $h\operatorname{Stab}(s)$ to the only element hs of $h\operatorname{Stab}(s)s$ is a bijection: if $gs = hs$ then $h^{-1}gs = s$ so $h^{-1}g \in \operatorname{Stab}(s)$, i.e. $g\operatorname{Stab}(s) = h\operatorname{Stab}(s)$. Thus, the class formula becomes

$$|G| = \sum_{|\mathcal{O}_i|=1} 1 + \sum_{|\mathcal{O}_i|>1} |\mathcal{O}_i|$$

which is obviously true. (See Exercise A.3.14† for the definition of the group quotient G/H.)

We now consider the second part. We consider a finite skew field F as a multiplicative group once we remove its zero element, and our goal is to prove that it is abelian. Hence, we define its center $Z = (F^\times)$ as the group of non-zero elements which commute with every other element. Note that $Z \cup \{0\}$ is a finite field, say of cardinality q. Then, F is naturally a vector space over Z, hence of cardinality q^n for some n.

[7] In other words, a map $\cdot : G \times S \to S$ such that $e \cdot s = s$ and $(gh) \cdot s = g \cdot (h \cdot s)$ for any $g, h \in G$ and $s \in S$. See also Exercise A.3.20†.

The class equation for the action of $\mathbb{F}^{-1}$ into itself defined by the conjugation $g \cdot s := gsg^{-1}$ is

$$|F^\times| = |Z| + \sum_{i=1}^{r} \frac{|F^\times|}{|C(x_i)|}$$

where $C(x)$ is the *centraliser* of x, i.e. the group of elements which commute with x. Indeed, $\mathrm{Fix}(F^\times)$ is the set of elements x such that $gxg^{-1} = x$ for any g, i.e. x commutes with every g, while $\mathrm{Stab}(x)$ is the set of g such that $gxg^{-1} = x$, i.e. elements which commute with x. Here is the key point: for any $x \in F$, $C(x) \cup \{0\}$ is a vector space over F as well since Z commutes with everything so $ZC(x) = C(x)$. This implies that its cardinality is a power of q too, say $|C(x_i)| = q^{n_i} - 1$ for some $n_i \mid n$ since $q^{n_i} - 1 \mid |F^\times| = q^n - 1$. Hence, our equation becomes

$$q^n - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{n_i} - 1}.$$

Since the sum is taken over the orbits of size greater than 1, we have $n_i < n$ so, modulo $\Phi_n(q)$, this becomes

$$0 \equiv q - 1 + 0.$$

In other words, $\Phi_n(q)$ divides $q-1$. Since $\Phi_n(q) \geq (q-1)^{\varphi(n)}$ with equality iff $n = 1$, we conclude that $n = 1$, i.e. $F^\times = Z$ is commutative! ■

Chapter 5

Polynomial Number Theory

5.1 Factorisation of Polynomials

Exercise 5.1.1*. Prove that the content is well-defined: $c(Nf)/|N| = c(Mf)/|M|$ for any non-zero $M, N \in \mathbb{Z}$ such that $Nf, Mg \in \mathbb{Z}[X]$.

Solution

Assume without loss of generality that M and N are positive. rf has integer coefficients if and only if r is divisible by the lcm of the denominators of the coefficients of f. Thus it suffices to prove the result for $f, g \in \mathbb{Z}[X]$. Indeed, if we write $N = mN'$ and $M = mM'$ where m is the lcm of the denominators of the coefficients, we have

$$Mc(Nf) = Nc(Mf) \iff M'c(N'g) = N'c(M'g)$$

where $g = mf$ has integer coefficients. This follows from the fact that $c(rg) = rc(g)$ for any $r \in \mathbb{Z}$ (when you multiply all coefficients by r, the gcd also gets multiplied by r). ■

Exercise 5.1.2*. Suppose $f \in \mathbb{Q}[X]$ has integral content. Prove that f has integer coefficients.

Solution

Write $f = g/N$ with $f \in \mathbb{Z}[X]$ and $0 \neq N \in \mathbb{Z}$.The content of f for is $c(g)/N$. This is an integer iff N divides $c(g)$, i.e. N divides all coefficients of g, which is equivalent to $f = g/N$ having integer coefficients. ■

Exercise 5.1.3*. Prove Proposition 5.1.2.

Solution

Write $g = f^*h$. Then $c(h) = c(g) \in \mathbb{Z}$. Thus $h \in \mathbb{Z}[X]$. ■

Exercise 5.1.4*. Prove Corollary 5.1.2.

Solution

Consider the factorisation into irreducible polynomials of f in $\mathbb{Q}[X]$: $f = af_1 \cdot \ldots \cdot f_k$. The factorisation of f in $\mathbb{Z}[X]$ is then given as follow: replace each f_i by its primitive part $f_i^* = f_i/c(f_i) \in \mathbb{Z}[X]$. The multiplicative constant is then $c(f) \in \mathbb{Z}$ by Gauss's lemma. The uniqueness of the factorisation in $\mathbb{Q}[X]$ shows that this factorisation in $\mathbb{Z}[X]$ is unique too (each primitive irreducible factor must be a constant times an irreducible factor occuring in the factorisation in $\mathbb{Q}[X]$). ■

Exercise 5.1.5. Prove that Φ_{p^n} is irreducible with Eisenstein's criterion.

Solution

We have

$$\Phi_{p^n} = \frac{X^{p^n}-1}{X^{p^{n-1}}-1} \equiv (X-1)^{p^n-p^{n-1}} \pmod{p}$$

by Proposition 3.1.1 and Frobenius. Thus, $\Phi_{p^n}(X+1)$ has all its coefficients divisible by p except the leading one. Moreover, $\Phi_{p^n}(1) = p$ by expanding the division, which is not divisible by p^2. Hence, by Eisenstein's criterion, $\Phi_{p^n}(X+1)$ is irreducible and thus Φ_{p^n} too. ■

5.2 Prime Divisors of Polynomials

Exercise 5.2.1*. Why does CRT imply that there is a value reached 2^m times modulo $p_1 \cdot \ldots \cdot p_m$?

Solution

For each p_i, there is a value which is reached twice: $N_i = f(a_i) \equiv f(b_i) \pmod{p_i}$. Thus, the value congruent to N_i modulo p_i for $i = 1, \ldots, m$ is reached by m as long as $m \in \{a_i, b_i\} \pmod{p_i}$ for each b_i. There are two choices for each p_i, so 2^m possible systems of congruence, and by CRT all of these systems have a solution modulo $p_1 \cdot \ldots \cdot p_m$. ■

Exercise 5.2.2. Prove that $X - v$ works iff $0 \leq v \geq -2022$, and $-X + v$ works iff $0 \leq v \leq 2022$.

Solution

Without loss of generality, suppose $f = X - v$ by multiplying f by -1 if necessary. Note that, for $0 < a, b \leq n$, we have

$$||f(a)| - |f(b)|| \leq |f(a) - f(b)| < n$$

so the only pairs which work are those for which $|f(a)| = |f(b)|$. Since $a < b$, this means that $a < v$ and $b > v$ (they must lie in different affine parts). Thus we have $v - a = b - v$, i.e. $b = 2v - a$. This is indeed greater than $2a - a = a$ and less than n for sufficiently large n. Thus, for sufficiently large n, there are exactly $v - 1$ solutions and for smaller n there may be less. This means that our solutions are those for which $v - 1 \leq 2021$, i.e. $v \leq 2022$ as wanted. ■

5.3 Hensel's Lemma

Exercise 5.3.1*. Let p be an odd prime and a a quadratic residue modulo p. Prove that a is a quadratic residue modulo p^n, i.e. a square modulo p^n (coprime with p^n), for any positive integer n.

Solution

We apply Hensel's lemma on the polynomial $X^2 - a$. It has a root α by assumption, and the derivative 2α is not divisible by p since p is odd and $p \nmid a$. ■

Exercise 5.3.2*. Prove that an odd rational integer $a \in \mathbb{Z}$ is a quadratic residue modulo 2^n for $n \geq 3$ if and only if $a \equiv 1 \pmod 8$.

Solution

Since the only odd square modulo 8 is 1, we must have $a \equiv 1 \pmod 8$. For the converse, we consider the polynomial

$$\frac{(2Y+1)^2 - a}{4} = Y^2 + Y - \frac{a-1}{4}.$$

It has a root modulo 2 (e.g. 0) since $\frac{a-1}{4}$ is even, and its derivative is 1 which is indeed non-zero so we can use Hensel's lemma. ■

5.4 Bézout's Lemma

Exercise 5.4.1*. Prove Corollary 5.4.1.

Solution

Just multiply u and v in Proposition 5.4.1 by the lcm N of the denominators of their coefficients to get something in $\mathbb{Z}[X]$. ■

5.5 Exercises

Algebraic Results

Exercise 5.5.1†. Suppose $f, g \in \mathbb{Z}[X]$ are polynomials such that $f(n) \mid g(n)$ for infinitely many rational integers $n \in \mathbb{Z}$. Prove that $f \mid g$. In addition, generalise the previous statement to $f, g \in \mathbb{Z}[X_1, \ldots, X_m]$ such that $f(x) \mid g(x)$ fo $x \in S_1 \times \ldots \times S_n$, where $S_1, \ldots, S_n \subseteq \mathbb{Z}$ are infinite sets.

Solution

We have seen in Corollary 5.4.2 that this holds when the assumption $f(n) \mid g(n)$ is true for sufficiently large n (divide f and g by a primitive irreducible factor of f and repeat this process). To prove this stronger result, we will use a different method, a completely analytical one. Let $g = qf + r$ be the Euclidean division of g by f, and let $N \in \mathbb{Z}$ be a non-zero integer such that $Nq, Nr \in \mathbb{Z}[X]$. Then,

$$f(n) \mid Ng(n) - Nq(n)f(n) = Nr(n)$$

for infinitely many integers n. However, $\lim_{|n|\to\infty} \frac{Nr(n)}{f(n)} = 0$. Since it's a sequence of rational integers, it must be zero for sufficiently large n, which implies that $r = 0$, i.e. $f \mid g$.

For the second part, we proceed by induction on m (we have just done the case $m = 1$). If we fix x_m, we get that $f(X_1, \ldots, X_{m-1}, x_m) \mid g(X_1, \ldots, X_m, x_m)$ for any $x_m \in S_m$. Suppose that some irreducible factor π of f doesn't divide g (if all of them do we can divide f and g by them and repeat the argument, as we outlined in the first part). Note that this makes sense as $\mathbb{Z}[X_1, \ldots, X_m]$

is a UFD by Proposition 5.1.3. We shall use Bézout's lemma in $\mathbb{Q}(X_1,\dots,X_{m-1})[X_m]$ to get two polynomials $u,v\in\mathbb{Z}[X_1,\dots,X_m]$ such that

$$0\neq u\pi+vg=h\in\mathbb{Z}[X_1,\dots,X_{m-1}]$$

(by clearing denominators in the Bézout relation). We know that this h is divisible by $\pi(X_1,\dots,X_{m-1},n)$ for any infinitely many n. Since h has a finite number of divisors in $\mathbb{Z}[X_1,\dots,X_{m-1}]$, we get $\pi(X_1,\dots,X_{m-1},n)=d$ for a fixed d and infinitely many n. Thus, the polynomial $\pi(X_1,\dots,X_{m-1},X)-d$ has infinitely many roots so is identically zero, i.e. $\pi(X_1,\dots,X_{m-1},X_m)$ is constant in X_m. In that case, we can proceed by induction on $\deg_{X_m} g$: we have $\pi\mid g(k)$ for some k so we

$$\pi\mid\frac{g(X_1,\dots,X_{m-1},n)-g(k)}{n}$$

for any $n\in\mathbb{Z}$, and this has a smaller degree in n. ■

Exercise 5.5.2†. Let $f\in\mathbb{Q}[X]$ be a polynomial. Suppose that f always takes values which are mth powers in $\mathbb{Q}$. Prove that f is the mth power of a polynomial with rational coefficients. More generally, find all polynomials $f\in\mathbb{Q}[X_1,\dots,X_m]$ such that $f(x_1,\dots,x_m)$ is a (non-trivial) perfect power for any $(x_1,\dots,x_m)\in\mathbb{Z}^m$.

Solution

Without loss of generality, suppose $f\in\mathbb{Z}[X]$. Let $f=a\prod_{i=1}^k\pi_i^{r_i}$ be the factorisation of f in primitive irreducible polynomials. As stated in **??**, for any i, we can find an n and a prime p such that $v_p(f(n))=r_i$. Thus, this implies $m\mid r_i$ for all i, and clearly a must also be an mth power then: f is an mth power as wanted. For the general case where $f(n)$ is just always a perfect power, we can pick distinct primes p_i and an integer n_i such that $v_{p_i}(f(n_i))=r_i$. Then, if we pick an integer $n\equiv n_i\pmod{p_i}$, we get $v_{p_i}(f(n))=r_i$, which means that the r_i must all have a non-trivial common divisor. In other words, f is a constant times a perfect power, and it suffices to look at $v_p(f(n))$ for p dividing the constant to see that it is in fact a perfect power.

Now, we deduce the general case from the one variable case. Suppose again that $f\in\mathbb{Z}[X]$. Let π be a primitive irreducible factor of f. We shall find an arbitrarily large prime p such that $v_p(f(x))=v_\pi(f)$ for some $x\in\mathbb{Z}^m$ if f is non-constant. Then, using CRT, we can find primes p_π for each primitive irreducible factor of f and an element $y\in\mathbb{Z}^m$ such that $v_{p_\pi}(f(y))=v_\pi(f)$ for each π. Since $f(y)$ is a perfect power by assumption, we get that all v_π have a non-trivial common divisor, which means that f is a constant times a perfect power, and it is again easy to see that it is in fact a perfect power. Let π be a primitive irreducible factor of f. Suppose without loss of generality that it is non-constant in X_m, and let π' denote its derivative with respect to X_m. Use Bézout's lemma as in Exercise 5.5.1† to get $u,v\in\mathbb{Z}[X_1,\dots,X_{m-1}]$ such that

$$0\neq u\pi+v\pi'=h\in\mathbb{Z}[X_1,\dots,X_{m-1}].$$

Also, for every other primitive irreducible factor τ of f, consider a Bézout relation

$$0\neq u_\tau\pi+v_\tau\tau\in\mathbb{Z}[X_1,\dots,X_{m-1}].$$

Now, choose $x\in\mathbb{Z}^{m-1}$ such that $\pi(x,X)$ is non-constant, and such that $h(x)$ and $h_\tau(x)$ are non-zero for all $\pi\neq\tau\mid f$. This is possible by e.g. Exercise A.1.7* used on the product of the leading coefficient of f as a coefficient in X_m with h and all h_τ. Then, pick a large prime p and an integer n such that $p\mid\pi(x,n)$, there exists one by Theorem 5.2.1. When p is sufficiently large, by our Bézout relations, $p\nmid\tau(x,n)$ for $\pi\neq\tau\mid f$. Thus, $v_p(f(x,n))=v_\pi(f)v_p(\pi(x,n))$. Now, if $p^2\mid\pi(x,n)$, by assumption

$$p^2\nmid\pi(x,n+p)\equiv\pi(x,n)+p\pi'(x,n).$$

Thus, there is an n such that $v_p(f(x,n)) = v_\pi(f)$ as wanted and we are done. ■

Exercise 5.5.3†. Suppose $f, g \in \mathbb{Z}[X]$ are polynomials such that $f(a) - f(b) \mid g(a) - g(b)$ for any rational integers $a, b \in \mathbb{Z}$. Prove that there exists a polynomial $h \in \mathbb{Z}[X]$ such that $g = h \circ f$.

Solution

By Exercise 5.5.1†, we know that $f(X) - f(n) \mid g(X) - g(n)$ for all n (in fact we even have $f(X) - f(Y) \mid g(X) - g(Y)$ but we won't use that). Consider the base f expansion of g: $g = \sum_i h_i f^i$, where f^i means exponentiation and not iteration, and where $h_i \in \mathbb{Q}[X]$ are polynomials of degree less than $\deg f$. We have

$$g(X) \equiv \sum_i h_i(X) f(X)^i \equiv \sum_i h_i(X) f(n)^i \pmod{f(X) - f(n)}$$

so

$$f(X) - f(n) \mid \sum_i (h_i(X) - h_i(n)) f(n)^i.$$

However, the RHS has degree strictly less than $\deg g$ so must be identically zero. By taking n sufficiently large, we see that all h_i must be constant, otherwise the RHS will be non-zero. Indeed, if a_i is the coefficient of X^k of h_i for some $k \geq 1$, then the coefficient of X^k of the RHS is $\sum_i a_i f(n)^i$ so the polynomial $\sum_i a_i X^i$ must have infinitely many roots and thus be zero, i.e. $a_i = 0$ for all i. The fact that all h_i are constant is exactly what it means for g to be a polynomial in f. ■

Exercise 5.5.4 (RMM SL 2016)**.** Let p be a prime number. Prove that there are only finitely many primes q such that

$$q \mid \sum_{k=1}^{\lfloor q/p \rfloor} k^{p-1}.$$

Solution

Write $q = pn + r$ with $r \in [p-1]$. It suffices to prove that, for each r, $pn + r$ divides

$$\sum_{k=1}^{n} k^{p-1} := f_r(n)$$

finitely many times only. Note that, as we saw in Exercise A.3.8†, $f_r(n)$ is a polynomial in n of degree p and leading coefficient $1/p$. As a consequence, there is some integer $N \in \mathbb{Z}$ such that Nf_r has integer coefficients and is non-zero modulo p. By Exercise 5.5.1†, if $pn + r$ divides $f_r(n)$ infinitely many times, $pX + r \mid f_r$ in $\mathbb{Q}[X]$. By Gauss's lemma, since $pX + r$ is primitive, $pX + r$ divides Nf_r in $\mathbb{Z}[X]$. In particular, p divides the leading coefficient of Nf_r so Nf_r has degree at most $p - 1$ over $\mathbb{F}_p$. Since $Nf_r(n)$ is identically zero modulo p, as $f_r(n) \in \mathbb{Z}$ and $p \mid N$, this implies that $Nf_r = 0$ over $\mathbb{F}_p$ since it has degree at most $p - 1$ and p roots. This contradicts our initial assumption. ■

Polynomials over $\mathbb{F}_p$

Exercise 5.5.9† (Generalised Eisenstein's Criterion)**.** Let $f = a_n X^n + \ldots + a_0 \in \mathbb{Z}[X]$ be a polynomial and let p a rational prime. Suppose that $p \nmid a_n$, $p \mid a_0, \ldots, a_{n-1}$, and $p^2 \nmid a_k$ for some $k < n$. Then any factorisation $f = gh$ in $\mathbb{Q}[X]$ satisfies $\min(\deg g, \deg h) \leq k$.

Solution

Without loss of generality suppose $f = gh$ for some $g, h \in \mathbb{Z}[X]$ using Gauss's lemma. Modulo p, $f \equiv a_n X^n$ so $g \equiv bX^r$, $h \equiv cX^s$. If $r, s > k$, we get $p^2 \mid a_k$ which is a contradiction. Indeed, if $g = bX^r + pu$ and $h = cX^s + pv$, then $f \equiv bcX^{r+s} + p(buX^r + cvX^s) \pmod{p^2}$ and the coefficient of X^k of this polynomial is zero when $r, s > k$. ■

Exercise 5.5.10† (China TST 2008)**.** Let $f \in \mathbb{Z}[X]$ be a (non-zero) polynomial with coefficients in $\{-1, 1\}$. Suppose that $(X-1)^{2^k}$ divides f and $\deg f \geq 2^k$. Prove that $\deg f \geq 2^{k+1} - 1$.

Solution

We proceed as in Exercise 5.5.11†. Since $(X-1)^{2^k} \mid f$, we have $n := \deg f \geq 2^k$. Modulo 2, $f \equiv \frac{X^{n+1}-1}{X-1}$ and $(X-1)^{2^k} = X^{2^k} - 1$ by Frobenius. Thus, $X^{2^k} - 1 \mid X^{n+1} - 1$, which implies $2^k \mid n+1$ by Exercise 4.3.1*, and in particular $n \geq 2^{k+1} - 1$ as $n \geq 2^k$. ■

Exercise 5.5.11† (Romania TST 2002)**.** Let $f, g \in \mathbb{Z}[X]$ be polynomials with coefficients in $\{1, 2002\}$. Prove that $\deg f + 1 \mid \deg g + 1$.

Solution

Modulo 3 (which was chosen so that $1 \equiv 2002$), by Gauss's lemma, we get $f \equiv \frac{X^{\deg f+1}-1}{X-1}$ and $g \equiv \frac{X^{\deg g+1}-1}{X-1}$. Thus, $X^{\deg f+1} - 1 \mid X^{\deg g+1} - 1$ over $\mathbb{F}_3$, which implies $\deg f + 1 \mid \deg g + 1$ by Exercise 4.3.1*. ■

Exercise 5.5.12† (USAMO 2006)**.** Find all polynomials $f \in \mathbb{Z}[X]$ such that the sequence $(P(f(n^2)) - 2n)_{n \geq 0, f(n^2) \neq 0}$ is bounded above, where P is the greatest prime factor function. (In particular, since $P(0) = +\infty$, we have $f(n^2) \neq 0$ for any $n \in \mathbb{Z}$.)

Solution

Suppose that $P(f(n^2)) - 2n \leq N$ for all n. Suppose that $p \mid f(n^2)$ for some odd prime p and a rational integer n. Without loss of generality, suppose $0 \leq n < \frac{p}{2}$ by replacing n by its remainder upon its Euclidean division by p, and then replacing it by $p - n$ if necessary. By assumption, $p - 2n \in [N]$. Thus, the odd prime factors of n always divide the ones of

$$(2n+1) \cdot \ldots \cdot (2n+N)(2n-1) \cdot \ldots \cdot (2n-N) = (4n^2-1) \cdot \ldots \cdot (4n^2 - N^2).$$

By Exercise 5.5.1†, this implies that f divides

$$(4X-1) \cdot \ldots \cdot (4X - N^2),$$

i.e. f has the form $a \prod_i 4X - a_i^2$ for some $a \in \mathbb{Q}$ and $a_i \in \mathbb{Z}$. Since $f(n^2)$ has no root, all a_i must be odd, and this implies $a = \pm 1$ by Gauss's lemma since $4X - k$ is primitive for odd k. Conversely, these all work, $p \mid f(n^2) \implies p \mid 2n \pm a_i$ and thus $p - 2n \leq \max_i(|a_i|) := N$. ■

Exercise 5.5.14† (China TST 2021)**.** Suppose the polynomials $f, g \in \mathbb{Z}[X]$ are such that, for any sufficiently large rational prime p, there is an element $r_p \in \mathbb{F}_p$ such that $f \equiv g(X + r_p) \pmod{p}$. Prove that there exists a rational number $r \in \mathbb{Q}$ such that $f = g(X + r)$.

Solution

It is clear that f anf g have the same degree. We proceed by induction on $\deg f$. When f is constant it is trivial. For the inductive step, notice that the statement still holds for f' and g'. Since they have degree $\deg f - 1$, we conclude that $f' = g'(X+r)$ for some r, i.e. $f = g(X+r)+c$ for some $c \in \mathbb{Q}$. When $\deg f = 1$ this already implies that $f = g(X+s)$ for some s. Otherwise, since we have $g'(X+r_p) \equiv g'(X+r)$, we get $r_p \equiv r$. In that case, we get $c \equiv 0 \pmod{p}$ for infinitely many p so $c = 0$ as wanted. ■

Iterates

Exercise 5.5.16†. Let $f \in \mathbb{Z}[X]$ be a polynomial. Show that the sequence $(f^n(0))_{n\geq 0}$ is a *Mersenne sequence*, i.e.

$$\gcd(f^i(0), f^j(0)) = f^{\gcd(i,j)}(0)$$

for any $i, j \geq 0$.

Solution

If $f^i(0) \equiv 0 \pmod{d}$, then we get $f^{ki}(0) \equiv 0$ for any integer $k \geq 0$ by applying f^i multiple times on both sides. This shows that $f^{\gcd(i,j)}(0) \mid \gcd(f^i(0), f^j(0))$. For the converse, suppose that d divides $f^i(0)$ and $f^j(0)$ where $j > i$. Then,

$$0 \equiv f^j(0) \equiv f^{j-i}(f^i(0)) \equiv f^{j-i}(0)$$

so $d \mid f^{j-i}(0)$ too. This shows that we can apply Euclid's algorithm to get $d \mid f^{\gcd(i,j)}(0)$. ■

Exercise 5.5.17†. Suppose the non-constant polynomial

$$f = a_d X^d + \ldots + a_2 X^2 + a_0 \in \mathbb{Z}[X]$$

has positive coefficients and satisfies $f'(0) = 0$. Prove that the sequence $(f^n(0))_{n\geq 1}$ always has a primitive prime factor.

Solution

Notice that the coefficient of f^i of X^2 is also 0 for any i (this can be seen via direct expansion or via $(f^i)'(0) = f'(0)f'(f^{i-1}(0)) = 0$). Thus, we have $f^i(x) \equiv f^i(0) \pmod{x^2}$ for any $x \in \mathbb{Z}$. Letting $x = f^j(0)$ yields $f^{i+j}(0) \equiv f^i(0) \pmod{f^j(0)^2}$. By induction, we get

$$f^{km}(0) \equiv f^m(0) \pmod{f^k(0)^2} \qquad (*)$$

for any integers $k, m \geq 0$.

Suppose now that $f^n(0)$ doesn't have a primitive prime factor for some $n \geq 2$. This means that, if $p \mid f^n(0)$ is prime, $p \mid f^k(0)$ for some k. By Exercise 5.5.16†, we may assume that $k \mid n$ by replacing it by $\gcd(k, n)$ if necessary. Then, by $(*)$, we have $f^n(0) \equiv f^k(0) \pmod{f^k(0)^2}$. In particular, $v_p(f^n(0)) = v_p(f^k(0))$. Thus, we conclude that

$$v_p(f^n(0)) \leq v_p(f(0) \cdot \ldots \cdot f^{n-1}(0))$$

for any prime p. This means that

$$f^n(0)) \leq f(0) \cdot \ldots \cdot f^{n-1}(0).$$

We shall prove that this is impossible for $n \geq 2$ by induction. We clearly have $f(0) \geq 1$ since the coefficients are non-negative. Now, if $f^n(0) \geq f(0) \cdot \ldots \cdot f^{n-1}(0)$, then

$$f^n(0)^2 \geq f(0) \cdot \ldots \cdot f^{n-1}(0)$$

so it suffices to prove that $f^{n+1}(0) > f^n(0)^2$. This is clearly true since $f(x) > x^2$ for positive x. ■

Exercise 5.5.18† (Tuymaada 2003)**.** Let $f \in \mathbb{Z}[X]$ be a polynomial and $a \in \mathbb{Z}$ a rational integer. Suppose $|f^n(a)| \to \infty$. Prove that there are infinitely many primes p such that $p \mid f^n(a)$ for some $n \geq 0$ unless $f = AX^d$ for some A, d.

Solution

Suppose that there are finitely many such primes $p_1, \ldots, p_m$. Suppose first that $f(0) = 0$. Then, if we let $g = X^k f$ where $g(0) \neq 0$, we get

$$g(f^i(a)) \equiv g(0) \pmod{f^{i-1}(a)} \tag{$*$}$$

since $f(0) = 0$. Choose an n such that $p_1 \cdot \ldots \cdot p_m \mid f^n(a)$ there exists one by assumption (if $p \mid f^j(a)$ then $p \mid f^{j+1}(a)$). Let p be one of $p_1, \ldots, p_m$. By $(*)$, we have $v_p(g(f^i(a)) = 0$ if $p \nmid g(0)$, and, for $i > n$, if $p \mid g(0)$,

$$v_p(f^i(a)) = v_p(f^{i-1}(a)^k g(f^{i-1}(a))) \geq v_p(f^{i-1}(a)) + 1$$

since $g(f^{i-1}(a)) \equiv g(0) \equiv 0$. Hence, for sufficiently large i we get $v_p(f^{i-1}(a)) > v_p(g(0))$ for all $p = p_1, \ldots, p_m$. Combined with $(*)$, we must have $g(f^k(a)) = g(0)$ since the p_i are the only prime factors, and for large k this implies that g is constant as wanted.

Let n be a large integer. Consider the $k+1$ numbers $f^n(a), f^{n+1}(a), \ldots, f^{n+m}(a)$. Each of them is divisible by a large power of a p_k, since by assumption they are large and their only prime factors are the p_i. By the pigeonhole principle, two of them must be divisible by a large power of the same p_k, say $p_k^r \mid f^{n+i}(a), f^{n+j}(a)$ with $j > i$. Then, $p_k^r \mid f^{j-i}(0)$. Taking $n \to \infty$ and thus $r \to \infty$ yields $f^s(0) = 0$ for some $1 < s \leq m$. Now, the previous discussion implies that $f^s = AX^d$ for some d. However, if $\deg f \geq 2$, it is easy to see that f^s can only be of this form is f is. Indeed, if the two leading terms of g are $UX^u + VX^v$ and the leading term of f is WX^w, then the leading terms of $f \circ g$ are

$$WU^w X^{uw} + wVU^{w-1} X^{u(w-1)+v}$$

(the situation is different when $\deg f = 1$ because the contribution we also need to take in account the second term of f). Thus, we are done when $\deg f \neq 1$. Otherwise, suppose that $f = uX + v$ with $v \neq 0$. Then,

$$f^n(a) = u^n \left(a + \frac{v}{u-1}\right) - \frac{v}{u-1}.$$

Our previous discussion implies that $a \neq 0$, otherwise the sequence $(f^n(a))_{n \geq 0}$ is bounded. If we take

$$n = \varphi((p_1 \cdot \ldots \cdot p_k)^N),$$

we get $f^n(a) \in \{a, -\frac{v}{u-1}\}$ modulo p_i^N for every i. For sufficiently large N, both of these are non-zero modulo p_i^N, so the p-adic valuation are bounded which implies that the sequence is too since these are the only prime factors. This is a contradiction. ■

Exercise 5.5.19† (USA TST 2020)**.** Find all integers $n \geq 2$ for which there exist a rational integer $m > 1$ and a polynomial $f \in \mathbb{Z}[X]$ such that $\gcd(m, n) = 1$ and $n \mid f^k(0) \iff m \mid k$ for any positive rational integer k.

Solution

Let $k\#$ denote the product of the first k prime numbers (the kth *primorial*). We shall prove that n works if and only if $\operatorname{rad} n \neq k\#$ for any integer $k \geq 1$.

Suppose first that $\operatorname{rad} n \neq k\#$ for any integer $k \geq 1$. Let p be the greatest prime factor of n and $r = v_p(n)$, and let q be the smallest prime which doesn't divide n. By assumption, $q < p$. Consider the cycle $\tau : 0 \to 1 \to \ldots \to q \to 0$. Construct the polynomial

$$g = \sum_{i=0}^{p-1} \tau(i) \prod_{P} j \neq i \frac{X - i}{i - j} \in \mathbb{Z}/p^r\mathbb{Z}[X]$$

which interpolates τ. Note that this is indeed in $\mathbb{Z}/p^r\mathbb{Z}$ as the denominators are in $]-p, p[$ and non-zero, and thus coprime with p. Lift g to any polynomial with integer coefficients which is congruent to g modulo p^k. We shall denote this new g abusively by g again. Let $u \in \mathbb{Z}$ be such that $a \cdot \frac{n}{p^k} \equiv 1 \pmod{p^k}$. Then, $f := \frac{un}{p^k} g$ works as we have

$$n \mid f^k(0) \iff p^k \mid g^k(0) \iff q \mid k$$

$(m = q)$.

Now, suppose $\operatorname{rad} n = k\#$ for some k. Suppose for the sake of a contradiction that there is some $f \in \mathbb{Z}[X]$ and $m \in \mathbb{Z}$ coprime such that $n \mid f^k(0)$ if and only if $m \mid k$. Notice that this implies that the sequence $(f^k(0))_{k \geq 0}$ is periodic modulo n, and thus also modulo p for any $p \mid n$. Since it can take only p values modulo p, the period is at most p. Since it is coprime with n, it must be 1 (by assumption all primes $q \leq p$ divide n). Thus, the sequence $(f^k(0))_{k \geq 0}$ is constant modulo $\operatorname{rad} n$. We shall prove by induction on ℓ that $p^\ell \mid f(0)$ for any $p \mid n$ and $\ell \leq v_p(n)$, which implies that $f(0) \equiv 0$, contradicting the fact that $m > 1$. We have already proved the base case. Note that, by Corollary 5.3.1, we have

$$f^{k+1}(0) \equiv f(0) + f^k(0) f'(0) \pmod{p^{\ell+1}}. \tag{$*$}$$

Suppose for the sake of a contradiction that $p \nmid f'(0)$. If $f'(0) \equiv 1 \pmod{p}$, by induction, we get $f^k(0) \equiv k f(0) \pmod{p^{\ell+1}}$. Thus, if $p^{\ell+1} \nmid f(0)$, we have $p^{\ell+1} \mid f^k(0) \iff p \mid k$ which contradicts the fact that m was coprime with n.

Thus, $f'(0) \not\equiv 1 \pmod{p}$. Accordingly, $(*)$ becomes

$$\left(f^{k+1}(0) + \frac{f(0)}{f'(0) - 1}\right) \equiv f'(0) \left(f^{k+1}(0) + \frac{f(0)}{f'(0) - 1}\right).$$

By induction, we get

$$f^k(0) \equiv f(0) \cdot \frac{f'(0)^k - 1}{f'(0) - 1}.$$

If $p^{\ell+1} \nmid f(0)$, we have

$$p^{\ell+1} \mid f^k(0) \iff p \mid f'(0)^k - 1 \iff s \mid k$$

where s is the order of $f'(0)$ modulo p. However, $s \mid p - 1$ so $s < p$ and is thus not coprime with n which is again a contradiction.

Finally, we conclude that we must in fact have $p \mid f'(0)$. But then, $(*)$ becomes $f^k(0) \equiv f(0)$, and since $f^m(0) \equiv 0$ we get $f(0) \equiv 0$ as wanted. ■

Exercise 5.5.20†. Let $f \in \mathbb{Q}[X]$ be a polynomial of degree k. Prove that there is a constant $h > 0$ such that that the denominator of $f(x)$ is greater than h times the denominator of x^k.

Solution

Let $x = \frac{m}{n}$ where m and n coprime rational integers, write $f = \sum_{i=0}^{k} a_i X^i$ (with $k = \deg f$) and pick $0 \neq N \in \mathbb{Z}$ such that $Nf \in \mathbb{Z}[X]$. Denote by $\mathbb{Z}_{(p)}$ the set of rational numbers with denominator not divisible by p. Let p be a prime factor of n and $c \geq 0$ be an integer. Then,

$$Np^{kv_p(n)-c} f\left(\frac{m}{n}\right) = \frac{Na_k m^k}{p^c}\left(\frac{n}{p^{v_p(n)}}\right) + \sum_{i=0}^{k-1} Na_i m^i \left(\frac{p^{v_p(n)}}{n}\right) p^{-c}.$$

For $v_p(n) \geq c$, the second sum is in $\mathbb{Z}_{(p)}$, while for $c > v_p(Na_k)$, the first term is not in $\mathbb{Z}_{(p)}$. Thus, for $v_p(n) \geq c > v_p(Na_k) := c_p$, $Np^{kv_p(n)-c} f\left(\frac{m}{n}\right) \notin \mathbb{Z}_{(p)}$, i.e. the denominator D of $Nf\left(\frac{m}{n}\right)$ is divisible by $p^{kv_p(n)+1-c}$. We conclude that, for $v_p(n) > c_p$, we have $p^{kv_p(n)-c_p} \mid D$.

We are now almost done. Let P be the product $p^{v_p(n)}$ over the primes p for which $v_p(n) \leq c_p$. Then,

$$P \leq \prod_p p^{c_p} = |Na_k| := C.$$

Thus, the denominator of $Nf\left(\frac{m}{n}\right)$, and hence of $f\left(\frac{m}{n}\right)$, is at least

$$\prod_{v_p(n)>c_p} p^{kv_p(n)-c_p} \geq \frac{1}{C^k} \cdot \prod_{p|n} p^{kv_p(n)-c_p} \geq \frac{1}{C^{k+1}} \prod_{p|n} p^{kv_p(n)} = \frac{|n|^k}{C^{k+1}}$$

as desired ($h = \frac{1}{C^{k+1}}$). ■

Exercise 5.5.21†. Let $f \in \mathbb{Q}[X]$ be a polynomial of degree at least 2. Prove that

$$\bigcap_{k=0}^{\infty} f^k(\mathbb{Q})$$

is finite.

Solution

Let $D(x)$ denote the denominator of a rational number $x \in \mathbb{Q}$. Note that, by Exercise 5.5.20†, when $D(x)$ is sufficiently large, $D(f(x)) > D(x)$ as $\deg f \geq 2$. This implies that, for a fixed r, if $r = f^k(s_k)$ for all k, the denominator of s_k is bounded (otherwise $f^k(s_k)$ would have a denominator which is too large). However, its absolute value is also bounded, since $|f(x)| > r$ for sufficiently large $|x|$. Thus, there are a finite number of possible s_k, and this implies that $f^i(s) = r = f^j(s)$ for some i, j and $s := s_i = s_j$. In other words, the intersection $\bigcap_{k=0}^{\infty} f^k(\mathbb{Q})$ consists only of pre-periodic points, since we also have $f^i(r) = f^{i+j}(s) = f^j(r)$. Thus, it suffices to show that there are finitely many pre-periodic points.

Let r be a pre-periodic point, i.e. such that $f^i(r) = f^j(r)$ for some $j > i$. The same trick as before shows that $D(r)$ is bounded. Indeed, if $D(r)$ is sufficiently large, then $D(f^i(r)) > D(r)$ is too, and thus

$$D(f^j(r)) = D(f^{j-i}(f^i(r))) > D(f^i(r)).$$

But at the same time, the absolute value of r is also bounded since $|f(x)| > |x|$ for $|x|$ sufficiently large (as $\deg f \geq 2$), so there are a finite number of preperiodic points as wanted. ■

Exercise 5.5.22† (Iran TST 2004)**.** Let $f \in \mathbb{Z}[X]$ be a polynomial such that $f(n) > n$ for any positive rational integer n. Suppose that, for any $N \in \mathbb{Z}$, there is some positive rational integer n such that

$$N \mid f^n(1).$$

Prove that $f = X + 1$.

Solution

Choose $N = f^{n+1}(1) - f^n(1)$ for some n. Then, the sequence $f^i(1)$ modulo N goes as follows:

$$f(1), f^2(1), \ldots, f^n(1), f^n(1), f^n(1), \ldots.$$

Thus, by assumption, $N \mid f^k(1)$ for some $k \leq n$. If $k = n$, then $f^{n+1}(1) - f^n(1) \equiv f(0)$. Thus, we get

$$f^{n+1}(1) - f^n(1) \leq f^{n-1}(0)$$

or $f^{n+1}(1) - f^n(1) \leq f(0)$. It is easy to see that this forces $f = X + m$. Finally, modulo m the sequence $f^n(1)$ is constant equal to 1 so $m = \pm 1$, and since $f(n) > 1$ this means that $f = X + 1$ as wanted. ■

Divisibility Relations

Exercise 5.5.23†. Find all polynomials $f \in \mathbb{Z}[X]$ such that $f(n) \mid n^{n-1} - 1$ for sufficiently large n.

Solution

Let n be a sufficiently large rational integer, and p be a prime factor of $f(n)$. Let $m \equiv n \pmod{p}$ and $m \equiv 2 \pmod{p-1}$ be an integer. Then, $p \mid f(m) \mid m^{m-1} - 1 \equiv n - 1$. Thus, every prime factor of $f(n)$ divides $n - 1$. By Corollary 5.4.2, this implies that f is a constant times a power of $X - 1$, say $c(X-1)^k$. By LTE, for any $p \mid n - 1$, we have

$$v_p(n^n - 1) = v_p(n-1) + v_p(n-1) = 2v_p(n-1)$$

so $k \leq 2$. Finally, the constant divides $n - 1$ for every sufficiently large n so must be ± 1. Conversely, by the previous discussion, $\pm 1, \pm(X-1), \pm(X-1)^2$ all work. ■

Exercise 5.5.25† (ISL 2012 Generalised)**.** Find all polynomials $f \in \mathbb{Z}[X]$ such that $\operatorname{rad} f(n) \mid \operatorname{rad} f(n^{\operatorname{rad} n})$. (You may assume Dirichlet's theorem.)

Solution

Let $n \in \mathbb{Z}$ and suppose that p is a prime factor of $f(n)$. Suppose that $p \nmid n$. Let $k \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times$ be arbitrary. Pick a prime number $q \equiv n \pmod{p}$ and $q \equiv k \pmod{p-1}$ using Dirichlet's theorem and CRT. Then, $p \mid \operatorname{rad} f(q) \mid f(n^q)$ so $p \mid f(n^k)$. Thus, whenever $p \mid f(n)$, either $p \mid n$ or $p \mid f(m)$ for any m with the same order as n modulo p. In particular, if n has order u modulo p, then f has u roots in $\mathbb{F}_p$. Let d be the degree of f. Since f has at most d roots in $\mathbb{F}_p$, this implies that the prime factors of $f(n)$ all divide $g(n)$ where g is

$$X\Phi_1\Phi_2 \cdot \ldots \cdot \Phi_d.$$

Now, suppose $f = \lambda X^{a_0} \prod_{s \in S}^{\ell} \Phi_s^{a_s}$. We claim that f works iff S if $r \mid s \implies r \in S$ for any $s \in S$. Clearly, these all work since if n has order s modulo p, i.e. $p \mid \Phi_s(n)$, then $n^{\operatorname{rad} n}$ has order r dividing s and $p \mid \Phi_r(s) \mid f(n^{\operatorname{rad} n})$ as wanted.

It suffices to that $r \mid s \implies r \in S$ when $\frac{s}{r}$ is prime, since we can obtain any divisor of s by dividing multiple times by a prime. Thus, suppose that $s = qr$ for some prime q. Let $p \equiv 1 \pmod{s}$ be a prime not dividing any element of S and let n be an element of order s modulo p. Pick a prime $q' \neq q$ such that $qq' \equiv n \pmod{p}$ and $q' \equiv 1 \pmod{\frac{p-1}{q}}$, there exists one by CRT and Dirichlet's theorem again. Then, $p \mid \operatorname{rad} f(qq') \mid f(n^{qq'})$ so $p \mid f(n^q)$. Since n^q is an element of order r modulo p, this means that $\Phi_r \mid f$ as wanted. We conclude that all solutions have the

form

$$f = \lambda X^{a_0} \prod_{s \in S}^{\ell} \Phi_s^{a_s}$$

where S is such that $r \mid s \in S$ implies $r \in S$. ■

Remark 5.5.1

There is an elementary way to avoid the use of Dirichlet's theorem. When we take a prime satisfying some congruence condition, we do not really care that it's prime, we just care about the value of its radical. Thus, it suffices to have a (sufficiently large) **squarefree** n such that $n \equiv a \pmod b$ for some coprime a, b. This can be done by showing that the density of such n is positive. More specifically, let N be a positive integer. We want to count how many $n \in [N]$ are congruent to $a \pmod b$ and **not** squarefree. If we show that this is $cN + o(N)$ for some $c < \frac{1}{\varphi(b)}$ we are done since there are $\frac{N}{\varphi(b)} + O(1)$ integers congruent to a modulo b in $[N]$. How many such integers are there then? Well, n is not squarefree if it is divisible by p^2 for some prime p. We can assume $p \nmid b$ as these primes can't divide $n \equiv a \pmod b$. Then, there are $\frac{N}{\varphi(b)p^2} + O(1)$ such integers congruent a modulo b since the conditions $n \equiv 0 \pmod{p^2}$ and $n \equiv a \pmod b$ are independent by CRT. Thus, the number of $n \equiv a \pmod b$ in $[N]$ which are not squarefree is at most

$$\frac{N}{\varphi(b)} \left(\sum_{p \nmid b, p \leq N} \left(\frac{1}{p^2} + O(1/N) \right) \right) = O(\pi(N)) + \frac{N}{\varphi(b)} \left(\sum_{p \nmid b} \frac{1}{p^2} \right)$$

where $\pi(n)$ is the number of primes less than n. In Exercise 3.5.14†, we proved that $\pi(N) = o(N)$, so we only need to show that $\sum_{p \nmid b} \frac{1}{p^2} < 1$ to be done. This follows from the following estimate:

$$\sum_{p} \frac{1}{p^2} < \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \sum_{n=2}^{\infty} \frac{1}{n-1} - \frac{1}{n} = 1.$$

We end this remark with one more observation: our previous approach can be refined to show that, in fact, the exact density of squarefree $n \equiv a \pmod b$ is

$$\frac{1}{\varphi(b)} \prod_{p \nmid b} 1 - \frac{1}{p^2} = \frac{1}{\zeta(2)\varphi(b) \prod_{p \mid b} 1 - \frac{1}{p^2}} = \frac{6}{\pi^2 \varphi(b) \prod_{p \mid b} 1 - \frac{1}{p^2}}.$$

Indeed, the product of $1 - \frac{1}{p^2}$ comes from the inclusion-exclusion principle: the density of n not divisible by p^2 is $1 - \frac{1}{p^2}$ and these densities are independent by CRT. More precisely, there are

$$\frac{N}{\varphi(b)} \prod_{p \nmid b, p \leq N} 1 - \frac{1}{p^2} + O(1/N)$$

integers in $[N]$ congruent to a modulo b which are not divisible by a square. If we take the logarithm, since

$$\log(x + \varepsilon) - \log x = \log(1 + \varepsilon/x) = \varepsilon/x + O(\varepsilon^2/x^2),$$

we will be able to sum the $O(1/N)$ and get $O(\pi(N)/N) \to 0$. When we retake the exponential, this gives us a constant which goes to 1. Hence, after dividing by N, we get the wanted result.

Exercise 5.5.27†. Find all polynomials $f \in \mathbb{Z}[X]$ such that $f(p) \mid 2^p - 2$ for any prime p. (You may assume Dirichlet's theorem.)

Solution

Let $n \in \mathbb{Z}$ be an integer and suppose p is an odd prime factor of $f(n)$. Suppose for the sake of a contradiction that $p \nmid n$. Usin Dirichlet's theorem, we may find a prime $q \equiv n \pmod{p}$ and $q \equiv -1 \pmod{p-1}$. This gives $p \mid f(q) \mid 2^q - 2 \equiv -\frac{3}{2} \pmod{p}$ so $p = 3$. Thus, the sufficiently large prime divisors of $f(n)$ divide n which implies that $f = aX^k$ for some $a \in \mathbb{Z}$ and some integer $k \geq 0$ by Corollary 5.4.2. Since $f(2) \mid 2$, we get the solutions $f = \pm 2$ and $f = \pm X$, which work by Fermat's little theorem. ■

Miscellaneous

Exercise 5.5.29† (Generalised Hensel's Lemma)**.** Let $f \in \mathbb{Z}[X]$ be a polynomial and $a \in \mathbb{Z}$ an integer. Let $m = v_p(f'(a))$. If $p^{2m+1} \mid f(a)$, prove that f has exactly one root b modulo p^k which is congruent to a modulo p^{m+1} for all $k \geq 2m+1$.

Solution

We need to show that we can still perform the inductive step for $k \geq 2m+1$. Write $b_{k+1} = b_k + up^{k-m}$. We have

$$f(b_{k+1}) \equiv f(b_k) + up^{k+1-m} f'(a) \pmod{p^{k+1}}$$

as before. This can be congruent to 0 if and only if $v_p(p^{k+1-m} f'(a)) < v_p(f(b_k))$, which is true since

$$v_p(f(b_k)) > k = (k-m) + v_p(f'(a)).$$

As before, this u is unique modulo p which shows the wanted result. ■

Remark 5.5.2

This doesn't work under the weaker assumption that $v_p(f(a)) > m$, as can be seen from $f = 14X^2 + 3X + 9$ which doesn't have a root modulo 3^3 (this may seem very random but it was in fact carefully constructed from our previous proof), because the congruence we get with the derivative holds modulo $p^{2(k-m)}$, and $2(k-m) \geq k+1$ only for $k \geq 2m+1$.

Exercise 5.5.30†**.** Let $f \in \mathbb{Z}[X]$ be a non-constant polynomial. Is it possible that $f(n)$ is prime for any $n \in \mathbb{Z}$?

Solution

Let f be a polynomial which is always prime. If $f(n) = p$, then $p \mid f(n + kp)$, so we must have $f(n + kp) = p$. For sufficiently large k, this implies that $f = p$ is constant. ■

Exercise 5.5.31†**.** Find all polynomials $f \in \mathbb{Q}[X]$ which are surjective onto $\mathbb{Q}$.

Solution

Without loss of generality, suppose that $f \in \mathbb{Z}[X]$ and $f(0) = 0$. We will prove that f must have degree 1 (and conversely, these polynomials are surjective). Let p be a rational prime. Examine the equation $f(r) = p$: by Exercise 1.1.2, the potential rational solutions have the form $\frac{p}{s}$ or $\frac{1}{s}$ where s is a divisor of the leading coefficient of f. The latter is impossible for large p, while the

former is only possible for large p if f has degree 1, otherwise $f(r) = f\left(\frac{p}{s}\right)$ grows too fast, of the order of p^n where n is the degree of f. ■

Exercise 5.5.35† (ISL 2005)**.** Let $f \in \mathbb{Z}[X]$ be a non-constant polynomial with positive leading coefficient. Prove that there are infinitely many positive rational integers n such that $f(n!)$ is composite.

Solution

Wilson's theorem tells us that, if p is prime and $0 \leq n \leq p-1$,

$$(p-1-n)! \equiv \frac{(p-1)!}{(-1)\cdot(-2)\cdot\ldots\cdot(-n)} \equiv \frac{(-1)^{n-1}}{n!}.$$

In other words, if we let $g(X)$ be the polynomial $X^{\deg f} f(1/X)$, for any prime p and any positive rational integer n, $p \mid f(n!) \iff p \mid g((-1)^{n-1}(p-1-n)!)$. Hence, we wish to find an integer m such that $g((-1)^{m-1}m!)$ has a prime factor $p > m$ for which $f((p-1-m)!)$ is greater than p. That way, $f((p-1-m)!)$ will be divisible by p and not equal to p which means that it's composite as desired. Suppose that there are finitely many such primes. Note that, for sufficiently large m, if $p \mid g(m!)$ and $p \leq m$, then $p \mid g(0)$. In particular, there are finitely many such primes since $g(0)$ is the leading coefficient and f, and the same argument shows that

$$\prod_{p \mid g(m!), p \leq m} p^{v_p(g(m!)) \leq g(0)}.$$

This implies that, for sufficiently large m, $g((-1)^{m-1}m!)$ has a prime factor $p > m$. Then, for this p, we have $p \mid f((p-1-m)!)$ by construction so $f((p-1-m)!) = p$ for sufficiently large p by assumption. In particular, since $f(n!) \geq n!/2 > 2^n$ for large n, we have $p \leq 2m$, otherwise $f((p-1-m)!) > 2^{m-1} \geq p$. In other words, p is fairly close to m: between m and $2m$. We are almost done. Consider the sequence $(f(n!))_{n \geq 0}$. By assumption, p is an element of this sequence. However, the terms of $f(n!)$ grow further and further away: $f((n+1)!)/f(n!) \to \infty$. Hence, if we choose $m = 2f(n!)$ for instance, p will be greater than $f(n!)$ but smaller than $f((n+1)!)$ and so won't be in the sequence (for large n). ■

Chapter 6

The Primitive Element Theorem and Galois Theory

6.1 General Definitions

Exercise 6.1.1*. Prove that $R[\alpha_1, \ldots, \alpha_n]$ is indeed the smallest ring containing R and $\alpha_1, \ldots, \alpha_n$, in the sense that any other such ring must contain $R[\alpha_1, \ldots, \alpha_n]$. Similarly, prove that any field containing K and $\alpha_1, \ldots, \alpha_n$ contains $K(\alpha_1, \alpha_n)$.

Solution

If a ring contains R and $\alpha_1, \ldots, \alpha_n$, it contains all polynomials in $\alpha_1, \ldots, \alpha_n$ with coefficients in R since these are obtained from multiplication and addition of elements of R and the α_i. Thus, it contains $R[\alpha_1, \ldots, \alpha_n]$. Similarly, if a field contains K and $\alpha_1, \ldots, \alpha_n$, it contains all rational functions in $\alpha_1, \ldots, \alpha_n$ with coefficients in K since these are obtained from multiplication of elements of $K[\alpha_1, \ldots, \alpha_n]$ with inverses of other elements (we have already shown that the field must contain $K[\alpha_1, \ldots, \alpha_n]$ since a field is also a ring). ■

Exercise 6.1.2*. Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number. Prove that $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$.

Solution

We wish to prove that $\mathbb{Q}[\alpha]$ is closed under inversion. Let $f(\alpha)$ be a non-zero element of $\mathbb{Q}[\alpha]$, i.e. $\pi_\alpha \nmid f$. Then, since π_α is irreducible, it is coprime with f. Thus, by Bézout's lemma, we have $rf + s\pi_\alpha = 1$ for some $a, b \in \mathbb{Q}[X]$. Evaluating at α yields $r(\alpha)f(\alpha) = 1$ as wanted. ■

Exercise 6.1.3*. Prove that the minimal polynomial of $\frac{(i+1)\sqrt{2}}{2}$ over $\mathbb{Q}(i)$ is $X^2 - i$.

Solution

$\frac{(i+1)\sqrt{2}}{2}$ is a root of $X^2 - i$ and not in $\mathbb{Q}(i)$ so its minimal polynomial has degree 2 and divide $X^2 - i$ and is therefore equal to it. ■

Exercise 6.1.4*. Check that L is a K-vector space.

Solution

Since $K \subseteq L$, multiplication of elements of L (vectors) by elements of K (scalars) is well-defined and satisfies the obvious properties since it's just the multiplication of two elements of L! ■

Exercise 6.1.5*. Prove that $(u_i v_j)_{i\in[m],j\in[n]}$ is a K-basis of M.

Solution

Suppose that $\sum_{i,j} a_{i,j} u_i v_j = 0$ for some $a_{i,j} \in K$. Rewrite it as

$$\sum_i u_i \left(\sum_j a_{i,j} v_j \right) = 0.$$

This is a linear combination of the L-basis of M. Thus, by definition of a basis, $\sum_j a_{i,j} v_j = 0$ for each i. Again by the definition of a basis, this means that $a_{i,j} = 0$ for each j and each i.

Thus this family is linearly independent. It remains to show that it generate all of M. We can proceed exactly as we did but in the reverse direction: let $\alpha = \sum_i b_i u_i$ be an element of M, with $b_i \in L$ (recall that u_i is the L-basis of M). Write each b_i as a linear combination $\sum_j a_{i,j} v_j$ with $a_{i,j} \in K$ (v_i is the K-basis of L). We get

$$\alpha = \sum_{i,j} a_{i,j} u_i v_j$$

as wanted. ■

Exercise 6.1.6*. Let $M/L/K$ be a tower of extensions and $\alpha \in M$. Prove that the minimal polynomial of α over L divides the minimal polynomial of α over K. In other words, its L-conjugates are among its K-conjugates.

Solution

The minimal polynomial of α over K is also a polynomial over L since $K \subseteq L$. Since it vanishes at α, this means that it is divisible by the minimal polynomial of α over L. ■

Exercise 6.1.7*. Prove that finite extensions of K are exactly the fields of the form $K(\alpha_1, \ldots, \alpha_n)$ for $\alpha_1, \ldots, \alpha_n$ algebraic elements over K, using Proposition 6.1.1.

Solution

We proceed by induction on $[L : K]$, where L is a finite extension of K (we do not fix K). When this is one we have $L = K$. For the induction step, let $\alpha \in L$ be an element which is not in K. By the tower law,

$$[L : K] = [L : K(\alpha)][K(\alpha) : K].$$

Since $\alpha \notin K$, $[K(\alpha) : K] > 1$ so that $[L : K(\alpha)] < [L : K]$. By the induction hypothesis, this means

$$L = K(\alpha)(\alpha_1, \ldots, \alpha_n) = K(\alpha, \alpha_1, \ldots, \alpha_n)$$

as wanted. ■

6.2 The Primitive Element Theorem and Field Theory

Exercise 6.2.1. Let K be a number field. Prove that the embeddings of K are the non-zero functions $f : K \to \mathbb{C}$ which are both multiplicative and additive.

Solution

This is the Cauchy equation: we shall show that any additive function is $\mathbb{Q}$-linear. By induction, we have $f(nx) = nf(x)$ for any $n \in \mathbb{Z}$. Thus, for $0 \neq m, n \in \mathbb{Z}$, we have

$$nf(xm/n) = f(xm) = mf(x)$$

which means $f(xm/n) = f(x)m/n$, i.e. f is $\mathbb{Q}$-linear. ■

Exercise 6.2.2*. Let L/K be a finite extension and $\varphi \in \mathrm{Emb}_K(L)$ an embedding of L. Prove that $\varphi(f(\alpha)) = f(\varphi(\alpha))$ for any $f \in K[X]$ and $\alpha \in L$.

Solution

Let $f = \sum_i a_i X^i$. Then,

$$\varphi\left(\sum_i a_i \alpha^i\right) = \sum_i \varphi(a_i \alpha^i) = \sum_i \varphi(a_i)\varphi(\alpha)^i = \sum_i a_i \varphi(\alpha)^i$$

since φ fixes K. (Note that we have used the fact the sum is finite here, it is not true in general that embeddings commute with power series.) ■

Exercise 6.2.3*. Let $\alpha \in L$ be an element and $\sigma \in \mathrm{Emb}_K(L)$ be an embedding. Prove that $\sigma(\alpha)$ is a conjugate of α.

Solution

Let f be the minimal polynomial of α. By Exercise 6.2.2*, we have

$$0 = \sigma(f(\alpha)) = f(\sigma(\alpha))$$

so $\sigma(\alpha)$ is a conjugate of α. ■

Exercise 6.2.4*. Prove that an embedding is injective.

Solution

Suppose that $\alpha \neq \beta$. Then,

$$\sigma(\alpha - \beta)\sigma\left(\frac{1}{\alpha - \beta}\right) = \sigma(1) = 1$$

so $\sigma(\alpha - \beta) = \sigma(\alpha) - \sigma(\beta)$ is non-zero which means that $\sigma(\alpha) \neq \sigma(\beta)$. (In algebraic terms, we have shown that the kernel was trivial to prove that the morphism was injective. See Exercise A.2.13*.) ■

Exercise 6.2.5. Solve Problem 6.2.1 without field theory, i.e. using only the content of Chapter 1.

Solution

One could proceed as follow. Let S denote the sum of the α_i. Choose an $k \in [n]$, we shall prove that α_k is rational. For this, consider

$$\alpha_k = S - \sum_{i \neq k} \alpha_i.$$

The fundamental theorem of symmetric polynomials tells us that each conjugate α_k' of α_k has the form $S - \sum_{i \neq k} \alpha_i'$ where α_i' is some conjugate of α_i. Thus, we have

$$\sum_{i=1}^{n} \alpha_i = S = \sum_{i=1}^{n} \alpha_i'.$$

Since the α_i are maximal among their conjugates, proceeding as in the field theory solution, we get $\alpha_i' = \alpha_i$ for each i. But since α_k' was an arbitrary conjugate of α_k, this means α_k has only one conjugate, i.e. $\alpha_k \in \mathbb{Q}$. You can see that this was a lot messier than with field theory! ■

Exercise 6.2.6*. Check that $N_{\mathbb{Q}(\sqrt[3]{2})}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 + 2b^3 + 4c^3 - 6abc$.

Solution

Let j be a primitive cube root of unity. The norm of $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ is

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4})(a + bj\sqrt[3]{2} + cj^2\sqrt[3]{4})(a + bj^2\sqrt[3]{2} + cj\sqrt[3]{4}).$$

This is

$$\begin{aligned}
&a^3 + (b\sqrt[3]{2})^3 + (c\sqrt[3]{4})^3 + (1 + j + j^2)(a(b\sqrt[3]{2})^2 + a(c\sqrt[3]{4})^2) + (1 + j + j^2)(a^2 b\sqrt[3]{2} + a^2 c\sqrt[3]{4}) \\
&+ (1 + j + j^2)((b\sqrt[3]{2})^2(c\sqrt[3]{4}) + (b\sqrt[3]{2})(c\sqrt[3]{4})^2) + 3(j + j^2)a(b\sqrt[3]{2})(c\sqrt[3]{4}) \\
&= a^3 + 2b^3 + 4c^3 + 0 + 0 + 0 - 3(2abc) \\
&= a^3 + 2b^3 + 4c^3 - 6ab.
\end{aligned}$$

■

Remark 6.2.1

It is perhaps easier to use the definition of the norm as a determinant (see Remark C.3.5). One can check that the matrix of the linear map $x \mapsto (a + b\sqrt[3]{2} + c\sqrt[3]{4})x$ in the basis $1, \sqrt[3]{2}, \sqrt[3]{4}$ is

$$\begin{bmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{bmatrix}$$

which has determinant

$$a\left(a^2 - 2bc\right) - 2c\left(ba - 2c^2\right) + 2b(b^2 - ac) = a^3 + 2b^3 + 4c^3 - 6abc.$$

6.3 Galois Theory

Exercise 6.3.1*. Check that $K(\alpha_1, \ldots, \alpha_n)/K$ is Galois and prove that any Galois extension has this form.

Solution

$K(\alpha_1, \ldots, \alpha_n)/K$ is Galois because K-embeddings send α_i to some other α_j so send $K(\alpha_1, \ldots, \alpha_n)$ to itself and are thus all automorphisms. Conversely, if L/K is Galois, let α be a primitive element for L and $\alpha_1, \ldots, \alpha_n$ its conjugates. Then,

$$L = K(\alpha) = K(\alpha_1, \ldots, \alpha_n)$$

since L/K is Galois. ■

Exercise 6.3.2*. Can you write the Galois group of a quadratic extension L/K in a way that doesn't depend on L or K? (More specifically, show that the Galois groups of quadratic extensions are all isomorphic.)

Solution

The embeddings of a quadratic extension $K(\sqrt{d})/K$ are the identity and the conjugation $a + b\sqrt{d} \mapsto a - b\sqrt{d}$. The Galois group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ (with addition): the identity is sent to 0 and the conjugation to 1: conjugation composed with conjugation gives the identity, i.e. $1 + 1 = 0$. (Coincidentally the only group with two elements is $\mathbb{Z}/2\mathbb{Z}$ so we could have directly concluded that they were isomorphic.) ■

Exercise 6.3.3*. Check that the Galois group is a group under composition. (You may assume that each element has an inverse, this will be proven later as a corollary of Theorem 2.5.1.)

Solution

There are two things to check: that the operation is associative and that it has an identity. The former is trivial since composition is associative, and the latter too since $\sigma \circ \mathrm{id} = \mathrm{id} \circ \sigma = \sigma$ for any embedding σ. ■

Exercise 6.3.4. Let L/K be Galois and $K \subseteq M \subseteq L$ be an intermediate field. Prove that $\mathrm{Emb}_K(M)$ is a system of representatives of $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$, where the quotient means $\mathrm{Gal}(L/K)$ modulo $\mathrm{Gal}(L/M)$, i.e. we say $\sigma' \equiv \sigma$ if $\sigma^{-1} \circ \sigma' \in \mathrm{Gal}(L/M)$. (Our quotient A/B is more commonly though of as the set of *right-cosets* of B in A, i.e. the sets Ba for $a \in A$ (which we just wrote as a in our case).) (See also Exercise A.3.14†.)

Solution

Extend any embedding $\sigma \in \mathrm{Emb}_K(M)$ to an embedding $\sigma' \in \mathrm{Emb}_K(L) = \mathrm{Gal}(L/K)$. This is a well defined map from $\mathrm{Emb}_K(M)$ to $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$: if φ and ψ are equal on M, then $\psi^{-1} \circ \varphi$ is the identity on M so is in $\mathrm{Gal}(L/M)$ as wanted.

This map is clearly injective, to show that it is bijective we just follow our argument in the other way. Let $\sigma \in \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$. We prove that its image on M is well defined: if $\sigma' \equiv \sigma$ then σ and σ' have the same images on M since $\sigma^{-1} \circ \sigma'$ is the identity on M. ■

Exercise 6.3.5. Prove Proposition 6.2.4 using Exercise 6.3.4. (This is a bit technical.)

Solution

We have $N_{M/K} = \prod_{\sigma \in \mathrm{Emb}_K(M)} \sigma$ and

$$N_{L/K} \circ N_{M/L} = \prod_{\varphi \in \mathrm{Emb}_K(L)} \varphi \circ \prod_{\psi \in \mathrm{Emb}_L(M)} \psi.$$

We would like to say that this is $\prod_{\varphi,\psi} \varphi \circ \psi$ and then show that $\varphi \circ \psi$ correspond to the K-embeddings of M but there is one problem: $\operatorname{im} \psi$ is in general not contained in L, the domain of φ. Thus, let F be the *Galois closure* of M, i.e., if $M = K(\alpha)$, then $F = K(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the conjugates of α. Using Exercise 6.3.4, we extend embeddings of L to embeddings of F.

Let $G_K = \mathrm{Gal}(F/K)$, $G_M = \mathrm{Gal}(F/M)$ and $G_L = \mathrm{Gal}(F/L)$. By Exercise 6.3.4, we have $N_{M/K} = \prod_{\sigma \in G_K/G_M} \sigma$ and

$$N_{L/K} \circ N_{M/L} = \prod_{\varphi \in G_K/G_L} \varphi \circ \prod_{\psi \in G_M/G_L} \psi = \prod_{\varphi \in G_K/G_L, \psi \in G_L/G_M} \varphi \circ \psi.$$

To conclude, we prove that if φ_i are a system of representatives of G_K/G_L and ψ_j of G_L/G_M, then $\varphi_i \circ \psi_j$ is a system of representatives of G_K/G_M. By looking at the cardinalities, it sufficies to show that they are distinct in G_K/G_M. Thus, suppose that

$$\varphi'\psi' \equiv \varphi\psi \pmod{G_M} \iff \varphi^{-1}\varphi'\psi' \equiv \psi \pmod{G_M}.$$

If we look at this modulo G_L, we get $\varphi^{-1}\varphi' = \mathrm{id}$, i.e. $\varphi = \varphi'$. Then if we look at the remainder modulo G_M, we have $\psi' = \psi$ which shows what we wanted. ■

Exercise 6.3.6*. Compute $\sigma_{(0,-1)} \circ \sigma_{(1,1)}$ and $\sigma_{(1,1)} \circ \sigma_{(0,-1)}$.

Solution

This follows from the fact that $\sigma_{(a,b)} \circ \sigma_{(c,d)} = \sigma_{(a+bc,bd)}$. Indeed, $\sigma_{(a,b)}$ sends ζ to

$$\sigma_{(a,b)}(\zeta^d)^b = (\zeta^d)^b = \zeta^{bd}$$

and $\sqrt[3]{2}$ to

$$\sigma_{(a,b)}(\zeta^c \sqrt[3]{2}) = (\zeta^c)^b \cdot \zeta^a \sqrt[3]{2} = \zeta^{a+bc} \sqrt[3]{2}.$$

Thus,

$$\sigma_{(0,-1)} \circ \sigma_{(1,1)} = \sigma_{(0-1\cdot 1,-1\cdot 1)} = \sigma_{(-1,-1)}$$

but

$$\sigma_{(1,1)} \circ \sigma_{(0,-1)} = \sigma_{(1+1\cdot 0,1\cdot(-1))} = \sigma_{(1,-1)}$$

■

Exercise 6.3.7*. Prove that $e_i(\sigma_1(\alpha), \ldots, \sigma_k(\alpha))$ is fixed by H for any i.

Solution

We shall prove that any symmetric polynomial f evaluated at $\sigma_i(\alpha)$ is fixed by H (this is in fact equivalent to what we need to prove by the fundamental theorem of symmetric polynomials). For this, note that

$$\sigma(f(\sigma_1(\alpha), \ldots, \sigma_k(\alpha)) = f(\sigma\sigma_1(\alpha), \ldots, \sigma\sigma_k(\alpha))$$

by a slightly generalised version of Exercise 6.2.2*. Since $\sigma_i \mapsto \sigma\sigma_i$ is a permutation of H (since H is a group!) and f is symmetric, this is exactly equal to $f(\sigma_1(\alpha), \dots, \sigma_k(\alpha))$. ■

Exercise 6.3.8*. Given two subfields A and B of a field L, define their *compositum* or *composite field* AB as the smallest subfield of L containing both A and B (in other words, the field generated by A and B). Let L/K be a finite Galois extension and A, B be intermediate fields. Prove that $\mathrm{Gal}(L/AB) = \mathrm{Gal}(L/A) \cap \mathrm{Gal}(L/B)$.

Solution

Note that any embedding which fixes both AB fixes both A and B. Hence, $\mathrm{Gal}(L/AB) \subseteq \mathrm{Gal}(L/A) \cap \mathrm{Gal}(L/B)$. Conversely, if $A = K(\alpha)$ and $B = K(\beta)$, then $AB = K(\alpha, \beta)$ and it is clear that the embeddings which fix both α and β fix AB. ■

Exercise 6.3.9*. Given two subgroups H_1, H_2 of a group H, define the subgroup they generate, $\langle H_1, H_2 \rangle$, as the smallest subgroup containing both H_1 and H_2. Let L/K be a finite Galois extension and A, B be intermediate fields. Prove that $\mathrm{Gal}(L/A \cap B) = \langle \mathrm{Gal}(L/A), \mathrm{Gal}(L/B) \rangle$.

Solution

Note that any embedding which fixes A or B fixes $A \cap B$. Hence, $\langle \mathrm{Gal}(L/A), \mathrm{Gal}(L/B) \rangle \subseteq \mathrm{Gal}(L/A \cap B)$ (if a group contains two subgroups it also contains the subgroup generated by them, by definition). Conversely, if $\langle \mathrm{Gal}(L/A), \mathrm{Gal}(L/B) \rangle$ fixes all of M, then M is fixed both by the embeddings of A and by the embeddings of B, which implies that $M \subseteq A \cap B$. This shows that $\mathrm{Gal}(L/A \cap B) \subseteq \langle \mathrm{Gal}(L/A), \mathrm{Gal}(L/B) \rangle$. ■

Exercise 6.3.10*. Prove Proposition 6.3.2.

Solution

If $H_1 \subseteq H_2$ then L^{H_1} is fixed by less embeddings than L^{H_2} so has more elements (any element fixed by the embeddings of H_2 is also fixed by the embeddings of H_1). Conversely, if $M_1 \subseteq M_2$, there are more embeddings which fix M_1 than M_2 since any embedding which fix M_2 also fix M_1. ■

Exercise 6.3.11*. Let L/K be a finite Galois extension and let M be an intermediate field. Prove that, for any $\sigma \in \mathrm{Gal}(L/K)$, $\mathrm{Gal}(L/\sigma M) = \sigma \,\mathrm{Gal}(L/M)\sigma^{-1}$. Deduce that the intermediate fields which are also Galois (over K) are $M = L^H$ where H is a *normal* subgroup of $G = \mathrm{Gal}(L/K)$, meaning that $\sigma H \sigma^{-1} = H$ for any $\sigma \in G$. In particular, if L/K is *abelian*, meaning that its Galois group is, any intermediate field is Galois over K.

Solution

If φ fixes M, $\sigma\varphi$ fixes sends M to σM and thus $\sigma\varphi\sigma^{-1}$ sends σM to itself as wanted (this is of course reversible). M is Galois over K iff it is fixed under conjugation, i.e. $\sigma M = M$ for any $\sigma \in \mathrm{Gal}(L/K)$. By the fundamental theorem of Galois theory, this is equivalent to $\mathrm{Gal}(L/M) = \mathrm{Gal}(L/\sigma M) = \sigma \,\mathrm{Gal}(L/M)\sigma^{-1}$. This proves the second part. For the third, simply note that $\sigma H \sigma^{-1} = \sigma\sigma^{-1} H = H$ when G is abelian. ■

Exercise 6.3.12*. Fill in the details of this proof of the quadratic reciprocity law.

Solution

Here is a summary of the proof. First, we prove that $\sqrt{q^*} \in \mathbb{Q}(\omega_q)$ where ω_q is a primitive qth root of unity, say $\sqrt{q^*} = f(\omega_q)$. Then, we assume that $f \in \mathbb{Z}_{(p)}[X]$, where $\mathbb{Z}_{(p)}$ denote the rational numbers with non-negative p-adic valuation. This follows for instance from Exercise 3.5.26†. After that, we apply the Frobenius morphism on both sides to get

$$\sigma_p(\sqrt{q^*}) = f(\omega_q^p) \equiv (\sqrt{q^*})^p,$$

i.e.

$$\left(\frac{p}{q}\right)\sqrt{q^*} \equiv (\sqrt{q^*})^p$$

since the Galois group of $\mathbb{Q}(\omega_q)/\mathbb{Q}(\sqrt{q^*})$ is $\{\sigma_k \mid \left(\frac{k}{q}\right) = 1\}$, i.e. these embeddings fix $\sqrt{q^*}$ and the others negate it. To see that this is necessarily the Galois group of $\mathbb{Q}(\omega_q)/\mathbb{Q}(\sqrt{q^*})$, notice that the only subgroup of cardinality $\frac{q-1}{2}$ of $\mathbb{Z}/(q-1)\mathbb{Z}$ is $2\mathbb{Z}/(q-1)\mathbb{Z}$, which corresponds to the quadratic residue once we raise a primitive root to these powers (since primitive roots are what give us an isomorphism $\mathbb{Z}/(q-1)\mathbb{Z} \simeq (\mathbb{Z}/q\mathbb{Z})^\times$).

Now that we have this equality, we can rewrite it as

$$\left(\frac{p}{q}\right) \equiv \left((-1)^{\frac{q-1}{2}}q\right)^{\frac{p-1}{2}} \pmod{p},$$

i.e.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

as wanted. ■

Exercise 6.3.13*. Convince yourself of this solution.

Solution

Here is the proof written in the correct order. We pick a primitive element r of $\mathbb{Q}(\omega)^H$, say $r = \prod_{h\in H} u - \omega^h$ for some $u \in \mathbb{Z}$ by **??**, and consider its minimal polynomial f. Then, let p be any prime not dividing n and consider an element $\zeta \in \overline{\mathbb{F}}_p$ of order n. If $p \pmod{n} \in H$, then

$$\rho_k = \prod_{h\in H} u - \zeta^{kh}$$

is in $\mathbb{F}_p$ since

$$\rho_k^p = \prod_{h\in H} u - \zeta^{khp} = \rho_k$$

as $h \mapsto hp$ is a permutation of H since $p \pmod{n} \in H$. By the fundamental theorem of symmetric polynomials,

$$\prod_{h\in H} X - f(\rho_h) \equiv \prod_{h\in H} X - f(\sigma_h(r)) = X^{\varphi(n)} \pmod{p}$$

so f has all its roots ρ_h in $\mathbb{F}_p$ as asserted.

Now, suppose for the sake of a contradiction that infinitely many $p \equiv m \pmod{n}$ are such that f has a root in $\mathbb{F}_p$. Since the roots of f are still the ρ_h, this means that, for some $h \in H$, $\rho_h \in \mathbb{F}_p$ for infinitely many $p \equiv m \pmod{n}$. Since $\rho_h \in \mathbb{F}_p$ is equivalent to $\rho_h^p = \rho_h$ and $\rho_h^p = \rho_{hp} = \rho_{hm}$,

we get

$$\rho_{hm} - \rho_h = 0$$

for infinitely many p. As a consequence, the product

$$\prod_{g \in (\mathbb{Z}/n\mathbb{Z})^\times / H} \rho_{ghm} - \rho_{gh} \equiv \prod_{g \in (\mathbb{Z}/n\mathbb{Z})^\times / H} \sigma_{ghm}(r) - \sigma_{gh} \pmod{p}$$

is divisible by infinitely many primes p by the fundamental theorem of symmetric polynomials. This implies that $\sigma_{ghm}(r) = \sigma_{gh}$ for some g, i.e. ghm and gh are in the same coset, which is false since $m \notin H$. (We can also assume that $g = 1$ by replacing ω by ω^g.) ■

Exercise 6.3.14*. Prove that the identity of a group is unique.

Solution

If e and e' are two identities than $e = ee' = e'$ so they are equal. ■

Exercise 6.3.15*. Prove the following refinement of Theorem 2.5.1: if G is a finite group and H a subgroup of G, $|H|$ divides $|G|$. Why does it imply Theorem 2.5.1?

Solution

Partition G into left-cosets aH, $a \in G$. Each coset has cardinality $|H|$, and two distinct cosets are disjoint so this is indeed a partition: if $ag = bh$ with $g, h \in H$, then $a = bhg^{-1}$ so $aH = bH$. Thus, the cardinality of a coset divides the cardinality of the union, i.e. $|H|$ divides $|G|$. When H is the subgroup generated by an element g, this means that the order of g divides the order of G. ■

6.4 Splitting of Polynomials

Exercise 6.4.1. Does there exist an $a \not\equiv 1 \pmod{n}$ such that any non-constant $f \in \mathbb{Z}[X]$ has infinitely many prime factors congruent to a modulo n?

Solution

No, a counterexample is $f = \Phi_n$. ■

6.5 Exercises

Field and Galois Theory

Exercise 6.5.1†. Let L/K be a finite separable extension of prime degree p. If $f \in K[X]$ has prime degree q and is irreducible over K but reducible over L, then $p = q$.

Solution

Let α be a root of f. On the one hand, $[L(\alpha) : K] = [L(\alpha) : K(\alpha)][K(\alpha) : K]$ is divisible by q. On the other hand,

$$[L(\alpha) : K] = [L(\alpha) : L][L : K].$$

The first factor is smaller than q so not divisible by q, and the second is p. Thus, $q \mid p$, i.e. $p = q$. ■

Exercise 6.5.2†. Let L/K be a finite Galois extension and M/K be a finite extension. Prove that $\mathrm{Gal}(LM : M) \simeq \mathrm{Gal}(L : L \cap M)$. In particular, $[LM : L] = [L : L \cap M]$. Conclude that, if L/K and M/K are Galois, we have

$$[LM : K][L \cap M : K] = [L : K][M : K].$$

Solution

For the first part, let $L = K(\alpha)$. Consider the restriction φ from $\mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/K)$ (an element of $\mathrm{Gal}(LM/M)$ is a function $\sigma : LM \to LM$ fixing M, which can be restricted to a function $\sigma : L \to L$ fixing K). This is injective, since $\sigma \in \mathrm{Gal}(LM/M)$ is determined by its value as α, and the same goes for $\sigma \in \mathrm{Gal}(L/K)$. We wish to show that the image of this restriction is $\mathrm{Gal}(L/L \cap M)$ (thus corresponding to an isomorphism between $\mathrm{Gal}(LM/M)$ and $\mathrm{Gal}(L/L \cap M)$ as wanted).

Notice for this that

$$\begin{aligned} L^{\varphi\,\mathrm{Gal}(LM/M)} &= \{x \in L \mid \sigma(x) = x \ \forall\ \sigma \in \varphi\,\mathrm{Gal}(LM/M)\} \\ &= \{x \in L \mid \sigma(x) = x \ \forall\ \sigma \in \mathrm{Gal}(LM/M)\} \\ &= M \cap L \end{aligned}$$

since $\mathrm{Gal}(LM/M)$ fixes exactly M but here we restrict it to L.

For the second part, we have $[LM : K] = [LM : L][L : K]$ by the tower law and $[LM : L] = [M : L \cap M]$ by the first part. Now, $[M : L \cap M] = \frac{[M:K]}{[L\cap M:K]}$ by the tower law again. Thus, we conclude that

$$[LM : K] = [LM : L][L : K] = [M : L \cap M][L : K] = \frac{[L : K][M : K]}{L \cap M : K]}$$

as wanted. ■

Exercise 6.5.3†. Prove that, for any n, there is a finite Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/n\mathbb{Z}$.

Solution

Pick a prime $p \equiv 1 \pmod{n}$, let ω be a primitive pth root of unity, and set $K = \mathbb{Q}(\omega)$. Note that, since K has abelian Galois group, every subfield of K is also Galois over $\mathbb{Q}$. We wish to find a subfield L such that $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/n\mathbb{Z}$. By Exercise 6.3.4, we have $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Gal}(K/\mathbb{Q})/\mathrm{Gal}(K/L)$, so we want to find a subgroup H of $\mathbb{Z}/(p-1)\mathbb{Z}$ such that

$$\Big(\mathbb{Z}/(p-1)\mathbb{Z}\Big)/H \simeq \mathbb{Z}/n\mathbb{Z}.$$

Now, note that the subgroups of $\mathbb{Z}/(p-1)\mathbb{Z}$ have the form $d \cdot \mathbb{Z}/(p-1)\mathbb{Z} \simeq \mathbb{Z}/\frac{p-1}{d}\mathbb{Z}$, and that

(e.g. by Exercise A.3.15†)

$$\Big(\mathbb{Z}/(p-1)\mathbb{Z}\Big)\Big/\Big(d\cdot\mathbb{Z}/(p-1)\mathbb{Z}\Big)\simeq\mathbb{Z}/d\mathbb{Z}.$$

Thus, if H is the subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ corresponding to $n\cdot\mathbb{Z}/(p-1)\mathbb{Z}$, we get $\mathrm{Gal}(K^H/\mathbb{Q})\simeq\mathbb{Z}/n\mathbb{Z}$ as wanted. ■

Remark 6.5.1

If we combine the structure of units from Exercise 3.5.18† with the structure of finite abelian groups from Exercise A.3.19†, we get that every finite abelian group is a Galois group $\mathrm{Gal}(K/\mathbb{Q})$ for some number field K.

Exercise 6.5.4† (Cayley's Theorem)**.** Let G be a finite group. Prove that it is a subgroup of $\mathfrak{S}_n$ for some n. Conclude that there is a finite Galois extension L/K of number fields such that $G\simeq\mathrm{Gal}(L/K)$. (This is part of the *inverse Galois problem*. So far, it has only been conjectured that we can choose $K=\mathbb{Q}$.)

Solution

We claim that $G\subseteq\mathfrak{S}_{|G|}$. Indeed, left-multiplication by g defines a permutation s_g of G, and it is clear that this is an isomorphism: $s_g\circ s_{g^{-1}}=\mathrm{id}$ and

$$s_g\circ s_h=x\mapsto hx\mapsto ghx=s_{gh}.$$

For the second part, we can consider an L such that $\mathrm{Gal}(L/\mathbb{Q})\simeq\mathfrak{S}_{|G|}$ and then take $K=L^G$ since G is a subgroup of $\mathfrak{S}_{|G|}$ by Cayley's theorem. To prove that such an L exists without invoking Exercise 6.5.22†, one can consider a prime number $p\geq n$ and a subgroup $S\simeq\mathfrak{S}_n$ of $\mathfrak{S}_p$. By Exercise 6.5.21†, there exists a number field M Galois over $\mathbb{Q}$ such that $\mathrm{Gal}(M/\mathbb{Q})\simeq\mathfrak{S}_p$. Indeed, it is clear that there exists a polynomial of degree p with real coefficients and exactly two non-real roots. We can then refine it to an irreducible polynomial with rational coefficients by replacing its coefficients by close rational numbers of p-adic valuation 1, except for its leading coefficient which we replace by a close rational number of p-adic valuation 1. This gives us a polynomial irreducible over $\mathbb{Q}$ by Eisenstein's criterion. Finally, we pick $L=M^S$. ■

Exercise 6.5.5† (Dedekind's Lemma)**.** Let L/K be a finite separable extension in characteristic 0. Prove that the K-embeddings of L are linearly independent.

Solution

Suppose for the sake of a contradiction that a non-zero linear combination annihilates the embeddings:

$$a_1\sigma_1+\ldots+a_k\sigma_k=0$$

and pick k to be minimal. Pick an element $a\in L$ such that $\sigma_1(a)\neq\sigma_k(a)$. Then,

$$a_1\sigma_1(ax)+\ldots+a_k\sigma_k(ax)=0$$

for all $x\in L$ by assumption, but this is also

$$a_1\sigma_1(a)\sigma_1(x)+\ldots+a_k\sigma_k(a)\sigma_k(x)$$

so we conclude that

$$a_1\left(1-\frac{\sigma_1(a)}{\sigma_k(a)}\right)\sigma_1+\ldots+a_{k-1}\left(1-\frac{\sigma_{k-1}(a)}{\sigma_k(a)}\right)\sigma_{k-1}=0,$$

contradicting the minimality of k. ■

Exercise 6.5.6† (Hilbert's Theorem 90)**.** Suppose L/K is a *cyclic* extension in characteristic 0, meaning its Galois group $\mathrm{Gal}(L/K)\simeq(\mathbb{Z}/n\mathbb{Z},+)$ for some n (like $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ or $\mathrm{Gal}(\mathbb{Q}(\exp(2i\pi/p))/\mathbb{Q})$). Prove that $\alpha\in L$ has norm 1 if and only if it can be written as $\beta/\sigma(\beta)$ for some $\beta\in L$, where σ is a generator of the Galois group (element of order n).

Solution

It is clear that $\beta/\sigma(\beta)$ has norm 1 for any β. Now suppose α has norm 1 and let $\sigma\in\mathrm{Gal}(L/K)$ be a generator. By Exercise 6.5.5†, pick a γ such that

$$\beta=\sum_{k=0}^{n-1}\sigma^k(\gamma)\prod_{i=0}^{k-1}\sigma^i(\alpha)$$

is non-zero. Then,

$$\begin{aligned}\alpha\sigma(\beta)&=\sum_{k=0}^{n-1}\sigma^{k+1}(\gamma)\prod_{i=0}^{k-1}\sigma^{i+1}(\alpha)\\&=\sigma^n(\gamma)\alpha\sigma(\alpha)\cdot\ldots\cdot\sigma^{n-1}(\alpha)+\sum_{k=1}^{n-1}\sigma^k(\gamma)\prod_{i=0}^{k-1}\sigma^i(\alpha)\\&=\gamma N_{L/K}(\alpha)+\sum_{k=1}^{n-1}\sigma^k(\gamma)\prod_{i=0}^{k-1}\sigma^i(\alpha)\\&=\beta\end{aligned}$$

since $N_{L/K}(\alpha)=1$ by assumption. Thus, $\alpha=\beta/\sigma(\beta)$ as wanted. ■

Remark 6.5.2

This theorem gives us very interesting corollaries such as Exercise 7.5.11†: $x+y\sqrt{d}$ has norm 1 iff $x+y\sqrt{d}=\frac{a+b\sqrt{d}}{a-b\sqrt{d}}=\frac{a^2+db^2}{a^2-db^2}+\frac{2ab}{a^2-db^2}\sqrt{d}$.

Exercise 6.5.8† (Lüroth's Theorem)**.** Let K be a field and L a field between K and $K(T)$. Prove that there exists a rational functions $f\in K(T)$ such that $L=K(f)$.

Solution

The proof given here is taken from Bergman [3]. Without loss of generality, suppose that $L\neq K$. Given an element $h\in K(T)[X]$ express it as $h=f(T,X)/g(T)$ with coprime $f,g\in K[T,X]$ (g is constant in X) and define its *height* $\mathrm{ht}(h)$ as $\max(\deg_T(f),\deg_T(g))$. Now, pick any element of minimal height $u=f(T)/g(T)\in L$. We will prove that

$$f(X)-ug(X)$$

is the minimal polynomial of T both over L and $K(u)$. This implies that $[K(T):K(u)]=[K(T):$

$L]$ and $K(u) \subseteq L(u)$, i.e. $L = K(u)$ as desired.

Without loss of generality, we may assume that $\deg f \neq \deg g$, by replacing u by $u+t$ where $t \in K$ is such that $f+tg$ has degree less than $\deg f$ if $\deg f + \deg g$. Similarly, we can assume that $\deg f > \deg g$ by replacing u by $1/u$ if necessary. Finally, by multiplying u by a constant, we can suppose that f and g are monic. That way, the polynomial $f(X) - ug(X)$ is monic in X of degree $\deg f$. Note that, when $c = a(T,X)/b(T)$ is monic in X, $b(T)$ divides the leading coefficient of X of a so $\deg_T a \geq \deg_T b$ which implies that $\mathrm{ht}(c) = \deg_T(a)$. In particular, $\mathrm{ht}(cd) = \mathrm{ht}(c) + \mathrm{ht}(d)$ for polynomials c, d monic in X.

Suppose now that $f(X) - ug(X)$ is divisible by another monic polynomial $\pi = \sum_i u_i X^i \in L[X]$. We have

$$\mathrm{ht}(\pi(X)) \geq \mathrm{ht}(u_k) \geq \mathrm{ht}(u) = \mathrm{ht}(f(X) - ug(X))$$

where k is chosen so that u_k is non-constant. Hence, we conclude that, if $f(X) - ug(X) = \pi(X)\tau(X)$, we have $\mathrm{ht}(\tau) = 0$, i.e. $\tau = h(X) \in K[X]$. This h divides both f and g: indeed, 1 and u are linearly independent since $u \notin K$ so $f/h + ug/h \in K(T)[X]$ implies that f/h and g/h are in $K[X]$. This is of course impossible if τ is non-constant since f and g are coprime. Hence, $f(X) - ug(X)$ is the minimal polynomial of T over L.

The second part is a lot easier. Suppose that $\pi = \sum_i f_i(X)u^i \in K[u][X]$ with $f_i \in K[X]$ vanishes at $X = T$. We will prove that $\deg_X \pi \leq \mathrm{ht}(u) = \deg f$, thus showing that $f(X)ug(X)$ is the minimal polynomial of T over $K(u)$. Let $m = \deg_u \pi$. We have

$$0 = g(T)^{m-1}\pi(T) = f_m(T)f(T)^m/g(T) + \sum_{i=0}^{m-1} f_i(X)f(T)^i g^{m-1-t}.$$

Note that every term in the second sum is a polynomial, hence $f_m(T)f(T)^m/g(T)$ is too: $g(T)$ divides $f_m(T)$ since f and g are coprime so

$$\deg_X \pi \geq \deg f_m \geq \deg f = \mathrm{ht}\, u$$

as claimed. ■

nth Roots

Exercise 6.5.9†. Let K be a field, p a prime number, and α an element of K. Prove that $X^p - \alpha$ is irreducible over K if and only if it has no root.

Solution

Suppose that $X^p - \alpha$ is reducible for some $\alpha \neq 0$. We will show that α is a pth power in K. Let f be a non-trivial factor of $X^p - \alpha$, say of degree $k \in [p-1]$. Its constant term has the form $\omega\alpha^{k/p}$ by Vieta's formula (we are working in a field extension where $X^p - \alpha$ splits here), where ω is a pth root of unity. Thus, $\alpha^k := \beta^p$ is a pth power. If m is the inverse of k modulo p, say $mk = np + 1$, we get

$$\alpha = \frac{\alpha^{mk}}{\alpha^{np}} = \left(\frac{\beta^{mk}}{\alpha^n}\right)^p$$

as wanted. ■

Exercise 6.5.10†. Let $f \in K[X]$ be a monic irreducible polynomial and p a rational prime. Suppose that $(-1)^{\deg f} f(0)$ is not a pth power in K. Prove that $f(X^p)$ is also irreducible.

Solution

Suppose that $f(X^p)$ is reducible and let α be a root of f. By Lemma 6.1.1, $X^p - \alpha$ is reducible over $K(\omega)$, where ω is a primitive pth root of unity. By Exercise 6.5.9†, α is a pth power in $K(\omega)$, say $g(\alpha)^p$. Let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α. Then, by Vieta's formulas,

$$(-1)^n f(0) = \prod_{k=1}^{n} \alpha_k = \prod_{k=1}^{n} g(\alpha_k)^p = \left(\prod_{k=1}^{n} g(\alpha_k) \right)^p$$

is a pth power. ■

Exercise 6.5.11† (Vahlen, Capelli, Redei)**.** Let K be a field and $\alpha \in K$. When is $X^n - \alpha$ irreducible over K?

Solution

Suppose that $X^m - \alpha$ and $X^n - \alpha$ are irreducible over K. Then, so is $X^{mn} - \alpha$. Indeed, suppose that β is a root of $X^{mn} - \alpha$. Then, $[K(\beta) : K]$ is divisible by $[K(\beta^m) : K] = n$ and $[K(\beta^n) : K] = m$, which implies that it's divisible by mn as well since they are coprime. Thus, $[K(\beta) : K] = mn$ as wanted since it's clearly at most mn.

Hence, it suffices to study the case where $n = p^k$ is a prime power. First, suppose that p is odd. Then, we prove by induction that $X^{p^k} - \alpha$ is irreducible if and only if α is not a pth power, the base case being Exercise 6.5.9†. For the induction step, by Exercise 6.5.10†, if $f = X^{p^{k+1}} - \alpha$ is reducible, then $(-1)^{p^{k+1}} f(0) = \alpha$ is a pth power. For $p = 2$ we get $-\alpha$ which could be a square while α isn't, except if K has characteristic 2 since we then $\alpha = -\alpha$. Thus, we are already done if $\operatorname{char} K = 2$ so we may now suppose that $\operatorname{char} K \neq 2$.

Finally, it remains to study $X^{2^k} - \alpha$. We claim that, for $k \geq 2$, this is irreducible iff α is a square or -4 times a fourth power. One implication is Sophie Germain's identity: if $\alpha = -4\beta^4$, then

$$X^2 + 4\beta^4 = (X^2 + 2\beta X + 2\beta^2)(X^2 - 2\beta X + 2\beta^2).$$

It remains to prove that $X^{2^k} - \alpha$ is irreducible if α is not a square or -4 times a fourth power. Suppose that $X^{2^{k+1}} - \alpha$ is reducible. Then, $\alpha = -\beta^2$ for some β by Exercise 6.5.10†. Since α is not a square, -1 isn't as well. Let γ be a root of $X^{2^{k+1}} - \alpha$. We have $\gamma^{2^k} = i\beta$ for some $i^2 = -1 \in \overline{K}$. We will prove that $X^{2^r} - i\beta$ is irreducible over $K(i)$, thus showing that

$$[K(\gamma) : K] = [K(\gamma) : K(i)][K(i) : K] = 2^k \cdot 2 = 2^{k+1}$$

as wanted. If it were reducible, $i\beta$ would have the form $-(u + vi)^2 = (v + ui)^2$ for some $u, v \in K$. This gives us $u^2 - v^2 = 0$ and $\beta = 2uv$ so

$$\alpha = -\beta^2 = -4u^4$$

as wanted.

We can summarise the previous discussion as follows.

- $X^n - \alpha$ is irreducible iff α is not a pth power for any $p \mid n$, and not -4 times a fourth power in the case that $4 \mid n$ and $\operatorname{char} K \neq 2$.
- As a corollary, if α is not -4 times a fourth power or $4 \nmid n$ or $\operatorname{char} K = 2$, the minimal polynomial of $\sqrt[n]{\alpha}$ is $X^{n/d} - \sqrt[n]{\alpha^d}$ where $d \mid n$ is the greatest integer such that α^d is an nth power.

■

Exercise 6.5.12†. Let $n \geq 1$ be an integer and ζ a primitive nth root of unity. What is the Galois group of $\mathbb{Q}(\sqrt[n]{2}, \zeta)$ over $\mathbb{Q}$?

Solution

Knowing the embeddings of $\mathrm{Gal}(\zeta, \sqrt[n]{2})$ is equivalent to knowing the conjugates of $\sqrt[n]{2}$ over $\mathrm{Gal}(\zeta)$. By Exercise 6.5.11† and Problem 6.3.3, we know that the minimal polynomial of $\sqrt[n]{2}$ is $X^{n/2} - \sqrt{2}$ if $\sqrt{2} \in \mathrm{Gal}(\zeta)$ and $2 \mid n$, and $X^n - 2$ otherwise. The embeddings are thus

$$\sigma_{(a,b)} : \begin{cases} \zeta^2 \mapsto \zeta^{2a} \\ \sqrt[n]{2} \mapsto \zeta^b \sqrt[n]{2} \end{cases}$$

for independent $a \in \left(\mathbb{Z}/\frac{n}{2}\mathbb{Z}\right)^\times$ and $b \in \mathbb{Z}/n\mathbb{Z}$ in the first case, and

$$\sigma_{(a,b)} : \begin{cases} \zeta \mapsto \zeta^a \\ \sqrt[n]{2} \mapsto \zeta^b \sqrt[n]{2} \end{cases}$$

for independent $a \in (\mathbb{Z}/nZ)^\times$ and $b \in \mathbb{Z}/n\mathbb{Z}$ in the second case. (One may note that neither of these Galois groups are abelian for $n \geq 3$.) Since $\sqrt{2}$ is in $\mathbb{Q}(\zeta)$ iff $8 \mid n$ by Exercise 6.5.27, we are done. ■

Exercise 6.5.13†. Let $n \geq 1$ be an integer and $p_1, \ldots, p_m$ rational primes. Prove that

$$[\mathbb{Q}(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_m}) : \mathbb{Q}] = n^m.$$

(This is a generalisation of Exercise 4.6.24†.)

Solution

Suppose that the degree is strictly smaller than n^m, i.e. a non-trivial linear combination of powers is zero:

$$\sum_{i=1}^{k} b_i \sqrt[n]{a_i} = 0$$

for non-zero rational numbers $b_1, \ldots, b_k$ and distinct nth-powers-free positive integers $a_1, \ldots, a_k$. By mulyiplying this equation by $\sqrt[n]{a_1^{n-1}}$, we may assume that $a_1 = 1$. We will prove that $b_1 = 0$, thus reaching a contradiction. Let K be a Galois extension of $\mathbb{Q}$ containing all $\sqrt[n]{a_i}$ with Galois group G. Take the sum of the equations

$$\sum_{i=1}^{k} b_i \sigma(\sqrt[n]{a_i}) = 0,$$

over $\sigma \in G$. Exercise 6.5.11† shows that the sum of the conjugates of $\sqrt[n]{a_i}$ is zero for $i \neq 1$. Since the action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathbb{Q}(\alpha)$ restricts to multiple copies of $\mathrm{Emb}(\mathbb{Q}(\alpha))$ for any $\alpha \in \overline{\mathbb{Q}}$, the sum $\sum_{\sigma \in G} \sqrt[n]{a_i}$ is zero for any $i \neq 1$. Thus, we are left with the same

$$\sum_{\sigma \in G} b_1 \sigma(1) = b_1 |G|,$$

which means $b_1 = 0$ as wanted. ■

Exercise 6.5.14† (Kummer Theory)**.** Let L/K be a finite Galois extension in characteristic 0. Suppose that $\mathrm{Gal}(L/K) \sim \mathbb{Z}/n\mathbb{Z}$. If K contains a primitive nth root of unity, prove that $L = K(\alpha)$ for some $\alpha^n \in K$.

Solution

Let σ be a generator of $\mathrm{Gal}(L/K)$ and let $\omega \in K$ be a primitive nth root of unity. If we find a non-zero $\alpha \in L$ such that $\sigma(\alpha) = \omega\alpha$, we are done, since, by iterating σ, we get $\sigma^k(\alpha) = \omega^k\alpha$, i.e. L is generated by the nth root α of some element of K_{i+1} (as can be seen from considering its norm for instance). For this, consider

$$f = \frac{X^n - 1}{X - \omega} = X^{n-1} + \omega X^{n-2} + \ldots + \omega^{n-1}.$$

We have $0 = \sigma^n - \mathrm{id} = (\sigma - \omega\mathrm{id}) \circ (f(\sigma))$, hence, $\alpha = f(\sigma)(\beta)$ works for any β. We only need to ensure that $\alpha \neq 0$, and this follows from the linear independence of the embeddings from Exercise 6.5.5†. ■

Exercise 6.5.15† (Artin-Schreier Theorem)**.** Let L/K be a finite extension such that L is algebraically closed. Prove that $[L : K] \leq 2$.

Solution

First, we prove that $[L : K]$ is a power of 2. Suppose otherwise. Using Cauchy's theorem and the fundamental theorem of Galois theory, we can find an intermediate field M such that $[L : M] = p$ where $p \mid [L : K]$ is an odd prime. Thus, suppose without loss of generality that $[L : K] = p$. Consider a primitive pth root of unity $\omega \in L$. Since ω has degree at most $p - 1$ over K, its degree is not divisible by p which means that ω must be in K. Then, Kummer theory from Exercise 6.5.14† implies that $L = K(\alpha)$ for some $\beta = \alpha^p \in K$. Since α is not in K, β is not a pth power in K. This implies that the polynomial $X^{p^2} - \beta$ is irreducible over K by Exercise 6.5.11†. This is a contradiction since any element algebraic over K has degree at most p by assumption.

Thus, $[L : K] = 2^k$ for some k. In particular, any polynomial of odd degree has a root in K. Indeed, group the roots of a polynomial $f \in K[X]$ in disjoint orbits of the form

$$\sigma_{1,i}(\alpha_i), \ldots, \sigma_{k_i,i}(\alpha_i)$$

where α_i is a root of f and $\sigma_{1,i}, \ldots, \sigma_{k_i,i}$ form a set of representatives of $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/K(\alpha_i))$. In other words, we are simply asking that, for a fixed i, $\sigma_{j,i}(\alpha_i)$ go through every conjugate of α_i exactly once. Then, if $\alpha_i \notin K$,

$$k_i = |\mathrm{Gal}(L/K)/\mathrm{Gal}(L/K(\alpha_i))| = 2^k/|\mathrm{Gal}(L/K(\alpha_i))|$$

is even since $\mathrm{Gal}(L/K(\alpha_i)) < 2^k$. If this is the case for all i, then f has an even number of roots, contradicting the assumption that its degree is odd. (This is a generalisation of the fact that non-real roots always come by pair of complex conjugates.)

Accordingly, any polynomial of odd degree has a root in K. We will prove that any element $\alpha \in K$ is such that α is a square of $-\alpha$ is. Assuming this, notice that these are exactly the assumptions we used in our proof that $\mathbb{C} = \mathbb{R}(i)$ is closed, in Section B.3. Hence, $L = K(i)$ where $i^2 = -1$, which means in particular that $[L : K] \leq 2$ as wanted.

It remains to show this claim. For this, notice that $X^{2^{k+1}} - \alpha$ is reducible over K since L/K has degree 2^k. By Exercise 6.5.11†, this implies that α is a square, or -4 times a fourth power, and thus minus a square. ■

Constructibility and Solvability

Exercise 6.5.16†. Given two points, you are allowed to draw the line between them, as well as the circle of center one of the points going through the other. Initially, you may start with the points $(0, 0)$

and $(0,1)$ and define additional points that way. We say a real number r is *constructible* if the point $(0,r)$ is constructible. Prove that, if x and y are constructible, so are $x+y$, xy, $-x$, $\sqrt{|x|}$, and $\frac{1}{x}$ if $x \neq 0$.

Solution

■

Exercise 6.5.17†. Prove that a real number is constructible if and only if it is algebraic and the degree of its splitting field, meaning the field generated by its conjugates, is a power of 2. Deduce that, using only a (non-graded) ruler and a compass,

1. A regular n-gon is constructible if and only if $\varphi(n)$ is a power of 2.
2. It is not always possible to trisect an angle.
3. Given a square with area A, it is not possible to construct a square with area $2A$.

Solution

Note that $\alpha = \cos\left(\frac{2}{\pi}n\right)$ is constructible iff its degree $\varphi(n)/2$ (for $n \geq 2$) is a power of 2. In that case, we can construct the point $(\cos(2k\pi/n), 0)$ and the point $(0, \sin(2k\pi/n))$, and hence the point $(\cos(2k\pi/n), \sin(2k\pi/n))$ as well. Similarly, if we are able to trisect an angle of α, by intersecting with a vertical line we are able to construct $\cos(\alpha/3)$ (and this is equivalent). However, for $\alpha = \frac{2\pi}{3}$, we get $\cos(2\pi/9)$ which has degree 3 and is thus not constructible.

It remains to prove the characterisation of the constructible numbers. One direction is easy: when we intersect a line with a line, the field generated by the coordinates does not change, and when we intersect a line with a circle, the field generated by the coordinates becomes a quadratic extension of itself or does not change. Thus, the degree over $\mathbb{Q}$ gets multiplied by 1 or by 2 each time, and must thus be a power of 2. It is also clear that this is Galois: each time we take a square root, we could also take the other square root (this amounts to considering the other intersection with the circle). The other direction is almost given by Exercise 6.5.16†. To finish, we proceed by induction on $[K:\mathbb{Q}] = 2^k$ where K is the splitting field of α. By Cauchy's theorem 6.3.3, $\mathrm{Gal}(K/\mathbb{Q})$ has an element of order 2, and thus, K has a subfield of index 2 by the Galois correspondence, say $[K:L] = 2$. By assumption, the points of L are constructible since $[L:\mathbb{Q}] = 2^{k-1}$, and if $K = \mathbb{Q}(\alpha)$, we can recover α from L using the quadratic formula so α is also constructible by Exercise 6.5.16†. ■

Exercise 6.5.18†. We say a finite Galois extension L/K in characteristic 0 is *solvable by radicals* if there is a tower of extensions

$$K = K_0 \subset K_1 \subset \ldots \subset K_m \supseteq L$$

such that K_{i+1} is obtained from K_i by adjoining an nth root of some element of K_i to K_i, for some n. We also say a group G is *solvable* if there is a chain $0 = G_0 \subset G_1 \subset \ldots \subset G_m = G$ such that G_i is normal in G_{i+1} (see Exercise 6.3.11*) and G_{i+1}/G_i is cyclic. Prove that L/K is solvable by radicals if and only if its Galois group is. (When L is the field generated by the roots of a polynomial $f \in K[X]$, L/K being solvable by radicals means that the roots of f can be written with radicals, which explains the name.)

Solution

First, suppose that G is solvable. Consider the tower of fields $K_i = L^{G_i}$. Each K_{i+1}/K_i is Galois by Exercise 6.3.11*, with Galois group isomorphic to G_{i+1}/G_i by Exercise 6.3.4. We

wish to conclude that K_{i+1} is generated from K_i by adding the nth root of an element. The problem is that this is almost always false, since then K_{i+1}/K_i wouldn't be Galois extension! Hence, we shall to consider the tower of fields $K_i(\omega)$, where ω be a primitive $|G|$th root of unity (since $|G_{i+1}/G_i| \mid |G|$ by Lagrange). By Exercise 6.5.2†, the Galois group of $K_{i+1}(\omega)/K_i(\omega)$ is isomorphic to the subgroup $\mathrm{Gal}(K_{i+1}/K_i(\omega) \cap K_{i+1})$ of $\mathrm{Gal}(K_{i+1}/K_i)$, and hence cyclic as well, say of order n. Then, Kummer theory from Exercise 6.5.14† states that $K_{i+1}(\omega)$ is $K_i(\omega)(\alpha_i)$ for some $\alpha_i^n \in K_i(\varepsilon)$. This gives us that L/K is solvable as wanted since we have the tower

$$K \subseteq K(\omega) \subseteq K(\omega)(\alpha_1) \subseteq \dots K(\omega)(\alpha_m) = L(\omega) \supseteq L.$$

Now, we need to prove that G is solvable if L/K is. Note that, if G is solvable, then so is G/H for any normal subgroup H. Indeed, if $0 = G_0 \subseteq \dots \subseteq G_m = G$, then $H = G_0H/H \subseteq \dots \subseteq G_mH/H = G/H$ and

$$(G_{i+1}H/H)/(G_iH/H) \simeq G_{i+1}H/G_iH$$

by Exercise A.3.15†, and this is cyclic, since if gG_i generates G_{i+1}/G_i, then $gG_{i+1}H$ generates $G_{i+1}H/G_iH$.

Set $M = K_m(\omega)$, where ω is a root of unity chosen so that $K_{i+1}(\omega)/K$ is Galois for each i (and in particular M/K is). Since $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(M/K)/\mathrm{Gal}(M/L)$ is a quotient of $\mathrm{Gal}(M/K)$, it suffices to prove that $\mathrm{Gal}(M/K)$ is solvable. There is only one thing left to do now: add ω to all K_i so that K_{i+1}/K_i becomes Galois and we can simply take its Galois group. This gives us that $\mathrm{Gal}(M/K(\omega))$ is solvable, but we what we want is for $\mathrm{Gal}(M/K)$ to be. However,

$$\mathrm{Gal}(M/K)/\mathrm{Gal}(M/K(\omega)) \simeq \mathrm{Gal}(K(\omega)/K)$$

is cyclic, so we can add to a chain $0 = G_0 \subseteq \dots \subseteq G_m = \mathrm{Gal}(M/K(\omega)) \subseteq \mathrm{Gal}(M/K)$ to conclude that $\mathrm{Gal}(M/K)$ is solvable as wanted!

We shall however explain a bit more why taking Galois groups gives us cyclic extensions. Let us write $M_i = K_i(\omega) = M_{i-1}(\alpha_i)$ for some $\alpha_i^{n_i} \in M_i$. Then, $\mathrm{Gal}(M_{i+1}/M_i)$ is cyclic since its embeddings have the form $\sigma(\alpha_i) = \omega^k\alpha$ for some k, so they form a subgroup of $\mathbb{Z}/n\mathbb{Z}$ where n is the order of ω, which is thus cyclic. If we let $G_i = \mathrm{Gal}(M/M_i)$, we have

$$0 = \mathrm{Gal}(M/M) = G_m \subseteq \dots \subseteq G_0 = \mathrm{Gal}(M/K(\omega))$$

and

$$G_i/G_{i+1} = \mathrm{Gal}(M/M_i)/\mathrm{Gal}(M/M_{i+1}) \simeq \mathrm{Gal}(M_i/M_{i+1})$$

by Exercise 6.3.4 which is cyclic as wanted. ■

Exercise 6.5.19†. Let $n \geq 1$ be an integer. Prove that $\mathfrak{S}_n$ is not solvable for $n \geq 5$. Conclude from Exercise 6.5.21† that some polynomial equations are not solvable by radicals.[1] (This is quite technical.)

Solution

The usual proof proves a lot more than just the non-solvability of $\mathfrak{S}_n$: it completely characterise all its descending chains of normal subgroups. More precisely, the normal subgroups of $\mathfrak{S}_n$ are the symmetric group $\mathfrak{S}_n$, the alternating group of even permutations (Definition C.3.2) $\mathfrak{A}_n$, as well as the trivial group $0 = \{\mathrm{id}\}$, while the only strict normal subgroup of $\mathfrak{A}_n$ is 0 (we say it's *simple*). However, this demands a lot of work, and since this is a number theory book and not an algebra one, we will not prove this. See Weinstraub [31], appendix A, section 3 for an account of the more general result.

[1] If one only wants to show that there is no general formula, one doesn't need to do the first part since the general polynomial $\prod_{i=1}^n X - A_i \in \mathbb{Q}(A_1, \dots, A_n)[X]$ already has Galois group $\mathfrak{S}_n$ (where $A_1, \dots, A_n$ are formal variables).

Note that if G is solvable, so is any of its subgroups H: $0 = G_0 \subseteq \ldots \subseteq G_m = G$ becomes

$$0 = G_0 \cap H \subseteq \ldots \subseteq G_m \cap H = G$$

and

$$\frac{G_{i+1} \cap H}{G_i \cap H} = \frac{(H \cap G_{i+1}) \cap G_i}{G_i}$$

by the second isomorphism theorem (see Exercise A.3.15†). This is a subgroup of G_{i+1}/G_i, which is cyclic, so it's cyclic itself. Hence, to show that $\mathfrak{S}_n$ is not solvable for $n \geq 5$, it suffices to prove that $\mathfrak{S}_5$ is not solvable. This can be done using a computer for instance, as there are only 120 elements. However, we will still present a somewhat more satisfactory proof.

We first prove that the only strict subgroup G of $\mathfrak{S}_n$ such that $\mathfrak{S}_n/G$ is abelian is $\mathfrak{A}_n$. Let H be such a subgroup. Note that, in cycle notation, we have

$$\begin{aligned}(1,2,4)(1,4,2) &= \mathrm{id}\\ (1,3,5)(1,5,3) &= \mathrm{id}\\ (1,2,3) &= (1,2,4)(1,3,5)(1,4,2)(1,5,3).\end{aligned}$$

Hence, if we let $f((1,2,4)) = x$ and $f((1,3,5)) = y$, we get

$$f((1,2,3)) = f((1,2,4)(1,3,5)(1,4,2)(1,5,3)) = xyx^{-1}y^{-1} = \mathrm{id}$$

in $\mathfrak{S}_n/G$ which is abelian by assumption. By symmetry, G contains all 3-cycles. It remains to prove that the 3-cycles generate $\mathfrak{A}_n$. Since $\mathfrak{A}_n$ is generated by the products of two transpositions, it suffices to prove that 3-cycles generate all products of two transpositions. This follows from the following equalities

$$\begin{aligned}(i,k,j) &= (i,j)(i,k)\\ (i,k,j)(i,k,\ell) &= (i,j)(k,\ell)\end{aligned}$$

for distinct i,j,k,ℓ.

Now, we need to prove that $G = \mathfrak{A}_5$ has no non-trivial normal subgroup. For this, we shall find the conjugacy classes $\mathcal{C}_g = \{hgh^{-1} \mid h \in G\}$. We can check that there are 5 such conjugacy classes, of respective size 1, corresponding to the identity, 15, 20, 12 and 12. Assume we have proven this. Since a normal subgroup H is a union of conjugacy classes by definition, it must contain the trivial class of size 1, corresponding to the identity. But then, it is easy to see that its cardinality only divides $|\mathfrak{A}_5| = 60$ for $H = \mathfrak{A}_5$ or $H = \{\mathrm{id}\}$. Thus, by Lagrange's theorem from Exercise 6.3.15*, H must be $\mathfrak{A}_5$ or $\{\mathrm{id}\}$ as wanted. But $\mathfrak{A}_5/\{\mathrm{id}\} \simeq A_5$ is not cyclic so we are done.

To prove that these are the cardinalities of the conjugacy classes, recall Remark 6.5.3:if $\gamma = (i_1, \ldots, i_k)$ is a cycle, we have

$$\sigma\gamma\sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k)).$$

This means that the conjugates of 3-cycles are all 3-cycles, thus forming the class of size 20 (it is not hard to see that we can pick an even σ). Similarly, there are two pairs of conjugacy classes of 5-cycles of size 12, because this time our σ will not be even. It only remains to prove that all 15 products of two transpositions $(i,j)(k,\ell)$ with i,j,k,ℓ distinct are conjugate. This is not very hard:

$$\sigma(i,j)(k,\ell)\sigma^{-1} = (\sigma(i),\sigma(j))(\sigma(k),\sigma(\ell)).$$

Hence, if $(i',j')(k',\ell')$ is another product of two transpositions, we pick $\sigma(i) = i'$, $\sigma(j) = j'$, $\sigma(k) = k'$ and $\sigma(\ell) = \ell'$. If this has even signature we are done, otherwise exchange i' and j'.

Finally, to conclude that some algebraic numbers are not expressible by radicals, we only need to prove that there exist polynomials of prime degree with exactly two non-real roots. One example is $X^2 - 4X - 2$ (irreducible by Eisenstein's criterion). ■

Exercise 6.5.20†. We say a finite Galois extension L/K of real fields, i.e. $L \subseteq \mathbb{R}$, is *solvable by real radicals* if there is a tower of extensions

$$K = K_0 \subset K_1 \subset \ldots \subset K_m \supseteq L$$

such that K_{i+1} is obtained from K_i by adjoining the nth root of some positive element of K_i to K_i. Prove that L/K is solvable by real radicals if and only if $[L : K]$ is a power of 2.

Solution

Without loss of generality, by adding more intermediate fields, we can suppose that $K_{i+1} = K_i(\alpha_i)$, where $\alpha_i^p \in K$ for some prime p. The key point is that, if $[L : K]$ is equal to an odd prime q, then $[L(\alpha) : K(\alpha)]$ is also equal to q for any $\alpha^p \in K$. Let's see first how this implies our result: if $[L : K]$ is not a power of 2, say is divisible by an odd prime q, $\mathrm{Gal}(L/K)$ has an element of order q by Cauchy's theorem 6.3.3, and hence L has a subfield of index q by the Galois correspondence, say $[L : M] = q$. Then, L/M is also solvable by real radicals, but

$$[L : M] = [L(\alpha_1) : K(\alpha_1)] = [L(\alpha_1, \alpha_2) : K(\alpha_1, \alpha_2)] = \ldots,$$

i.e. $[LK_i : MK_i] = [L : M]$ by our lemma. This is a contradiction for $i = m$: we get $[L : L] = [L : M]$. Conversely, if $[L : K]$ is a power of 2, say $L = K(\alpha)$, L has a subfield M of index 2, i.e. $[L : M] = 2$. Then, α can be obtained by real radicals from M using the quadratic formula. Repeating this process yields that $[L : K]$ is solvable by square roots as well.

Hence, it suffices to show that, when $[L : K] = q$, $[L(\alpha) : K(\alpha)] = q$ as well. Note that $\mathrm{Gal}(L(\alpha)/K(\alpha))$ is a subgroup of $\mathrm{Gal}(L/K)$, as we saw in Exercise 6.5.2†. In particular, $[L(\alpha) : K(\alpha)]$ divides q so must be 1 or q. Suppose for the sake of a contradiction that it is 1 (in particular $\alpha \notin K$). This gives $L \subseteq K(\alpha)$, so q divides $[K(\alpha) : K]$, which is p by Exercise 6.5.9†. Hence, $p = q$ and $L = K(\alpha)$. But this is impossible, since the conjugates of α are not in L as primitive qth roots of unity are not real since $q \geq 3$. ■

Exercise 6.5.21†. Let p be a prime number and $G \subseteq \mathfrak{S}_p$ a subgroup containing a transposition τ (see the paragraph after Definition C.3.2) and an element γ of order p. Prove that $G = \mathfrak{S}_p$. Deduce that, if $f \in \mathbb{Q}[X]$ is an irreducible polynomial of degree p with precisely two non-real complex roots, then the Galois group of the field generated by its roots (called its *splitting field*, because it is a field where it splits) over $\mathbb{Q}$ is $\mathfrak{S}_p$.

Solution

Suppose without loss of generality that τ is $1 \leftrightarrow 2$ (which we usually denote in cycle notation $\tau = (1, 2)$). A power of γ, say γ^k sends 1 to 2. Suppose without loss of generality that γ. By symmetry between $3, 4, \ldots,$, we can in fact suppose that γ is the cycle $(1, 2, \ldots, p)$ which sends $1 \to 2 \to \ldots \to p \to 1$. We will prove that G contains all transpositions and thus must be $\mathfrak{S}_p$ since transpositions generate the symmetric group by Exercise C.3.12*. Notice that $\gamma\tau\gamma^{-1}$ is the transposition $(2, 3)$ since it goes $2 \to 1 \to 2 \to 3$ and $3 \to 2 \to 1 \to 2$ and must is the identity else where since τ is. Similarly, $\gamma^k\tau\gamma^{-k}$ is the transposition $(k + 1, k + 2)$. Since

$$(1, k) = (1, k - 1)(k - 1, k)(1, k - 1),$$

a straightforward induction tells us that $(1, k) \in G$ for all k. Finally, $(1, i)(1, j)(1, i) = (i, j)$ so G contains all transpositions as wanted.

Now, suppose f is an irreducible polynomial of degree p with only two non-real roots. Since its degree divides the degree of its splitting field, its Galois group G has an element of order p by Cauchy's theorem 6.3.3. Moreover, it contains the transposition corresponding to the complex conjugation, which exchanges the two non-real roots. ■

Exercise 6.5.22†. Let n be a positive integer. Prove that there is a number field K, Galois over $\mathbb{Q}$, such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathfrak{S}_n$. (You may assume the following result of Dedekind: if $f \in \mathbb{Z}[X]$ is a polynomial, for any prime number p not dividing the discriminant Δ of f, the Galois group of f over $\mathbb{F}_p$ is a subgroup of the Galois group of f over $\mathbb{Q}$.[2])

Solution

Let's look at what the injection of $\mathrm{Gal}_{\mathbb{F}_p}(f)$ in $\mathrm{Gal}_{\mathbb{Q}}(f)$ gives us. We use the cycle notation $\sigma_1 \cdot \ldots \cdot \sigma_k$ to mean the permutation σ which decomposes into the disjoint cycles $\sigma_1, \ldots, \sigma_k$. A cycle

$$\sigma : i_1 \mapsto i_2 \mapsto \ldots \mapsto i_k \mapsto i_1$$

will be denoted $(i_1, \ldots, i_k)$ (it is the identity on other elements).

We know from Chapter 4 that $\mathrm{Gal}_{\mathbb{F}_p}(f)$ is generated by the Frobenius morphism. Write $f \equiv f_1 \cdot \ldots \cdot f_k \pmod{p}$ with distinct irreducible polynomials $f_i \in \mathbb{F}_p[X]$ of respective degrees n_i (there is no repeated root since p doesn't divide the discriminant). Then, the Frobenius morphism acts as a cycle on the roots of each f_i, of length n_i. Hence, Frob can be written in cycle notation as $\sigma_1 \cdot \ldots \cdot \sigma_k$ with σ_i a cycle of length n_i. This implies, by assumption, that $\mathrm{Gal}_{\mathbb{Q}}(f)$ also has an element of the form.

We have a lot of freedom on the factorisation of f modulo primes, so let's put aside the question of ensuring that the primes we choose do not divide the discriminant of f for the moment and focus on the rest of the proof. Suppose that $G = \mathrm{Gal}_{\mathbb{Q}}(f)$ has an n-cycle σ, a transposition τ, and an $(n-1)$-cycle ψ. Without loss of generality, by symmetry, suppose that $\psi = (2, 3, \ldots, n)$. By consdering $\sigma^m \tau \sigma^{-m}$ for an appropriate m, we can assume that τ is the transposition $(1, k)$ for some k. Indeed, by symmetry, if $\sigma = (1, 2, \ldots, n)$ and $\tau = (i, j)$, we have $\sigma^m \tau \sigma^{-m} = (i+m, j+m)$. Since

$$\psi = (k, k+1, \ldots, n, 2, 3, \ldots, k-1),$$

we can, again by symmetry, suppose that in fact $k = 2$. To conclude, we will prove that $(1, 2)$ and $(2, 3, \ldots, n)$ generate $\mathfrak{S}_n$, thus implying that $G = \mathfrak{S}_n$ as desired. By Exercise C.3.12*, it suffices to prove that they generate all transpositions. Since $\varphi := \tau\psi = (1, 2, \ldots, n) \in G$, we can proceed as we did in Exercise 6.5.21†: $(m+1, m+2) = \varphi^m \tau \varphi^{-m} \in G$, and since $(1, m) = (1, m-1)(m-1, m)(1, m-1)$, we have $(1, m) \in G$ for all m by induction. Finally, since $(i, j) = (1, i)(1, j)(1, i)$, we have all transpositions and we are done: $G = \mathfrak{S}_n$.

It remains to prove that we can ensure that the Galois group contains an n-cycle, a transposition, and an $n-1$ cycle. For this, pick three primes p, q, r. Then, choose a polynomial $f \in \mathbb{Z}[X]$, using the Chinese remainder theorem, such that

- f is irreducible modulo p,
- f factorises as a product of a polynomial of degree 1 and an irreducible polynomial of degree $n-1$ modulo q, and
- f factorises as a product of an irreducible polynomial of degree 2 and $n-2$ polynomials of degree of degree 1 modulo r (choose r sufficiently large so that there is no common root).

Then, $\mathrm{Gal}_{\mathbb{F}_p}(f)$ contains an n-cycle, $\mathrm{Gal}_{\mathbb{F}_q}(f)$ a transposition, and $\mathrm{Gal}_{\mathbb{F}_p}(f)$ an $(n-1)$-cycle. In addition, the discriminant of f is not divisible by p, q, r since f has no repeated factor modulo these primes. Hence, by Dedekind's result and our previous observation, $\mathrm{Gal}_{\mathbb{Q}}(f) = \mathfrak{S}_n$ as desired. ■

[2]The Galois group of a polynomial f over a field F is defined as the Galois group of its splitting field over F, i.e. as $\mathrm{Gal}(F(\alpha_1, \ldots, \alpha_k)/F)$, where $\alpha_1, \ldots, \alpha_k$ are the roots of f.

Remark 6.5.3

If $\gamma = (i_1, \ldots, i_k)$ is a cycle, then it is straightforward to see that $\sigma\gamma\sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k))$. This explains how we found our relations.

Cyclotomic Fields

Exercise 6.5.23†. Let ω be a primitive nth root of unity. When is Φ_m irreducible over $\mathbb{Q}(\omega)$?

Solution

Let ζ be a primitive mth root of unity and let ξ be a primitive $\operatorname{lcm}(m,n)$th root of unity. Φ_m is irreducible over $\mathbb{Q}(\omega)$ if and only if ζ has degree $\varphi(m)$ over $\mathbb{Q}(\omega)$. We have, by Problem 6.3.2,

$$[\mathbb{Q}(\zeta,\omega):\mathbb{Q}(\omega)] = [\mathbb{Q}(\xi):\mathbb{Q}(\omega)] = \frac{[\mathbb{Q}(\xi):\mathbb{Q}]}{[\mathbb{Q}(\omega):\mathbb{Q}]} = \frac{\varphi(\operatorname{lcm}(m,n))}{\varphi(n)}.$$

Thus, Φ_m is irreducible over $\mathbb{Q}(\omega)$ if and only if $\varphi(\operatorname{lcm}(m,n)) = \varphi(m)\varphi(n)$. Finally, note that we always have

$$\begin{aligned}\varphi(m)\varphi(n) &= \prod_{p|m} p^{v_p(m)-1}(p-1)\prod_{q|n} q^{v_q(n)-1}(q-1)\\ &= \prod_{p|m,n} p^{\min(v_p(m),v_p(n))-1}(p-1)\prod_{q|mn} q^{\max(v_p(m),v_p(n))-1}(q-1)\\ &= \varphi(\operatorname{lcm}(m,n))\varphi(\gcd(m,n))\end{aligned}$$

since the $p-1$ factor is repeated twice when $p \mid m,n$ and only once otherwise, with exponent $v_p(m)+v_p(n)-2 = \min(v_p(m),v_p(n))-1+\max(v_p(m),v_p(n))-1$ in the first case and exponent $\max(v_p(m),v_p(n))-1$ in the second. Thus, Φ_n is irreducible over $\mathbb{Q}(\omega)$ iff $\varphi(\gcd(m,n)) = 1$, i.e. iff $\gcd(m,n) = 1$ or 2. ■

Exercise 6.5.25†. Let n be an integer and $m \in \mathbb{Z}/n\mathbb{Z}$ be such that $m^2 \equiv 1 \pmod{n}$. Prove that there exist infinitely many primes congruent to m modulo n, provided that there exists at least one which is greater than n^2. (It is also true that our Euclidean approach to special cases of Dirichlet's theorem only works for $m^2 \equiv 1 \pmod{n}$, see **??**.)

Solution

Suppose that $p > n^2$ is a prime congruent to $m \pmod{n}$. We have already done the case $m = 1$ in Exercise 3.3.8* and the case $m = -1$ in Theorem 4.4.1, so suppose $m \neq \pm 1$. Let ω be a primitive nth root of unity, and let $H = \{1, m\}$. Let also σ_k denote the embedding $\omega \mapsto \omega^k$. Consider $g = (X-\omega)(X-\omega^m)$. For large k, we have $\mathbb{Q}(g(N)) = \mathbb{Q}(\omega)^H$ by Remark 6.3.2. Now, let f be the minimal polynomial of $g(N)$, where N is an integer that we will choose later. Consider discriminant

$$\Delta = \pm\prod_i f'(\sigma_i(g(N)))$$

by Exercise 3.2.2*. This is a polynomial of degree $\varphi(n)(\varphi(n)-1) < n^2$ in N, which can't always be divisible by p since $p > n^2$ by assumption. Hence, there is some N such that this is not divisible by p. Choose this N to also be divisible by n, using CRT.

We are now ready to finish. Suppose for the sake of a contradiction that there are a finite number of such primes $p_1 = p, p_2, \ldots, p_k$. Let Q be the product of the possible exceptions, i.e. the prime divisors of f which are not congruent to 1 or m modulo p. Pick an M congruent to $g(N)$ or $g(N)+p$ modulo p^2, so that $v_p(f(M)) = 1$ using Corollary 5.3.1. Pick also M to be divisible by

$np_2 \cdot \ldots \cdot p_k Q$. Since

$$f(0) = \pm\Phi_n(N) \equiv \Phi_n(0) = \pm 1 \pmod{n}$$

, we know that the prime factors of $f(0)$ are all congruent to 1 modulo n. Thus, the prime factors of $f(M) \equiv f(0) \pmod{np_2 \cdot \ldots \cdot p_k Q}$ are all congruent to 1 or m modulo n since we don't run in an exception. Since, by assumption, the only primes congruent to m modulo n are the p_i, this means that $f(N)$ is divisible only by primes congruent to 1 modulo n, and potentially by p too. Since we also have $v_p(N) = 1$, we get $f(N) \equiv \pm m \pmod{n}$ depending on its sign. This is a contradiction if $m \neq \pm 1$ since we have $f(N) \equiv f(0) \equiv \pm 1 \pmod{n}$. ■

Exercise 6.5.26† (Mann)**.** Suppose that $\omega_1, \ldots, \omega_n$ are roots of unity such that $\sum_{i=1}^n a_i\omega_i = 0$ for some $a_i \in \mathbb{Q}$ and $\sum_{i\in I} a_i\omega_i \neq 0$ for any non-empty strict subset $I \subseteq [n]$. Prove that $\omega_i^m = \omega_j^m$ for any $i, j \in [n]$ where m is the product of primes at most n.

Solution

Suppose without loss of generality that $\omega_1 = 1$, by dividing everything by ω_1. Next, let m the smallest integer such that $\omega_i^m = 1$ for all m, let p be a prime factor of m and write $m = p^k r$ for some $p \nmid s$. We will prove that $p \leq n$ and $r \leq 1$, thus yielding the wanted result. Let $\omega = \exp\left(\frac{2i\pi}{p^k}\right)$ be a primitive p^kth root of unity, and write $\omega_i = \zeta^{t_i}\omega^{s_i}$ for some $s_i \leq p-1$, where $\zeta = \exp\left(\frac{2i\pi}{m/p}\right)$ is a primitive m/pth root of unity. Inded, if $\omega_i = \exp\left(\frac{2\ell i\pi}{m}\right)$, we have

$$\zeta^{t_i}\omega^{s_i} = \exp\left(\frac{t_i p + s_i r}{m}\right)$$

and it suffices to choose $s_i r \equiv \ell \pmod{p}$. The equation

$$\sum_{i=1}^n a_i\omega_i = 0$$

thus becomes $f(\omega) = 0$ for some $f \in \mathbb{Q}(\zeta)$ of degree at most $p-1$, which is non-zero by assumption. Let's compute the degree of ω over $\mathbb{Q}(\zeta)$:

$$[\mathbb{Q}(\omega,\zeta) : \mathbb{Q}(\zeta)] = \frac{[\mathbb{Q}(\omega,\zeta) : \mathbb{Q}]}{[\mathbb{Q}(\zeta) : \mathbb{Q}]} = \frac{\varphi(p^k r)}{\varphi(p^{k-1} r)} = \begin{cases} p-1 \text{ if } k = 1 \\ p \text{ if } k \geq 2 \end{cases}.$$

Thus, we already reach a contradiction if $k \geq 2$ since f has degree less than p. Hence, $k = 1$ and we must have

$$f = \alpha(1 + X + \ldots + X^{p-1}).$$

However, f has at most k non-zero coefficients, which implies $p \leq k$ as wanted. ■

Exercise 6.5.27. Which quadratic subfields does a cyclotomic field contain?

Solution

Given a positive integer m, we let ω_m denote a primitive mth root of unity. We have seen that, when p is odd, $\sqrt{\left(\frac{-1}{p}\right)p} \in \mathbb{Q}(\omega_p)$. Hence, $\sqrt{\left(\frac{-1}{p}\right)p} \in \mathbb{Q}(\omega_n)$ whenever $p \mid n$. This implies that $\sqrt{\left(\frac{-1}{m}\right)} \in \mathbb{Q}(\omega_n)$ whenever $m \mid n$ is odd, and $\left(\frac{-1}{m}\right)$ is the Jacobi symbol. In Problem 6.3.3, we also saw that $\sqrt{2} \in \mathbb{Q}(\omega_8)$ so $\sqrt{2} \in \mathbb{Q}(\omega_n)$ when $8 \mid n$. Also, we of course have $\sqrt{-1} \in \mathbb{Q}(\omega_4)$ so

$\sqrt{-1} \in \mathbb{Q}(\omega_n)$ when $4 \mid n$. To summarise the above discussion, $\mathbb{Q}(\omega_n)$ contains all the quadratic subfields of the form

- $\mathbb{Q}(\sqrt{\left(\frac{-1}{m}\right)})$ when m is a squarefree positive odd divisor of n
- $\mathbb{Q}(\sqrt{\pm m})$ when m is a squarefree odd divisor of n and $4 \mid n$
- $\mathbb{Q}(\sqrt{\pm 2m})$ when $8 \mid n$ and m is a squarefree odd divisor of n.

We claim that these are all the subfields of $\mathbb{Q}(\omega_n)$. Suppose that $\mathbb{Q}(\omega_n)$ contains $\mathbb{Q}(\sqrt{m})$ with minimal m not of the wanted form. Then, $\mathbb{Q}(\omega_n)$ and $\mathbb{Q}(\omega_{4m})$ have a non-trivial intersection so n and $4m$ have gcd at least 3 by **??**. First suppose that they have a common odd prime divisor p. Then $\mathbb{Q}(\omega_n)$ contains $\mathbb{Q}(\sqrt{\left(\frac{-1}{p}\right) m/p})$ which contradicts the minimality of m. Otherwise, if the gcd is exactly 4, the intersection is $\mathbb{Q}(i)$ so $m = -1$ which is in our list of described subfields. Otherwise, the gcd is at least 8 which means that m is odd and $\sqrt{2} \in \mathbb{Q}(\omega_n)$ so $\mathbb{Q}(\omega_n)$ contains $\mathbb{Q}(\sqrt{m/2})$ which contradicts the minimality of m again. ■

Exercise 6.5.28†. Prove the Gauss and Lucas formulas: given an odd squarefree integer $n > 1$, there exist polynomials $A_n, B_n, C_n, D_n \in \mathbb{Z}[X]$ such that

$$4\Phi_n = A_n^2 - (-1)^{\frac{n-1}{2}} n B_n^2 = C_n^2 - (-1)^{\frac{n-1}{2}} n X D_n^2.$$

Deduce that, given any non-zero rational number r, there are infinitely many pairs of distinct rational prime (p, q) such that r has the same order modulo p and modulo q.

Solution

Let ω be a primitive nth root of unity and set $n^* = \left(\frac{-1}{n}\right) n = (-1)^{\frac{n-1}{2}} n$. Notice that the expression $A^2 - n^* B^2$ is a norm in $\mathbb{Q}[X](\sqrt{n^*})$. Exercise 6.5.27 tells us that $\mathbb{Q}(\omega)$ contains $\mathbb{Q}(\sqrt{n^*})$, so we just need to write Φ_n in the form UV where U, V are polynomials conjugate in $\mathbb{Q}[X](\sqrt{n^*})$. This is easy: in $\mathbb{Q}(\omega)/\mathbb{Q}(\sqrt{n^*})$, we can see that the conjugates of ω are ω^k for $\left(\frac{k}{n}\right) = 1$. Indeed, $\sigma_k :\mapsto \omega^k$ fixes $\sqrt{p^*}$ iff $\left(\frac{k}{p}\right) = 1$ and negates it otherwise. Since $\left(\frac{k}{n}\right) = \prod_{p|n} \left(\frac{k}{p}\right)$, σ_k negates an even number of $\sqrt{p^*}$, i.e. fixes $\sqrt{n^*} = \prod_{p|n} \sqrt{p^*}$ iff $\left(\frac{k}{n}\right) = 1$. This means that $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}(\sqrt{n^*})) = \{\sigma_k \mid \left(\frac{k}{n}\right) = 1\}$. Thus, we can write

$$\Phi_n = \prod_{\left(\frac{k}{n}\right)=1} X - \omega^k \prod_{\left(\frac{k}{n}\right)=-1} X - \omega^k$$

as wanted. Note that the ring of integers of $\mathbb{Q}(\sqrt{n^*})$ is $\mathbb{Z}\left[\frac{1+\sqrt{n^*}}{2}\right]$ so the coefficients of A and B are in $\frac{1}{2}\mathbb{Z}$ which gives us the factor of 4 on the left as wanted. We also have the formula

$$A_n + B_n\sqrt{n^*} = \prod_{\left(\frac{k}{n}\right)=1} X - \omega^k,$$

which can be used to derive the explicit formulas

$$2A_n = \prod_{\left(\frac{k}{n}\right)=1} X - \omega^k + \prod_{\left(\frac{k}{n}\right)=-1} X - \omega^k$$

and

$$2B_n\sqrt{n^*} = \prod_{\left(\frac{k}{n}\right)=1} X - \omega^k - \prod_{\left(\frac{k}{n}\right)=-1} X - \omega^k.$$

For Lucas's formula, we wish to have

$$\Phi_n(X)\Phi_n(-X)\Phi_n(X^2) = C_n(X^2)^2 - n^*(XD_n(X^2))^2.$$

For this consider the equality

$$\begin{aligned} U_n + V_n\sqrt{n^*} &= (A_n(X) + B_n(X)\sqrt{n^*})(A_n(-X) - B_n(-X)\sqrt{n^*}) \\ &= (A_n(X)A_n(-X) - n^*B_n(X)B_n(-X)) + \sqrt{n^*}(A_n(-X)B_n(X) - A_n(X)B_n(-X)). \end{aligned}$$

Note that $U_n(-X) = U_n(X)$ so $U_n = C_n(X^2)$ for some C_n while $V_n(-X) = -V_n(X)$ so $V_n = XD_n(X^2)$ for some D_n. These C_n and D_n are the ones we were looking for.

Finally, we prove that, for any non-zero $r = a/b \in \mathbb{Q}$, there are infinitely many integers n such that (the numerator of) $\Phi_n(a,b)$ has at least two distinct prime factors, unless $r = \pm 1$ but these r have the same order modulo any odd prime. One piece of notation: by multiplying the equality $4\Phi_n(X/Y) = C_n(X/Y)^2 - X/YD_n(X/Y)^2$, we get an equality of the form

$$4\Phi_n(X,Y) = C_n(X,Y)^2 - XYD_n(X)^2.$$

Without loss of generality, a and b are coprime and $b > 0$. First, we treat the case where ab has even dyadic valuation. If we restrict ourselves to odd n, we can also assume that a is positive, since we then have $\Phi_{2n}(a,b) = \Phi_n(-a,b)$. Thus, suppose that a and b are positive and coprime and let m be the squarefree part of ab. Suppose that $m \neq 1$. Then, if p is a prime factor of m, we have

$$4\Phi_{p^km}(a,b) = 4\Phi_m(a^{p^k}, b^{p^k}) = C_m(a^{p^k}, b^{p^k})^2 - m(ab)^{p^k}D_m(a^{p^k}, b^{p^k})^2.$$

Here is the magic: $m(ab)^{p^k}$ is a perfect square so this is a difference of two squares which factorises! It remains to prove that the two factors are not both of the form $2q^\ell$ for some prime q. Indeed, we can ensure that all prime factors q of $\Phi_{p^km}(a,b)$ are such that a/b has order p^km modulo q: the only other possible prime factors are common divisors of a and b, of which there are none, and prime factors of $m \mid ab$, which also implies that they are common divisors of a and b. Finally, since $\deg C_n > \deg D_n$, the two factors are asymptotically equivalent (the quotient goes to 1), so if they both had the form $2q^\ell$, they would need to be equal for large p. This is of course impossible. When $m = 1$, we can consider the equation $\Phi_3 = X^2 + X + 1 = (X+1)^2 - X$ to get a difference of squares in the same way (replace p by 3) and the same conclusion applies.

It only remains to treat the case where ab has odd dyadic valuation. In that case, we shall derive a formula of the form

$$\Phi_{2n} = C_n(X)^2 - nXD_n(X)^2$$

for any squarefree even n. It is clear that the above argument will work as before as long as the squarefree part m of ab has an odd prime factor p, i.e. is not equal to 2 since it's even by assumption. We can simply consider $\Phi_{12} = X^4 - X^2 + 1 = (X^2 + X + 1)^2 - 2X(X+1)^2$ in that case (and raise X to the power 3^k for large k).

Hence, it suffices to show that there exist such polynomials C_n and D_n for even squarefree n. Without loss of generality, we can assume that n is positive since $\Phi_{2n}(X) = \Phi_n(X^2) = \Phi_{2n}(-X)$. Our formula is equivalent to $\Phi_{4n}(X) = C_n(X^2)^2 - n(XD_n(X^2))^2$. We will now proceed as before. Let ω be a primitive nth root. By Exercise 6.5.27, $\mathbb{Q}(\omega)$ contains $\mathbb{Q}(\sqrt{n})$ and we have $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}(\sqrt{n}) = \{\sigma_k \mid \left(\frac{k}{n}\right) = 1\}$, by definition of the Kronecker symbol $\left(\frac{k}{n}\right) = \left(\frac{k}{n/2}\right)\left(\frac{k}{2}\right)$, where $\left(\frac{k}{2}\right) = (-1)^{\frac{k^2-1}{8}}$. Indeed, it is easy to see that σ_k fixes $\sqrt{2}$ iff $\left(\frac{k}{2}\right) = 1$, and the rest follows from a parity argument as before. Thus,

$$U_n + \sqrt{n}V_n = \prod_{\left(\frac{k}{n}\right)=1} X - \omega^k$$

satisfty $\Phi_{4n} = U_n^2 - nV_n^2$. We wish to show that U_n is a polynomial in X^2 and V_n is X times a polynomial in X^2, i.e. that U_n is even and V_n odd. This follows from the equalities

$$2U_n = \prod_{(\frac{k}{n})=1} X - \omega^k + \prod_{(\frac{k}{n})=-1} X - \omega^k$$

and

$$2\sqrt{n}V_n = \prod_{(\frac{k}{n})=1} X - \omega^k - \prod_{(\frac{k}{n})=-1} X - \omega^k.$$

Indeed, we have

$$\begin{aligned}\prod_{(\frac{k}{n})=\pm 1} -X - \omega^k &= \prod_{(\frac{k}{n})=\pm 1} X + \omega^k \\ &= \prod_{(\frac{k}{n})=\pm 1} X - \omega^{k+2n} \\ &= \prod_{(\frac{k}{n})=\mp 1} X - \omega^k\end{aligned}$$

since $\left(\frac{k+2n}{p}\right) = \left(\frac{k}{p}\right)$ for any odd prime p but $\left(\frac{k+2n}{2}\right) = -\left(\frac{k}{2}\right)$ as $2n \equiv 4 \pmod 8$. This concludes the proof. ■

Remark 6.5.4

Schinzel has generalised our identities to give a wide class of cyclotomic polynomials with at least two distinct prime factors. See [25].

Miscellaneous

Exercise 6.5.30†. Let $f \in \mathbb{Q}[X]$ be an irreducible polynomial with exactly one real root of degree at least 2. Prove that the real parts of its non-real roots are all irrational.

Solution

Let α be the real root and let β be any non-real root. Suppose for the sake of a contradiction that $2\Re(\beta) = \beta + ol\beta$ is rational. Let σ be an embedding of $\mathbb{Q}(\beta)$ sending β to α. Then, $\alpha + \sigma(\overline{\beta}) = 2\Re(\beta)$ since $2\Re(\beta)$ is rational so fixed by σ, which implies that $\sigma(\overline{\beta})$ is real. Since α is the only real root by assumption, we get $\sigma(\overline{\beta}) = \alpha$ which implies that $\alpha = \Re(\beta)$ is rational and is a contradiction. ■

Remark 6.5.5

It is not true at all in general that embeddings commute with complex conjugation. For instance, over $\mathbb{Q}(\sqrt[3]{2}, j)$, the embedding $\sigma : \sqrt[3]{2} \mapsto \sqrt[3]{2}j, j \mapsto j^2$ sends $\sqrt[3]{2}j^2$ to $\sqrt[3]{2}$, and $\sqrt[3]{2}j$ to $\sqrt[3]{2}j^2$, which are not complex conjugate.

Exercise 6.5.31†. Let K be a number field of degree n. Prove that there are elements $\alpha_1, \ldots, \alpha_n$ of K such that

$$\mathcal{O}_K \subseteq \alpha_1\mathbb{Z} + \ldots + \alpha_n\mathbb{Z}.$$

By showing that any submodule of a $\mathbb{Z}$-module generated by n elements is also generated by n elements, deduce that $\mathcal{O}_K$ has an *integral basis*, i.e. elements $\beta_1, \ldots, \beta_n$ such that

$$\mathcal{O}_K = \beta_1\mathbb{Z} + \ldots + \beta_n\mathbb{Z}.$$

Solution

Let $\alpha \in \mathcal{O}_K$ be a primitive element for K. Suppose that $\sum_{i=0}^{n-1} a_i \alpha^i \in \overline{\mathbb{Z}}$ for some $a_i \in \mathbb{Q}$. We will prove that the denominator of the a_i are bounded. Set $\mathrm{Emb}(K) = \{\sigma_1, \ldots, \sigma_n\}$. Consider the following system of equations:

$$\begin{cases} a_0 + a_1\sigma_1(\alpha) + \ldots + a_{n-1}\sigma_1(\alpha)^{n-1} = A_1 \\ a_0 + a_1\sigma_2(\alpha) + \ldots + a_{n-1}\sigma_2(\alpha)^{n-1} = A_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_0 + a_1\sigma_n(\alpha) + \ldots + a_{n-1}\sigma_n(\alpha)^{n-1} = A_n \end{cases}.$$

for some $A_1, \ldots, A_n \in \overline{\mathbb{Z}}$. This can be written in matrix form as

$$\begin{bmatrix} 1 & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha)^n \\ 1 & \sigma_2(\alpha) & \cdots & \sigma_2(\alpha)^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_n(\alpha) & \cdots & \sigma_n(\alpha)^n \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{bmatrix}.$$

Write this equation as $Ma = A \iff a = AM^{-1}$. Then, by Exercise C.3.18*, we know that the a_i are linear combinations of algebraic integers divided by $\det M$. However,

$$D := \det(M)^2 = \pm \prod_{i \neq j} \sigma_i(\alpha) - \sigma_j(\alpha) \in \mathbb{Z}$$

by Vandermonde, so that $Da_i \in \overline{\mathbb{Z}}$ for any i, i.e. $Da_i \in \mathbb{Z}$ since $Da_i \in \mathbb{Q}$. (This is the application of the exact value of the Vandermonde determinant promised in Remark C.3.2!) This shows that

$$\mathcal{O}_K \subseteq \frac{1}{D}\mathbb{Z} + \ldots + \frac{1}{D}\alpha^{n-1}\mathbb{Z}$$

as wanted.

It remains to prove the second part. We proceed by induction on the number of generators n (it is trivial when $n = 0$). Suppose that $M = \sum_{i=1}^{n} \alpha_i \mathbb{Z}$ and $N \subseteq M$ is a submodule. Define M' as $\sum_{i=2}^{n} \alpha_i \mathbb{Z}$, and N' as $N \cap M'$. Using the induction hypothesis, set $N' = \beta_2\mathbb{Z} + \ldots + \beta_n\mathbb{Z}$. Now, consider the S set of rational integers k such that $k\alpha_1 + \beta \in N$ for some $\beta \in N'$. Since N is a $\mathbb{Z}$-module, A is an additive subgroup of $\mathbb{Z}$ which thus has the form $b_1\mathbb{Z}$ for some b. (Indeed, pick the smallest positive element $b_1 \in A$ and consider the remainder of the Euclidean division of $k \in A$ by b_1 to show that $b_1 \mid k$, as otherwise A would contain a smaller positive element.)

Set

$$\beta_1 = b_1\alpha_1 + b_2\alpha_2 + \ldots + b_n\alpha_n \in N$$

for some $b_2, \ldots, b_n$. If $\alpha = \sum_{i=1}^{n} a_i\alpha_i$ is an element of N, we have $a_1 \in A$ so $a_1 = kb_1$ for some k and thus $\alpha - k\beta \in N'$. Hence,

$$N = \beta_1\mathbb{Z} + N' = \beta_1\mathbb{Z} + \beta_2\mathbb{Z} + \ldots + \beta_n\mathbb{Z}$$

as wanted. ■

Exercise 6.5.32†. Let $f \in \mathbb{Q}[X]$ be an irreducible polynomial of prime degree p and denote its roots by $\alpha_0, \ldots, \alpha_{p-1}$. Suppose that

$$\lambda_0\alpha_0 + \ldots + \lambda_{p-1}\alpha_{p-1} \in \mathbb{Q}$$

for some rational λ_i. Prove that $\lambda_0 = \ldots = \lambda_{p-1}$.

Solution

Let $K = \mathbb{Q}(\alpha_0, \ldots, \alpha_{p-1})$. Since $p = [\mathbb{Q}(\alpha_0) : \mathbb{Q}]$ divides $[K : \mathbb{Q}] = |\operatorname{Gal}(K/\mathbb{Q})$, $\operatorname{Gal}(K/\mathbb{Q})$ has an element σ of order p by Cauchy's theorem 6.3.3. By relabelling the α_i, suppose without loss of generality that σ sends α_k to α_{k+1}. Let $S = \sum_{i=0}^{p-1} \lambda_i \alpha_i \in \mathbb{Q}$. Then, by applying σ to the equation $\sum_{i=0}^{p-1} \lambda_i \alpha_i$ multiple times, we get the following system of equations in the α_i

$$\begin{cases} \lambda_0\alpha_0 + \ldots + \lambda_{p-1}\alpha_{p-1} = S \\ \lambda_0\alpha_1 + \ldots + \lambda_{p-1}\alpha_0 = S \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \lambda_0\alpha_{p-1} + \ldots + \lambda_{p-1}\alpha_{p-2} = S. \end{cases}$$

Since this system has a non-trivial solution (the trivial one being $\alpha_0 = \ldots = \alpha_{p-1}$), its determinant must be zero. By Exercise C.5.6, this circulant determinant is

$$g(\omega)g(\omega^2) \cdot \ldots \cdot g(\omega^{p-1})$$

where ω is a primitive pth root of unity and $g = \sum_{i=0}^{p-1} \lambda_i X^i$. Thus, $g(\omega^k) = 0$ for some $k \in [p-1]$. Since p is prime, the ω^k for $k \in [p-1]$ are all conjugate with minimal polynomial $\Phi_p = 1 + \ldots + X^{p-1}$. Thus, $\Phi_p \mid g$. Since $\deg \Phi_p \geq \deg g$, we have $g = \lambda\Phi_p$ for some $\lambda \in \mathbb{Q}$. This yields $\lambda_0 = \ldots = \lambda_{p-1} = \lambda$ as wanted. (Conversely, all such λ_i work since the sum of the conjugates of an algebraic number is rational.) ■

Exercise 6.5.33† (TFJM 2019)**.** Let N be an odd integer. Prove that there exist infinitely many rational primes $p \equiv 1 \pmod{N}$ such that $x \mapsto x^{n+1} + x$ is a bijection of $\mathbb{F}_p$, where $n = \frac{p-1}{N}$.

Solution

The idea is that, if $\omega + 1$ is an Nth power in $\mathbb{F}_p$ for all Nth roots of unity $\omega \in \mathbb{F}_p$, then f is a bijection. Indeed, this means that $(\omega+1)^n = (\omega+1)^{\frac{p-1}{N}} = 1$ for any k. Then, if $x^{n+1} + x = y^{n+1} + y$, by raising the equation to the $n = \frac{p-1}{N}$th power, since x^n and y^n are Nth roots of unity, we get

$$x^n = y^n$$

as $(x^n+1)^n = (y^n+1)^n = 1$. But then, our original equation becomes

$$x(1 + x^n) = y(1 + y^n)$$

so $x = y$ or $x^n = -1$. However, the latter implies $(-1)^N = x^{p-1} = 1$ which is impossible since N is odd by assumption.

, Thus, we are done if we find infinitely many p such that $\omega + 1$ is an Nth power in $\mathbb{F}_p$ for any Nth root $\omega \in \mathbb{F}_p$. Let $\zeta \in \mathbb{C}$ be a complex primitive Nth root of unity. Consider the polynomial

$$f = \prod_{i,j} X - \zeta^i \sqrt[N]{\zeta^j + 1},$$

which has integer coefficients by the fundamental theorem of symmetric polynomials. Then, any $p \in \mathcal{P}_{\text{split}}(f)$ which doesn't divide N nor $f(0)$ works (the idea is that $\sqrt[N]{\omega+1}$ will exist in $\mathbb{F}_p$ for such a p). Let p be such a prime, and let $\alpha_1, \ldots, \alpha_m$ be the roots of f in $\mathbb{F}_p$. We will prove that, for any root Nth root of unity $\omega \in \overline{\mathbb{F}}_p$, $\omega+1$ is the Nth power of an element of $\mathbb{F}_p$ (in particular, $\omega + 1 \in \mathbb{F}_p$). Note that $\omega + 1 \neq 0$ since $p \nmid f(0)$. By the fundamental theorem of symmetric polynomials, we have

$$\prod_{\omega} \prod_{k} \omega + 1 - \alpha_k^n = \prod_{k} \prod_{i,j} \zeta^k - (\zeta^i \sqrt[N]{\zeta^j + 1})^n = 0$$

as wanted. ■

Exercise 6.5.34†. Let $f \in \mathbb{C}(X)$ be a rational function, and suppose f sends rational integers algebraic integers to algebraic integers. Prove that f is a polynomial.

Solution

By linear algebra, f has coefficients in a number field K (which we will assume without loss of generality to be Galois). Indeed, consider the system of linear equations in the coefficients of its numerator g and denominator g

$$g(n_1) = \alpha_1 h(n_1), \dots, g(n_k) = \alpha_k h(n_k)$$

for $n_1, \dots, n_k \in \mathbb{Z}$ and $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Z}}$. It has in solution in some finite-dimensional $K := \mathbb{Q}(\alpha_1, \dots, \alpha_k)$-vector space V (the one generated by the coefficients), and thus also in K, for instance by considering a basis $1, v_1, \dots, v_m$ of V and looking at the coefficient of 1. Next, notice that for $k > \deg g + \deg h$, these conditions completely determine f: if $\frac{g(n)}{h(n)} = \frac{u(n)}{v(n)}$ for $\deg g + \deg h + 1$ values of n and some polynomials u and v of same degrees as g and h, the polynomial $gu - hv$ has more roots than its degree so must be identically zero.

Now, consider its conjugates

$$(f_1, \dots, f_k) = (\sigma_1(f), \dots, \sigma_k(f)),$$

where $\{\sigma_1, \dots, \sigma_k\} = \mathrm{Gal}(K/\mathbb{Q})$. By assumption, for any i,

$$e_i(f_1, \dots, f_k)$$

takes infinitely many values which are rational integers at rational integers. Thus, it is a polynomial by Exercise 5.5.1†. This implies that f is *integral* over the ring of polynomials $\mathbb{C}[X]$: it's a root of the monic polynomial

$$(Y - f_1) \cdot \ldots \cdot (Y - f_k) \in \mathbb{C}[X][Y].$$

However, it is also rational over $\mathbb{C}[X]$ since it is in $\mathbb{C}(X)$. Thus, an analogue of Proposition 1.1.1 shows that it must be in $\mathbb{C}[X]$, as a rational integral (over $\mathbb{C}[X]$) element of $\overline{\mathbb{C}}(X)$ ($\mathbb{C}[X]$ is a UFD so the same proof as Proposition 1.1.1 works). ■

Chapter 7

Units in Quadratic Fields and Pell's Equation

7.1 Fundamental Unit

Exercise 7.1.1*. Prove that α is invertible if and only if its norm is ± 1.

Solution

If α is invertible than so are its conjugate $\sigma_i(\alpha)$ since $\alpha\beta = 1$ transforms into $\sigma_i(\alpha)\sigma_i(\beta) = 1$. Thus, so is the product of its conjugates, i.e. its norm. But we have seen that the only invertible rational integers are ± 1. Conversely, if $\mathrm{N}(\alpha) = \pm 1$ then α times $\pm$ the product of its other conjugates is 1 so α is invertible. ■

7.2 Pell-Type Equations

Exercise 7.1.2*. Prove Proposition 7.1.1.

Solution

We have already shown that these were the only units of $\mathbb{Q}(i)$ and $\mathbb{Q}(j)$ in Chapter 2. The units of $\mathbb{Q}(\sqrt{-d})$ are the elements $a + b\sqrt{-d}$ of $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ satisfying $N(a + b\sqrt{-d}) = a^2 + db^2 = 1$ since the norm is positive so cannot be -1. For $d = 2$, there are only the trivial solutions ± 1 since $\mathcal{O}_{\mathbb{Q}(\sqrt{-2})} = \mathbb{Z}[\sqrt{-2}]$ and $|b| \geq 1$ implies $a^2 + 2b^2 \geq 2$ while $|a| \geq 2$ implies $a^2 + 2b^2 \geq 4$.

If $d \geq 5$ ($d = 4$ is not squarefree), a and b are both half integers so $a^2 + db^2 \geq \frac{5}{4} > 1$ if $|b| \geq 1$ which implies $b = 0$ from which we get $a = \pm 1$, corresponding to the units ± 1. ■

Exercise 7.2.1*. Prove that $\mathcal{O}_{\mathbb{Q}(\sqrt{u})}/\beta\mathcal{O}_{\mathbb{Q}(\sqrt{u})}$ is finite if $\beta \neq 0$.

Solution

Let α be such that $\mathcal{O} := \mathcal{O}_{\mathbb{Q}(\sqrt{u})} = \mathbb{Z}[\alpha]$ (see Proposition 2.1.1). Note that, when $\beta = m$ is a rational integer, this has exactly $m^2 = N(m)$ elements since $m \mid a + b\alpha$ iff $m \mid a, b$ (by definition $c + d\alpha$ is an algebraic integer for rational c, d iff c and d are integers).

For the general case, note that $\mathcal{O}/\beta\mathcal{O} \subseteq \mathcal{O}/N(\beta)\mathcal{O}$ since $\beta \mid N(\beta)$ so the former has a finite number of elements too. ■

7.3 Størmer's Theorem

Exercise 7.3.1*. Prove that $y_m \mid y_n$ iff $m \mid n$.

Solution

This is exactly the same as Exercise 4.3.1* but in number fields. Write $y_n = \frac{\alpha^n - \beta^n}{2\sqrt{d}}$ with $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Note that $y_m \mid y_n$ iff $\alpha^m - \beta^m \mid \alpha^n - \beta^n$ which is equivalent to $\alpha/\beta = \alpha^2$ having order dividing n modulo $\alpha^m - \beta^m$. Since its order is exactly m, this is equivalent to $m \mid n$. ■

Remark 7.3.1

This solution also works for the more general problem where α, β are in any number field K, but the difficulty lies in showing that $\mathcal{O}_K$ mod γ is finite for any non-zero $\gamma \in \mathcal{O}_K$, so that talking about the order makes sense. This follows for instance from Exercise 6.5.31†.

7.4 Units in Complex Cubic Fields and Kobayashi's Theorem

Exercise 7.4.1. Why does looking at the $(2^k)^2$ Pell-type equations $ax^2 - by^2 = k$ for squarefree integral S-units a, b not prove that $u - v = k$ has finitely many integral S-units solutions?

Solution

It doesn't work because there are no reason for it to work, we were simply lucky before. Indeed, the solutions of Proposition 7.2.4 are very messy: they have the form $\alpha^k \beta_i$ for some α and elements $\beta_1, \ldots, \beta_n$. The problem is the additional factor: if we look as the $\sqrt{d}$ part we get something of the form

$$y_n = a \sum_k \binom{n}{2k+1} x^{n-2k-1} y^{2k} d^k + b \sum_k \binom{n}{2k} x^{n-2k} y^{2k} d^k$$

which has too many terms to work with. In particular, we can't even restrict ourselves to the $n = p$ prime case since we do not necessarily jave $y_n \mid y_m$ when $n \mid m$. ■

Exercise 7.4.2*. Prove Theorem 7.4.2 in the case where a/b is a rational cube.

Solution

Write $au^3 = bv^3 = c$ with non-zero $u, v \in \mathbb{Z}$. Then, $ax^3 + by^3 = k$ becomes

$$(xv)^3 + (yu)^3 = ku^3v^3/c$$

so it suffices to consider the case where $a = b = 1$. We have $x + y \mid x^3 + y^3 = k$, say $x + y = d$. It suffices to show that there are finitely many solutions for a fixed d since k has finitely many

divisors. In fact we will prove that there is at most one solution for a fixed d. We have

$$x^2 - xy + y^2 = \frac{k}{x+y} = \frac{k}{d} := d'.$$

Thus, $3xy = (x+y)^2 - (x^2 - xy + y^2) = d^2 - d'$. Hence, x and y are roots of

$$X^2 - \frac{d^2 - d'}{3}X + d$$

by Vieta's formulas which implies that there is at most one (unordered) pair of solutions as wanted. ■

Exercise 7.4.3*. Prove that the only roots of unity of $\mathbb{Q}(\sqrt[3]{d}, j)$ are ± 1, $\pm j$ and $\pm j^2$.

Solution

Note that

$$\mathbb{Q}\left(\exp\left(\frac{2i\pi}{n}\right), \exp\left(\frac{2i\pi}{m}\right)\right) = \mathbb{Q}\left(\exp\left(\frac{2i\pi}{\operatorname{lcm}(m,n)}\right)\right)$$

since the RHS clearly contains the LHS, and $\exp\left(\frac{2i\pi}{\operatorname{lcm}(m,n)}\right) = \exp\left(\frac{2i\pi}{n}\right)^a \exp\left(\frac{2i\pi}{m}\right)^b$ where $am + bn = \gcd(m,n)$ by Bézout. Thus, if n is the greatest order of a root of unity ω contained in $K = \mathbb{Q}(\sqrt[3]{d}, j)$, then $6 \mid n$ since $-j$ has order 6.

By Chapter 3, ω has degree $\varphi(n)$, and since K has degree 6 we get $\varphi(n) \mid 6$. This implies $n \in \{6, 12, 18\}$. $n = 6$ is what we want, so we need to show that the other two cases are impossible. For this, note that $\varphi(12) = \varphi(18) = 6$, so if it were the case then we would have $K = \mathbb{Q}(\omega)$.

To finish, we shall imitate the solution of Problem 6.3.1 to show that this is impossible, i.e. that the Galois group of K is not abelian. Note that the embeddings of K are

$$\sigma_{(a,b)} : \begin{cases} \sqrt[3]{d} \mapsto j^a \sqrt[3]{d} \\ j \mapsto j^b \end{cases}$$

for $a \in \mathbb{Z}/3\mathbb{Z}$ and $b \in (\mathbb{Z}/3\mathbb{Z})^\times$. Moreover, by Exercise 6.3.6*, we have

$$\sigma_{(0,-1)} \circ \sigma_{(1,1)} = \sigma_{(-1,-1)}$$

and

$$\sigma_{(1,1)} \circ \sigma_{(0,-1)} = \sigma_{(1,-1)}$$

so $\sigma_{(0,-1)}$ and $\sigma_{(1,1)}$ do not commute which means that Galois group of K is not abelian as wanted. ■

Exercise 7.4.4*. Prove that $\theta/\sigma(\theta) \in \{\pm j, \pm j^2\}$ is also impossible.

Solution

- $\theta/\sigma(\theta) = \pm j$ yields

$$x + y\sqrt[3]{d} + z\sqrt[3]{d^2} = \pm j(x + yj\sqrt[3]{d} + zj^2\sqrt[3]{d^2})$$

which means $x = 0$ since there's no j term on the left and $y = 0$ since there's no j^2 term

on the left. Thus $\theta = z\sqrt[3]{d^2}$ which is impossible since the norm of $z\sqrt[3]{d^2}$ is z^3d^2 which can't be 1.

- $\theta/\sigma(\theta) = \pm j^2$ yields

$$x + y\sqrt[3]{d} + z\sqrt[3]{d^2} = \pm j^2(x + yj\sqrt[3]{d} + zj^2\sqrt[3]{d^2})$$

which means $x = 0$ since there's no j^2 term on the left and $z = 0$ since there's no j term on the left. Thus $\theta = y\sqrt[3]{d}$ which is impossible since the norm of $y\sqrt[3]{d}$ is y^3d which can't be 1.

■

7.5 Exercises

Diophantine Equations

Exercise 7.5.1† (ISL 1990)**.** Find all positive rational integers n such that $\frac{1^2+\ldots+n^2}{n}$ is a perfect square.

Solution

Note that

$$\frac{1^2 + \ldots + n^2}{n} = \frac{(n+1)(2n+1)}{6}.$$

Thus, this is equal to k^2 is and only if

$$2n^2 + 3n + 1 = (n+1)(2n+1) = 6k^2,$$

i.e.

$$(4n+3)^2 - 48k^2 = 1.$$

Thus, we want to solve the Pell equation $x^2 - 48y^2 = 1$ with $x \equiv 3 \pmod 4$. The solutions are given by $x = \frac{(7+\sqrt{48})^n + (7-\sqrt{48}^n)}{2}$ and it is easy to see that this is congruent to 3 modulo 4 when n is odd. Indeed, modulo 4 it is congruent to

$$\frac{(7^n + n7^{n-1}\sqrt{48}) + (7^n - n7^{n-1}\sqrt{48})}{2} = 7^n \equiv (-1)^n.$$

■

Exercise 7.5.2† (BMO 1 2006)**.** Let n be a rational integer. Prove that, if $2 + 2\sqrt{1 + 12n^2}$ is a rational integer, then it is a perfect square.

Solution

The solutions to the equation $x^2 - 3y^2 = 1$ are given by $x_m = \frac{\alpha^m + \beta^m}{2}$, $y_m = \frac{\alpha^m - \beta^m}{2(\alpha - \beta)}$, where α and β are the conjugate fundamental units $2 \pm \sqrt{3}$). Since $y_1 = 1$ and $y_2 = 4$, y_m is even iff n is. Thus, by assumption, since $\sqrt{1 + 3(2n)^2}$ is an integer, we have $2n = y_{2m}$ and $\sqrt{1 + 12n^2} = x_{2m}$ for some m, i.e.

$$2 + \sqrt{1 + 12n^2} = 2 + 2 \cdot \frac{\alpha^{2m} + \beta^{2m}}{2} = 2\alpha^m\beta^m + \alpha^{2m} + \beta^{2m} = (\alpha^m + \beta^m)^2 = (2x_m)^2.$$

■

Exercise 7.5.4† (RMM 2011)**.** Let $\Omega(\cdot)$ denote the number of prime factors counted with multiplicity of a rational integer, and define $\lambda(\cdot) = (-1)^{\Omega(\cdot)}$. Prove that there are infinitely many rational integers n such that $\lambda(n) = \lambda(n+1) = 1$ and infinitely many rational integers n such that $\lambda(n) = \lambda(n+1) = -1$.

Solution

For the first part, let (x, y) be a solution to the Pell equation $x^2 - 6y^2 = 1$. Then, $n = 6y^2$ has an even number of prime factors and so does $n + 1 = x^2$.

For the second part, let (x, y) be a solution to the Pell-type equation $3x^2 - 2y^2 = 1$. Then, $n = 3y^2$ has an odd number of prime factors, and so does $n+1 = 2x^2$. Note that this equation has infinitely many solutions. Indeed, the Pell equation $z^2 - 2y^2 = 1$ has the solutions $z = \frac{(3+2\sqrt{2})^n + (2-2\sqrt{2})^n}{2}$, and this is divisible by 3 iff n is odd. ■

Exercise 7.5.5†**.** Let k be a rational integer. Prove that there are infinitely positive integers n such that $n^2 + k \mid n!$.

Solution

By Proposition 7.2.3, the equation $x^2 - dy^2 = -k$ has infinitely many solutions if it has at least one and d isn't a perfect square. Thus, pick an r such that $r^2 + k = d$ is not a perfect square (this is true for sufficiently large m since gaps between consecutive perfect squares are increasing) and consider any solution n to the equation $n^2 - dm^2 = -k$, which has infinitely many solutions since $(n, m) = (r, 1)$ is one. Finally, note that

$$n^2 + k = dy^2 = y \cdot dy \mid (dy^2 - k)! = n!$$

for sufficiently large y. ■

Pell-Type Equations

Exercise 7.5.11†**.** Let d be a rational integer. Solve the equation $x^2 - dy^2 = 1$ over $\mathbb{Q}$.

Solution

We will solve this geometrically! The idea is that we (almost) get a correspondence between the rational points of our conic (the curve $x^2 + dy^2 = 1$), and the rational points of the horizontal line $y = 0$. Indeed, if we have a rational point p on the conic, we get a rational point on the horizontal line by intersecting it with the line going through p and $(1, 0)$. Conversely, if we have a rational point q on the horizontal line and intersect the conic with the line going through q and $(1, 0)$, we get a rational point on the conic.

Let's make this more explicit. Let $(0, t)$ be a rational point on the horizontal line. Then, the line joining $(0, t)$ with $(1, 0)$ is $y = t(1 - x)$. When we intersect this with the conic, we get

$$x^2 + dt^2(1 - x)^2 = 1 \iff x + 1 + dt^2(1 - x) = 0 \iff x = \frac{dt^2 + 1}{dt^2 - 1}.$$

From this, we get $y = \frac{2t}{dt^2-1}$. Thus, the solutions are

$$\left[\left(\frac{dt^2+1}{dt^2-1}, \frac{2t}{dt^2-1}\right) \;\middle|\; t \in \mathbb{Q}\right] \cup \{(1,0)\}.$$

■

Exercise 7.5.13†. Prove that the equation $x^2 - 34y^2 = -1$ has no non-trivial solution in $\mathbb{Z}$ despite -1 being a square modulo 34.

Solution

The fundamental unit of $\mathbb{Q}(\sqrt{-34})$ is $35 + 6\sqrt{34}$ which has norm 1. ■

Fundamental Units

Exercise 7.5.15†. Let $d \equiv 1 \pmod 4$ be a squarefree integer, and suppose $\eta = \frac{a+b\sqrt{d}}{2} \notin \mathbb{Z}[\sqrt{d}]$ is the fundamental unit of $\mathbb{Q}(\sqrt{d})$. Prove that $\eta^n \in \mathbb{Z}[\sqrt{d}]$ if and only if $3 \mid n$.

Solution

Let's look at $\mathbb{Z}[\eta] = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ modulo 2: there are four elements since $\frac{a+b\eta}{2} \in \mathbb{Z}[\eta]$ iff $\frac{a}{2}, \frac{b}{2} \in \mathbb{Z}$. Out of these four, three are invertible modulo 2 and the last isn't (it's 0): $1 \cdot 1 \equiv 1$, $\eta \cdot \overline{\eta} \equiv 1$, and $\eta + 1 \equiv \overline{\eta}$ which is invertible by the previous equality. Indeed, by assumption $\eta - \overline{\eta} \equiv \eta + \overline{\eta} \equiv 1 \pmod 2$.

In other words, 2 is prime in $\mathbb{Z}[\eta]$, since an element is either invertible modulo 2 or divisible by 2 (note that this relies on the assumption that $\eta \notin \mathbb{Z}[\sqrt{d}]$, in general, for $d \equiv 1 \pmod 4$, 2 is prime iff $d \equiv 5 \pmod 8$). Thus, by Fermat's little theorem in $\mathbb{Z}[\eta]/2\mathbb{Z}[\eta]$ (this is a finite field with 4 elements, see Theorem 4.2.1), the order of η modulo 2 divides 3. Since $\eta \not\equiv 1$, its order must be exactly 3. Finally, we have

$$\eta^n \in \mathbb{Z}[\sqrt{d}] \iff \frac{\eta^n - \eta^{-n}}{2} \in \mathbb{Z} \iff 2 \mid \eta^{2n} - 1 \iff 3 \mid 2n \iff 3 \mid n$$

as wanted. ■

Exercise 7.5.16†. Let $d \neq 1$ be a squarefree rational integer, and suppose that $2^{2n} + 1 = dm^2$ for some integers $n, m \geq 0$. Show that $2^n + m\sqrt{d}$ is the fundamental unit of $\mathbb{Q}(\sqrt{d})$, provided that $d \neq 5$.

Solution

Clearly, m is odd. Suppose for the sake of a contradiction that $2^n + m\sqrt{d}$ is not the fundamental unit of $\mathbb{Q}(\sqrt{d})$. Then, $2^n + m\sqrt{d}$ is the mth power of an element $\eta \in \mathbb{Q}(\sqrt{d})$ for some m. Without loss of generality, we may assume that $m = p$ is prime (by replacing η by $\alpha^{m/p}$). First, suppose that p is odd. Suppose also that $\eta = u + v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, where u and v are positive. Then,

$$2^n + m\sqrt{d} = (u + v\sqrt{d})^p$$

gives us

$$2^n = \sum_k \binom{p}{2k} u^{p-2k} v^{2k} d^k = u \sum_k \binom{p}{2k} u^{p-2k-1} v^{2k} d^k.$$

Thus, $u \mid 2^n$. Notice that the second factor is congruent to $pv^{p-1}d^{\frac{p-1}{2}}$ modulo u and that this is coprime with u as p and d are odd and u, v are coprime since 2^n and m are. Thus, either $u = 1$ or $u = 2^n$. The former is impossible since the unit is non-trivial, and the latter as well since the second factor is at least $pv^{p-1}d^{\frac{p-1}{2}} > 1$.

Now, suppose that $\eta = \frac{u+v\sqrt{d}}{2}$ for some odd u, v. Then, we get exactly the same equation as before, but with n replaced by $n + p$:

$$2^{n+p} = \sum_k \binom{p}{2k} u^{p-2k} v^{2k} d^k = u \sum_k \binom{p}{2k} u^{p-2k-1} v^{2k} d^k.$$

(We distinguished the two cases because we want u and v to be coprime for the two factors to be as well.) As before, $u = 1$ or $u = 2^{n+p}$: the latter is still impossible as the second factor is at least $pv^{p-1}d^{\frac{p-1}{2}} > 1$, but now the former could be possible since the unit is non-trivial (the rational part is now $\frac{1}{2}$ and not 1). However, it gives $dv^2 \in \{5, -3\}$: the first case is ruled out by the hypothesis and the latter is impossible.

It only remains to settle the case $p = 2$ now. In that case, suppose first that $\eta = u+v\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Then, we get

$$2^n + m\sqrt{d} = (u + v\sqrt{d})^2 = (u^2 + dv^2) + 2uv\sqrt{d}$$

and this is impossible since m is odd. Finally, if $\eta = \frac{u+v\sqrt{d}}{2}$ for some odd u, v, we get

$$2^{n+2} + 4m\sqrt{d} = (u + v\sqrt{d})^2 = (u^2 + dv^2) + 2uv\sqrt{d}$$

which is impossible since $2uv$ is not divisible by 4. ■

Remark 7.5.1

We could have also used Carmichael's theorem from Exercise 4.6.33†: we have

$$2^n = \frac{\alpha^m + \beta^m}{2},$$

with m odd (since $2^n + y\sqrt{d}$ is not a square), where α and β are the conjugate fundamental units of $\mathbb{Z}[\sqrt{d}]$. Since m is odd, we do not have to consider any exceptions, and we get that $\alpha^m - (-\beta)^m$ has a primitive prime factor p which does not divide $\alpha + \beta$. Since $\alpha + \beta$ is even (it's twice the rational part of α), this implies that p is odd, which is a contradiction since 2^n has no odd prime factor. Thus, $2^n + y\sqrt{d}$ is the fundamental unit of $\mathbb{Z}[\sqrt{d}]$, but it might not be the fundamental unit of $\mathbb{Q}(\sqrt{d})$. The last case we need to consider is when $2^n + y\sqrt{d} = \eta^3$, where η is the fundamental unit of $\mathbb{Q}(\sqrt{d})$, by Exercise 7.5.15†.

Exercise 7.5.17†. Suppose that $d = a^2 \pm 1$ is squarefree, where $a \geq 1$ is some rational integer and let $k \geq 0$ be a rational integer. Suppose that the equation $x^2 - dy^2 = m$ has a solution in $\mathbb{Z}$ for some $|m| < ka$. For sufficiently large d, prove that $|m|$, $d + m$ or $d - m$ is a square.

Solution

Note that, the assumption that $d = a^2 \pm 1$ gives us that $\theta = a + \sqrt{d}$ is the fundamental unit of $\mathbb{Q}(\sqrt{d})$. Indeed, if $x^2 - dy^2 = \pm 1$ for some $y \neq 0$, then $x \geq \sqrt{d-1}$ so $x \geq a$.

Suppose (x, y) is a positive solution to $x^2 - dy^2 = m$. By dividing $x + y\sqrt{d}$ by a suitable power

of θ (this may change the sign of m but doesn't change its absolute value), we may assume that $1 \leq x + y\sqrt{d} < \theta$. Then,

$$|2y\sqrt{d}| \leq |x + y\sqrt{d}| + |x - y\sqrt{d}| < \theta + \frac{|m|}{\theta} < 2a + k + o(1).$$

Thus, $|y| < 1 + o(1)$. For sufficiently large a, our inequality forces $|y| = 1$ or $y = 0$. If $|y| = 1$, we get that $m + d$ is a perfect square, and if $y = 0$ we get that m is a perfect square as wanted. ■

Remark 7.5.2

The argument used in Remark 5.5.1 can be slightly modified to show that, for any choice of ± 1, there exist infinitely many squarefree numbers of the form $a^2 \pm 1$.

Exercise 7.5.18†. Solve completely the equation $x^3 + 2y^3 + 4z^3 = 6xyz + 1$ which was seen in Problem 6.2.2.

Solution

Since the norm of $x + y\sqrt[3]{2} + z\sqrt[3]{4}$ is $x^3 + 2y^3 + 4z^3 - 6xyz$ (see Problem 6.2.2), we wish to find units in $K = \mathbb{Q}(\sqrt[3]{2})$. We claim that the fundamental unit of $\mathbb{Q}(\sqrt[3]{2})$ is $\theta = 1 + \sqrt[3]{2} + \sqrt[3]{4}$. Thus, the solutions will be the one considered in Problem 6.2.2, i.e. $x + y\sqrt[3]{2} + z\sqrt[3]{4} = (1 + \sqrt[3]{2} + \sqrt[3]{4})^n$ for some n (the only roots of unity of $\mathbb{Q}(\sqrt[3]{2})$ are ± 1 and -1 has norm -1 so does not work).

We need to show that this unit has minimal absolute value (among the ones greater than 1). Suppose that there is a unit greater than 1 $a + b\sqrt[3]{2} + c\sqrt[3]{4} := \varepsilon < \theta < 4$. Let σ be a complex embedding of K. Then, $|\sigma(\varepsilon)|^2 = \frac{1}{\varepsilon} \in \left[\frac{1}{2}, 1\right]$. Hence, the minimal polynomial $X^3 + uX^2 + vX \pm 1$ of ε satisfies

$$0 < -u = \varepsilon + \sigma(\varepsilon) + \overline{\sigma}(\varepsilon) < \varepsilon + \frac{2}{\sqrt{\varepsilon}} < 5$$

and

$$|v| = \left|\varepsilon(\sigma(\varepsilon) + \overline{\sigma}(\varepsilon)) + |\sigma(\varepsilon)|^2\right| \leq 2\sqrt{\varepsilon} + \frac{1}{\varepsilon} < 5.$$

Thus, $u \in [-4, -1]$ and $v \in [-4, 4]$. However, we also have $u = -3a$ and $v = 3(a^2 - 2bc)$. Thus, $u = -3$ and $v = \pm 3$, which yield $a = 1$, and $b = c = 1$ or $b = 0$ or $c = 0$. If $b = 0$, then $a^3 + 2b^3 + 4c^3 - 6abc = 1 + 4c^3$ so c must also be 0, and if $c = 0$ then $a^3 + 2b^3 - 6abc = 1 + 2b^3$ so $b = 0$ or $b = -1$.

Thus, we conclude that $\varepsilon = 1 + \sqrt[3]{2} + \sqrt[3]{4}$ as wanted, or $\varepsilon = 1 - \sqrt[3]{2}$. However, $1 - \sqrt[3]{2} < 1$ so we must be in the first case, as asserted. (In fact, it turns out that $1 - \sqrt[3]{2} = -\frac{1}{1 + \sqrt[3]{2} + \sqrt[3]{4}}$, which is perhaps a neater choice of fundamental unit.) ■

Exercise 7.5.19† (Weak Dirichlet's Unit Theorem)**.** Let K be a number field with r real embeddings and s pairs of complex embeddings. Prove that there exist units $\varepsilon_1, \ldots, \varepsilon_k$ with $k \leq r + s - 1$ such that any unit of K can be written uniquely in the form

$$\zeta \varepsilon_1^{n_1} \cdot \ldots \cdot \varepsilon_k^{n_k}$$

for some integers n_i and a root of unity ζ.

Solution

Let $\sigma_1, \dots, \sigma_r$ be the real embeddings of K, and $\sigma_{r+1}, \overline{\sigma}_{r+1}, \dots, \sigma_{r+s}, \overline{\sigma}_{r+s}$ its pairs of complex embeddings and let U be the group of units of K. We look at the logarithms of the embeddings of units:

$$L = \{(\log|\sigma_1(\varepsilon)|, \dots, \log|\sigma_{r+s-1}(\varepsilon)|) \mid \varepsilon \in U\} \subseteq \mathbb{R}^{r+s-1}.$$

We claim that this set is a discrete additive subgroup of $\mathbb{R}^{r+s-1}$, meaning that it's closed under addition and subtraction, and, for any $x \in \mathbb{R}^{r+s-1}$, there is no sequence of distinct elements of L tending to x. To show this, we will prove that, for any $A, B > 0$, there are finitely many units such that $A < |\sigma_i(\varepsilon)| < B$ for $i = 1, \dots, r+s-1$. Notice that such a number also satisfies

$$\frac{1}{B^{r+s-1}} < |\sigma_{r+s-1}| < \frac{1}{A^{r+s-1}}$$

since it is a unit (so the product of $|\sigma_i(\varepsilon)|$ is 1). Thus, all the conjugates of ε have bounded absolute value, which implies that its minimal polynomial has bounded coefficients. This shows that there are a finite number of such ε.

Next, we show that any discrete additive subgroup Γ of $\mathbb{R}^m$ is a *lattice*, i.e. admits a linearly independent basis as a $\mathbb{Z}$-module, or in other words, there are $\alpha_1, \dots, \alpha_k$ such that any element of Γ can be written in a unique way as $\sum_{i=1}^k n_i\alpha_i$ with $n_i \in \mathbb{Z}$. Since $\mathbb{R}^m$ has dimension m as a $\mathbb{R}$-vector space, this implies that $k \leq m$ by Proposition C.1.2. To show this, pick any maximal set of linearly independent elements $\beta_1, \dots, \beta_k \in \Gamma$ and let $\Gamma' = \beta_1\mathbb{Z} + \dots + \beta_k\mathbb{Z}$. We will prove that there are a finite numbers of elements in Γ modulo Γ', i.e. that Γ/Γ' is finite, say has N elements. Then, Lagrange's theorem 2.5.1 implies that $N\alpha \in \Gamma'$ for any $\alpha \in \Gamma$, i.e.

$$\Gamma \subseteq \frac{1}{N}\Gamma' = \frac{\beta_1}{N}\mathbb{Z} + \dots + \frac{\beta_k}{N}\mathbb{Z}.$$

We can then conclude with Exercise 6.5.31† (so many intermediate results!) that Γ also has a $\mathbb{Z}$-basis. Thus, it remains to prove that Γ/Γ' is finite. For this, note that it suffices to prove that $\beta_1[0,1] + \dots + \beta_k[0,1]$ contains finitely many elements of Γ, as this is a system of representatives of $\mathbb{R}^m/\Gamma'$. If there were infinitely many elements of Γ there, Γ would have a convergent subsequence by the Bolzano-Weierstrass theorem from 8.7.10†, contradicting its discreteness (we do not actually need BW since we actually directly showed that there were a finite number of elements of L in any interval).

Finally, the previous discussion implies that L has a basis corresponding to the image of $\varepsilon_1, \dots, \varepsilon_k$ under the logarithmic embedding, for some $k \leq r+s-1$. Thus, by raising everything to the exponential, we get that, for every unit ε, there are unique integers $n_1, \dots, n_k$ such that the number

$$\frac{\varepsilon}{\varepsilon_1^{n_1} \cdot \dots \cdot \varepsilon_k^{n_k}}$$

has all its conjugates on the unit circle. By Exercise 1.5.27†, this implies that it is a (unique) root of unity ζ as wanted. ■

Remark 7.5.3

There is nothing particularly deep about the logarithm in this proof, apart from the fact that it transforms multiplication into addition and that we feel more comfortable working with addition. We could of course transform our additive proof into a multiplicative one by removing the logarithms and turning addition into multiplication.

Exercise 7.5.20† (Gabriel Dospinescu)**.** Find all monic polynomials $f \in \mathbb{Q}[X]$ such that $f(X^n)$ is reducible in $\mathbb{Q}[X]$ for all $n \geq 2$ but f is irreducible.

Solution

Let α be a root of f and let K be the splitting field of f, i.e. $\mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ where α_i are the roots of f (the conjugates of α). Note that the statement is equivalent to $f(X^p)$ being reducible for any prime p. In fact we only need this assumption for infinitely many primes. By Lemma 6.1.1, $f(X^p)$ is reducible over $\mathbb{Q}$ if and only if $X^p - \alpha$ is reducible over $\mathbb{Q}(\alpha)$, and by Exercise 6.5.9†, this is equivalent to α being a pth power in $\mathbb{Q}(\alpha)$, and thus in K too.

By looking at the norm of α in K, we see that α must have norm 1 or 0 since its norm is a pth power in $\mathbb{Q}$ for infinitely many p. If $\alpha = 0$, then $f = X$ since it is irreducible, which works. Otherwise, α must be a unit. By Exercise 7.5.19†, there are multiplicatively independent units $\varepsilon_1, \ldots, \varepsilon_k \in K$ and integers $n_1, \ldots, n_k$ as well as root of unity ζ such that

$$\alpha = \zeta \varepsilon_1^{n_1} \cdot \ldots \cdot \varepsilon_k^{n_k}.$$

Since $\varepsilon_1, \ldots, \varepsilon_k$ are multiplicatively independent, the fact that α is a pth power means that $p \mid n_i$ for every i. For sufficiently large p, we find $n_1 = \ldots = n_k = 0$. Thus, α is a root of unity. However, since a primitive mth root of unity has degree $\varphi(m)$ over $\mathbb{Q}$, K contains finitely many roots of unity ($\varphi(m)$ is greater than $[K : \mathbb{Q}]$ for sufficiently large m), which implies $\zeta = 1$ since it's a pth power for infinitely many primes p. Thus, we conclude that $\alpha = 1$. The two solutions are hence $f = X$ and $f = X - 1$, which indeed work. ■

Miscellaneous

Exercise 7.5.21† (Liouville's Theorem)**.** Let α be an algebraic number of degree n. Prove that there exists a constant $C > 0$ such that

$$\left| \alpha - \frac{p}{q} \right| > \frac{C}{q^n}$$

for any $p, q \in \mathbb{Z}$ (with $q > 0$).

Solution

Let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α. We have

$$q^n \left| \prod_{i=1}^{n} \frac{p}{q} - \alpha_i \right| = \left| \prod_{i=1}^{n} p - q\alpha_i \right| \geq 1$$

since it's a non-zero integer. If $\left| \frac{p}{q} - \alpha \right| < 1$, then $\left| \frac{p}{q} - \alpha' \right| < 1 + |\alpha - \alpha'|$ for any conjugate $\alpha' \neq \alpha$. Thus, in this case we have

$$|p - q\alpha| \prod_{i=1}^{n} 1 + |\alpha - \alpha_i| \geq \frac{1}{q^n}$$

as wanted ($C = \frac{1}{\prod_{i=1}^{n} 1+|\alpha-\alpha_i|}$). Otherwise, we have $\left| \frac{p}{q} - \alpha \right| \geq 1 > \frac{C}{q^n}$ too. ■

Exercise 7.5.22†. Prove that $5n^2 \pm 4$ is a perfect square for some choice of $\pm$ if and only if n is a Fibonacci number.

Solution

Simply note that $\frac{1+\sqrt{5}}{2}$ is the fundamental unit of $\mathbb{Q}(\sqrt{5})$, and that the solutions to the equation $x^2 - 5y^2 = \pm 1$ for $x \equiv y \pmod 1$ half-integers, i.e. the rational integers solutions to the equation

$(2x)^2 - 5(2y)^2 = \pm 4$ are thus

$$2y = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}} = F_n.$$

■

Exercise 7.5.23† (ELMO 2020)**.** Suppose n is a Fibonacci number modulo every rational prime. Must it follow that n is a Fibonacci number?

Solution

By Exercise 7.5.22†, the statement means that, for every p, $5n^2 + 4$ or $5n^2 - 4$ is a quadratic residue (or zero). This implies that $5n^2 + 4$ or $5n^2 - 4$ is a perfect square by an argument similar to Exercise 4.6.20†, i.e. n is a Fibonacci number too. Indeed, if, modulo sufficiently large primes, one of a and b is a quadratic residue, then one of them must be a square (this is not true anymore with 3 numbers, see Exercise 4.6.22†). By Exercise 4.6.20†, we may assume that $a \neq b$.

Suppose without loss of generality that a and b are squarefree. Write $a = \varepsilon 2^r p_1 \cdot \ldots \cdot p_k$ and $b = \eta 2^s q_1 \cdot \ldots \cdot q_m$ with $\varepsilon, \eta \in \{-1, 1\}$, $r, s \in \{0, 1\}$, and $p_1, \ldots, p_k, q_1, \ldots, q_m$ odd primes. Let t be a quadratic non-residue modulo p_1 (if $k \geq 1$). If a and b are both divisible by an odd prime, say $p_1 = q_1$, then pick a large prime

$$p \equiv 1 \pmod{8p_2 \cdot \ldots \cdot p_k q_2 \cdot \ldots \cdot q_m}$$

and $p \equiv t \pmod{p_1}$. Then, quadratic reciprocity gives us $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$ which is a contradiction.

Suppose for the sake of a contradiction that $k, m \geq 1$. Then, pick a large prime

$$p \equiv 1 \pmod{8p_2 \cdot \ldots \cdot p_k q_2 \cdot \ldots \cdot q_m},$$

$p \equiv t \pmod{p_1}$ and $p \equiv t' \pmod{q_1}$ where t' is a quadratic non-residue modulo q_1 to get $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$. Thus, suppose without loss of generality that $m = 0$. If $k \geq 1$, pick a large prime $p \equiv 8 \pmod{p_1 \cdot \ldots \cdot p_k}$ and $p \equiv t \pmod{p_1}$ to get $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$ again.

Finally, we have $k = m = 0$ so $\{a, b\} \in \{1, -1, 2, -2\}$. It remains to show that $\{a, b\} = \{2, -2\}$, $\{a, b\} = \{-1, -2\}$ and $\{a, b\} = \{-1, 2\}$ are all impossible. For the first, note that they are both quadratic non-residues modulo $p \equiv 5 \pmod 8$, for the second, note that they are both quadratic non-residues modulo $p \equiv -1 \pmod 8$, and for the last note that they are both quadratic non-residues modulo $p \equiv 3 \pmod 8$.

As a final remark, as in Exercise 4.6.20†, we may avoid Dirichlet's theorem on primes in arithmetic progressions with Jacobi's quadratic reciprocity law (by picking any rational integer $p \equiv u \pmod v$ with sufficiently large prime factors instead of a prime). ■

Exercise 7.5.24† (Nagell, Ko-Chao, Chein)**.** Let p be an odd rational prime. Suppose that $x, y \in \mathbb{Z}$ are rational integers such that $x^2 - y^p = 1$. Prove that $2 \mid y$ and $p \mid x$. Deduce that this equation has no solution for $p \geq 5$. (The case $p = 3$ is Exercise 8.7.19†.)

Solution

If y is odd, then the two factors of $y^p = (x-1)(x+1)$ are coprime so $x-1$ and $x+1$ are pth powers. This is impossible, as there are no pth power distant by 2: $(m+1)^p - m^p \geq p+1$. Now, suppose for the sake of a contradiction that $p \nmid x$. Then, the two factors of $x^2 = (y+1) \cdot \frac{y^p+1}{y+1}$ are coprime. Indeed, this is a product of cyclotomic polynomials, but it can also be seen more elementarily: $\frac{y^p+1}{y+1} \equiv p \pmod{y+1}$. This implies that $y+1 = a^2$ and $y^p+1 = b^2$. Now consider the Pell equation $u^2 - yv^2 = 1$. We have two solutions: $(u,v) = (a,1)$ and $(u,v) = (b, y^{\frac{p-1}{2}})$. Notice that, for both of them, v is a y-unit. By Størmer's theorem, this implies that they are both the fundamental solution, which is impossible.

Thus, $p \mid x$ and $2 \mid y$. Without loss of generality, suppose that $x+1 = 2^{p-1}a^p$ and $x-1 = 2b^p$ (by replacing x by $-x$ if necessary). Since $|x| > 1$, a and b have the same sign, and $|a| < |b|$. The key (magical?) point is that

$$b^{2p} + (2a)^p = \left(\frac{x-1}{2}\right)^2 + 2(x+1) = \left(\frac{x-3}{2}\right)^2.$$

For $p \neq 3$, this is not divisible by p since $p \mid x$, so $b^2 + 2a$ and $\frac{b^{2p}+(2a)^p}{b^2+2a}$ are perfect square. However,

$$b^2 < b^2 + 2a < (b+1)^2$$

if a and b are positive, and

$$(b-1)^2 < b^2 + 2a < b^2$$

if a and b are negative. In all cases, we have reached a contradiction. ■

Exercise 7.5.25†. Prove that there are at most $3^{|S|}$ pairs of S-units distant by 2.

Solution

If $u - v = 2$, then $(v+1)^2 - uv = 1$. We let $\mathrm{rad}(uv) \mid d$ be minimal such that uv/d is a square. There are $3^{|S|}$ possible d. As before, any $u - v = 2$ give rise to a solution to the Pell equation $x^2 - dy^2 = 1$ for some d-unit number y, which must thus be the minimal unit by Proposition 7.3.1. Thus, there are also at most $3^{|S|}$ pairs of S-units distant by 2. ■

Exercise 7.5.26†. Assuming the finiteness of rational solutions to the S-unit equation $u + v = 1$ for any finite S, determine all functions $f : \mathbb{Z} \to \mathbb{Z}$ such that $m - n \mid f(m) - f(n)$ for any m, n and f is a bijection modulo sufficiently large primes.

Solution

Let S be the set of primes p for which f is not a bijection modulo p or $p = 2$. By assumption, $f(n+1) - f(n)$, $f(n+2) - f(n+1)$, and $f(n+2) - f(n)$ are all S-units. Thus, we have a solution

$$(f(n+2) - f(n+1)) + (f(n+1) - f(n)) = f(n+2) - f(n)$$

to the S-unit equation. There are a finite number of solutions to this equation (up to scaling), so we get that $\frac{f(n+2)-f(n+1)}{f(n+1)-f(n)}$ is in a finite set U. Now, pick a large prime $p \notin S$ such that $|U \pmod p| = |U|$ and let $a \in \mathbb{Z}$. Since $\frac{f(n+2)-f(n+1)}{f(n+1)-f(n)}$ and $\frac{f(n+ap+2)-f(n+ap+1)}{f(n+1+ap)-f(n+ap)}$ are congruent modulo p and in U, they must be equal. By picking another sufficiently large prime $q \neq p$ and

$b \in \mathbb{Z}$ such that $ap + bq = 1$, we get

$$\frac{f(n+2) - f(n+!)}{f(n+1) - f(n)} = \frac{f(n+ap+bq+2) - f(n+ap+bq+1)}{f(n+1+ap+bq) - f(n+ap+bq)} = \frac{f(n+3) - f(n+2)}{f(n+2) - f(n+1)}$$

which means that the quotient $\frac{f(n+2)-f(n+1)}{f(n+1)-f(n)}$ is in fact constant, say equal to r. Then, f satisfies the following linear recurrence: $f(n+2) = f(n+1) + r(f(n+1) - f(n)) = sf(n+1) - f(n)$ which, unless $s = 2$ which implies that the characteristic polynomial has a double root, reduces to $f(n) = u\alpha^n + v\beta^n$ for some conjugate quadratic integers α, β. But then, if $p \neq 2$ is such that the characteristic polynomial $X^2 - sX + 1$ splits modulo p, we get

$$f(n) \equiv u_p \alpha_p^n + v_p \beta_p^n \pmod{p}$$

for some $u_p, v_p, \alpha_p, \beta_p \in \mathbb{F}_p$, so that $f(p-1) = u_p + v_p = f(1)$. This is a contradiction. Thus, $s = 2$, which gives $f(n) = un + v$ for some $u, v \in \mathbb{Z}$. Conversely, it is clear that arithmetic progressions work. ■

Remark 7.5.4

If f is taken to be $|g|_p$ for some g, which is usually how the theorem is used in p-adica analysis, there is in fact a simpler argument. Since the distance of $\mathbb{Q}_p$ is almost *discrete*, i.e. the values that it reaches $0, \ldots, 1/p^2, 1/p, 1, p, p^2, \ldots$ are all isolated except 0, we get the stronger conclusion that f has a maximum if and only if it is bounded above, and it has a minimum if $0 \in \operatorname{im} f$ or if it is bounded below by a positive number.

Chapter 8

p-adic Analysis

8.1 p-adic Integers and Numbers

Exercise 8.1.1*. Check that $\mathbb{Z}_p$ is an integral domain. What is its characteristic?

Solution

$ab = 0$ means $a_i b_i = 0$ for all i, where $a = (a_1, a_2, a_3, \ldots)$ and $b = (b_1, b_2, b_3, \ldots)$. Suppose that a is non-zero, and let k be such that $a_k \neq 0$. Then, $v_p(a_i) = v_p(a_k)$ for $i \geq k$ since $a_i \equiv a_k \pmod{p^k}$. Thus, for $i \geq k$, we have $v_p(b_i) \geq i - v_p(k)$. Hence, the coordinates of b have arbitrarily large p-adic valuation which means that they are all zero by compatibility: if $v_p(b_i) \geq N$ and $i \geq N$, then $b_N \equiv b_i \equiv 0 \pmod{p^N}$.

$\mathbb{Z}_p$ has characteristic zero since $(n, n, n, \ldots)$ is zero only when $n = 0$, otherwise n has a non-zero v_p and it thus a non-zero coordinate too. ■

Exercise 8.1.2*. Check that $a \mapsto (a \pmod{p}, a \pmod{p^2}, a \pmod{p^3}, \ldots)$ is indeed an embedding of $\mathbb{Z}_{(p)}$ into $\mathbb{Z}_p$, i.e. that it's injective.

Solution

It is clearly additive and multiplicative, and it is injective since the kernel is trivial: if a is non-zero then it has a non-zero v_p so a non-zero component under this embedding too. ■

Exercise 8.2.1*. Convince yourself of this proof.

Solution

Another way to write this proof is to define b_k as

$$\sum_{i=0}^{\infty} a_i \pmod{p^k} \equiv \sum_{k=0}^{|a_i| < p^{-k}} a_i.$$

This sequence is Cauchy since $|b_i - b_j| < p^{-\min(i,j)}$ by the strong triangle inequality and clearly converges to $\sum_{i=0}^{\infty} a_i$ by the strong triangle inequality again. ■

8.2 p-adic Absolute Value

Exercise 8.2.2*. Prove that the strong triangle inequality also holds for series: if $a_i \to 0$ then $|\sum_i a_i|_p \leq \max_i |a_i|_p$ with equality if the maximum is achieved only once.

Solution

We have

$$\left|\sum_{i=1}^{n} a_i\right| \leq \max_{1\leq i\leq n} |a_i|_p \leq \max_i |a_i|_p$$

for all n and this yields the wanted inequality by taking the limit as $n \to \infty$. For the equality part, just note when the maximum is achieved only once, we have equality when n is sufficiently large so taking the limit yields the equality again. ■

Exercise 8.2.3*. Prove the product formula.

Solution

This is a consequence of the prime factorisation:

$$\prod_p |x|_p = \prod_p p^{-v_p(x)} = \frac{1}{|x|_\infty}.$$

■

8.3 Binomial Series

Exercise 8.3.1*. Prove that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

Solution

This is a consequence of the density of $\mathbb{Z}$ in $\mathbb{Z}_p$: if α is an element of $\mathbb{Q}_p$ then write $\alpha = p^k a$ with $a \in \mathbb{Z}_p$. There is a sequence of rational integers approaching a, and multiplying this sequence by p^k yields a sequence of rational numbers approaching α. ■

Exercise 8.3.2*. Let $f \in \mathbb{Q}_p[X]$ be a polynomial. Prove that f is continuous on $\mathbb{Q}_p$.

Solution

The proof is the same as in $\mathbb{R}$: if ε is very small then

$$(x+\varepsilon)^n - x^n = \varepsilon \sum_{k=1}^{n} \binom{k}{n} \varepsilon^{k-1} x^{n-k}$$

is also very small by the triangular inequality (it is in fact even neater in $\mathbb{Q}_p$ since we have the strong triangle inequality to bound the second factor). ■

Exercise 8.3.3*. Let $f : \mathbb{Z}_p \to \mathbb{Q}_p$ be a continuous function. If $|f(x)|_p \leq 1$ for any n in a dense subset (in $\mathbb{Z}_p$), prove that $|f(x)|_p \leq 1$ for any $x \in \mathbb{Z}_p$.

Solution

Let $x \in \mathbb{Z}_p$ be a p-adic integer and let $a_1, a_2, \ldots$ be sequence of elements of that dense subset approaching x. By the triangular inequality, we have

$$|f(x)|_p - 1 \leq |f(x)|_p - |f(a_n)|_p \leq |f(x) - f(a_n)|_p \to 0$$

which means that $|f(x)|_p \leq 1$ as wanted. ■

Exercise 8.3.4*. Prove that, if $p > 5$ is a rational prime, $p^2 \mid \sum_{k=1}^{p-1} \frac{1}{k^3}$ and $p \mid \sum_{k=1}^{p-1} \frac{1}{k^4}$.

Solution

Note that

$$\frac{1}{k^3} + \frac{1}{(p-k)^3} = \frac{k^3 + (p-k)^3}{(p(p-k))^3} \equiv -\frac{3k^2 p}{(k(p-k))^3} \pmod{p^2}$$

so we need to prove that $p \mid \sum_{k=1}^{\frac{p-1}{2}} \frac{k^2}{(k(p-k))^3}$. Since p is odd and $\frac{k^2}{(k(p-k))}^3 \equiv \frac{(p-k)^2}{((p-k)k)^3}$, this is equivalent to

$$p \mid \sum_{k=1}^{p-1} \frac{k^2}{(k(p-k))^3}.$$

Since

$$\frac{k^2}{(k(p-k))^3} \equiv \frac{k^2}{(-k^2)^3} \equiv -k^{-4},$$

we need to show that $\sum_{k=1}^{p-1} k^{-4} \equiv 0 \pmod{p}$. Let ω be a primitive root modulo p. Then,

$$\sum_{k=1}^{p-1} k^{-4} \equiv \sum_{k=1}^{p-1} \omega^{-4k} \equiv \frac{\omega^{-4(p-1)} - 1}{\omega^{-4} - 1} \equiv 0$$

since the numerator is zero and the denominator is non-zero as $p > 5$. Note that this is also the second claim. ■

Exercise 8.3.5*. Prove Proposition 8.3.4.

Solution

If we consider only the nth coordinate of these series, then, since $a_{i,j} \to 0$, the series become finite sums (the nth coordinate of $a_{i,j}$ is zero for sufficiently large $i+j$). In particular, both sides are equal. Letting n go to infinity, this shows both that the series converge and that they are equal. ■

Exercise 8.3.6*. Let $n \in \mathbb{N}$ be a positive rational integer and p be a prime number. Prove that

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Solution

There are $\left\lfloor \frac{n}{p} \right\rfloor$ numbers in $[n]$ which are divisible by p, which explains this term in the sum. However, their contribution to the total p-adic valuation might not always be one: some of these numbers are divisible by p^2 too. Hence we add $\left\lfloor \frac{n}{p^2} \right\rfloor$ to account for them too (combining with $\left\lfloor \frac{n}{p} \right\rfloor$ this constitutes a contribution of 2 for the multiples of p^2). Then we take in account the contribution of multiples of p^3 with $\left\lfloor \frac{n}{p^3} \right\rfloor$, then the multiples of p^4, etc. ■

Exercise 8.3.7*. Prove Corollary 8.3.1.

Solution

Since $(1+u)^x = \sum_k \binom{x}{k} u^k$, we need to prove that $u^k/k! \to 0$ for $|u|_p < p^{-1/(p-1)}$ by Proposition 8.3.3. Proposition 8.3.5 gives us $|k!|_p \geq p^{-k/(p-1)}$ so that

$$|u^k/k!|_p = |u|_p^k/|k!|_p \geq \left(\frac{|u|_p}{p^{-1/(p-1)}} \right)^k \to 0.$$

■

8.4 Analytic Functions

Exercise 8.4.1*. Prove that locally analytic functions are continuous.

Solution

Let $\alpha \in \mathbb{Z}_p$ be a p-adic integer. We prove that, if f is analytic at α, it is continuous at α. Write $f(x) = \sum_{i=0}^{\infty} a_i (x-\alpha)^i$ around α. Then,

$$|f(x) - f(\alpha)|_p = \left| \sum_{i=1}^{\infty} a_i (x-\alpha)^i \right|_p \leq \max_{i \geq 1} \left| a_i (x-\alpha)^i \right|_p \leq C |x-\alpha|_p$$

for $|x-\alpha|_p$ sufficiently small and some constant C. Indeed, the series converge when $|x-\alpha|_p \leq \varepsilon$ for some $\varepsilon > 0$ so $a_i \varepsilon^i \to 0$ which implies

$$\max_i \left| a_i (x-\alpha)^i \right|_p = \max_{i \geq 1} \left| a_i \varepsilon^i \left(\frac{x-\alpha}{\varepsilon} \right)^i \right|_p \leq \max_{i \geq 1} \frac{x-\alpha}{\varepsilon} |a_i \varepsilon^i|_p$$

Thus, when $x \to \alpha$ we also have $f(x) \to f(\alpha)$ as wanted. ■

Exercise 8.4.2*. Prove that the sum and product of two locally analytic functions is again a locally analytic function.

Solution

It is clear that the sum of two analytic functions is analytic, thus we need to prove that the product of two analytic functions is also analytic. Let f and g be two analytic at $\alpha \in \mathbb{Z}_p$

functions. Write $f(x) = \sum_{i=1}^{\infty} a_i(x-\alpha)^i$ and $g(x) = \sum_{j=1}^{\infty} b_j(x-\alpha)^j$ for $|x-\alpha|_p \leq \varepsilon$. Then,

$$f(x)g(x) = \sum_{i=1}^{\infty} a_i(x-\alpha)^i \sum_{j=1}^{\infty} b_j(x-\alpha)^j = \sum_{i+j=k} a_i b_j (x-\alpha)^k.$$

We already allowed to do this expansion by Proposition 8.3.4 since

$$|a_i b_j (x-\alpha)^{i+j}|_p \leq \max(|a_i|_p, |b_j|_p)\varepsilon^{i+j} \to 0$$

when $i+j \to \infty$. ■

Exercise 8.4.3*. Prove that polynomials are locally analytic (everywhere).

Solution

This is Proposition 5.3.1. ■

Exercise 8.4.4*. Prove Proposition 8.4.2.

Solution

Since $|\alpha^k x^n a_{k+n}|_{\mathfrak{p}} \leq \max(|\alpha|, |x|)^{k+n}|a_{k+n}|_{\mathfrak{p}} \to 0$ when $x \in \mathbb{Z}_p$, Proposition 8.3.4 gives us

$$\begin{aligned}
f(x) &= \sum_k a_k(\alpha + (x-\alpha))^k \\
&= \sum_k \sum_n a_k \binom{n}{k} \alpha^{k-n}(x-\alpha)^n \\
&= \sum_n \sum_k a_k \binom{n}{k} \alpha^{k-n}(x-\alpha)^n \\
&= \sum_n (z-\alpha)^n \sum_k a_k \binom{n}{k} \alpha^{k-n} \\
&= \sum_n (x-\alpha)^n \sum_k a_{k+n} \binom{n}{k} \alpha^{k-n} \\
&= \sum_n (x-\alpha)^n \frac{f^{(n)}(\alpha)}{n!}
\end{aligned}$$

as wanted. ■

8.5 The Skolem-Mahler-Lech Theorem

Exercise 8.5.1*. Convince yourself of this proof.

Solution

Not much I can say here. ■

Exercise 8.5.2*. Do you think this proof could be formulated without appealing to p-adic analysis?

Solution

As said before, there is no known proof which doesn't use p-adic ideas. However, one could phrase the proof without mentionning p-adic numbers by looking at partial sums of our analytic functions modulo powers of p. See Block **??** for an example. ■

Exercise 8.5.3*. Prove that any number field has a finite number N of roots of unity, and that $\omega^N = 1$ for any root of unity ω of K. (In other words, the roots of unity of K are exactly the Nth roots of unity.)

Solution

Since $\varphi(n) \to \infty$ and a primitive nth root of unity has degree $\varphi(n)$ over $\mathbb{Q}$, contains finitely many roots of unity.

One way to finish from this is to say that the roots of unity of K form a subgroup of the multiplicative group of nth roots of unity for some n. Since this is a cyclic group, any of its subgroup is also cyclic, and in particular the group of roots of unity of K.

Another way to finish from the first observation is to pick a root of unity $\omega \in K$ of maximal order N. Then, if ζ is another root of unity of K, say of order n, $\mathbb{Q}(\omega, \zeta) \subseteq K$ contains a root of unity of order $\operatorname{lcm}(N, n)$ by Problem 6.3.2 which implies that n divides N by maximality of N. ■

8.6 Strassmann's Theorem

Exercise 8.6.1. Prove that $\mathbb{Q}(\sqrt{-7})$ is norm-Euclidean. (This is also Exercise 2.6.4†.)

Solution

Let $\alpha, \beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{-7})} = \mathbb{Z}\left(\frac{1+\sqrt{-7}}{2}\right)$ be quadratic integers with $\beta \neq 0$. Write $\frac{\alpha}{\beta} = x + y\sqrt{-7}$ with $x, y \in \mathbb{Q}$. Pick a half-integer n such that $|y - m| \leq \frac{1}{4}$, and a half integer $m \equiv n \pmod 1$ such that $|x - n| \leq \frac{1}{2}$. Then,

$$|N((x-m) + (y-n)\sqrt{-7})| \leq \left(\frac{1}{2}\right)^2 + 7\left(\frac{1}{4}\right)^2 = \frac{15}{16} < 1.$$

Thus, the remainder $\tau = \beta(((x-m) + (y-n)\sqrt{-7})$ works since it has norm less than $|N(\beta)|$ by the previous computation and $\alpha = \beta(m + n\sqrt{-7}) + \tau$. ■

Exercise 8.6.2. Prove that, if $x^2 + 7 = 2^n$, then $\frac{x \pm \sqrt{-7}}{2} = \left(\frac{1+\sqrt{-7}}{2}\right)^{n-2}$ for some choice of $\pm$.

Solution

By the uniqueness of the prime factorisation in $\mathbb{Q}(\sqrt{-7})$ (Exercise 8.6.1), we have $\frac{x+\sqrt{-7}}{2} = \alpha^k \beta^m$. Since the LHS is not divisible by 2, this means $\min(k, m) = 0$ as otherwise $2 = \alpha\beta$ divides the LHS. ■

Exercise 8.6.3*. Compute the Strassmann bounds for the function $s \mapsto (\alpha-\beta)(u_{s+10r} \pm 1)$, for each $r \in \{0, 1, \ldots, 9\}$. (If you do not want to do it all by hand, you may use a computer. In any case, it is better to do it to have a feel for why it works because it's very cool.)

Solution

Modulo 11, we can see that

$$\alpha^r - \beta^r \pm (\alpha - \beta) \equiv 5^r - 7^r \mp 2 \pmod{11}$$

can be zero only for $r \in \{1, 2, 3, 5\}$, which means that in the other cases the Strassmann bound is 0. Now, let's study the second coefficient:

$$a\alpha^r - b\beta^r \equiv 99 \cdot 5^r - 77 \cdot 7^r.$$

When $r = 1$, this is

$$99 \cdot 16 - 77 \cdot 7 \equiv 77 \pmod{11^2}$$

so the Strassmann bound is 1 since all other coefficients are divisible by 11^2. Similarly, when $r = 2$ this is $33 \not\equiv 0$, and when $r = 5$ this is $55 \not\equiv 0$.

Finally, we need to treat the case $r = 3$. This time, the second coefficient is divisible by 11^2 so we need to consider the third one:

$$\begin{aligned}(\alpha-\beta)(u_{r+10s} \pm 1) &= \alpha^r(1+a)^s - \beta^r(1+b)^s \pm (\alpha-\beta) \\ &= \alpha^r \sum_k \binom{s}{k} a^s - \beta^r \sum_k \binom{s}{k} b^s \pm (\alpha-\beta) \\ &\equiv \alpha^r \left(1 + as + a^2\frac{s(s-1)}{2}\right) - \beta^r \left(1 + bs + b^2\frac{s(s-1)}{2}\right) \pm (\alpha-\beta) \pmod{11^3}.\end{aligned}$$

The coefficient of s^2 is $\frac{a^2\alpha^r - b^2\beta^3}{2}$. Since we are now working modulo 11^3, we need to compute a and b modulo 11^3. For this, we also need to compute α and β modulo 11^3, but afterwards we can return to their values modulo 11 since $11^2 x \equiv 11^2 y \pmod{11^3}$ if and only if $x \equiv y \pmod{11}$. With the help of Hensel's lemma, we find $\alpha \equiv 137$ and $\beta \equiv 1195$. This yields $a \equiv 1188$ and $b \equiv 198$. Finally, $a^2\alpha^r - b^2\beta^3$ is

$$1188^2 \cdot 5^3 - 198^2 \cdot 7^3 \equiv 726 \not\equiv 0 \pmod{11^3}$$

so the Strassmann bound is 3 as claimed. ■

Exercise 8.6.4. Prove that $3, 4, 5, 7, 15$ are indeed solutions to the given equation. (You may use a computer for $n = 15$.)

Solution

We have

- $1^2 + 7 = 8 = 2^3$.
- $3^2 + 7 = 16 = 2^4$.
- $5^2 + 7 = 32 = 2^5$.
- $11^2 + 7 = 128 = 2^7$.
- $181^2 + 7 = 32768 = 2^{15}$.

■

8.7 Exercises

Analysis

Exercise 8.7.1† (Vandermonde's Identity)**.** Let x and y be p-adic integers. Prove that

$$\binom{x+y}{k} = \sum_{i+j=k, i,j\geq 0} \binom{x}{i}\binom{y}{j}$$

for any k.

Solution

When x and y are natural integers, this follows from considering the coefficient of X^k in $(X+1)^{x+y} = (X+1)^x(X+1)^y$. For arbitrary p-adic integers, this follows from the density of $\mathbb{N}$ in $\mathbb{Z}_p$. ■

Exercise 8.7.2† (Mahler's Theorem)**.** Prove that a function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is continuous if and only if there exist $a_i \to 0$ such that

$$f(x) = \sum_{i=0}^{\infty} a_i \binom{x}{i}$$

for all $x \in \mathbb{Z}_p$. These a_i are called the *Mahler coefficients* of f. Moreover, show that $\max(|f(x)|_p) = \max(|a_i|_p)$.

Solution

It is clear that any such function is continuous on $\mathbb{Z}_p$, hence we need to prove that the reverse holds as well. Let $\Delta f = x \mapsto f(x+1) - f(x)$ denote the discrete derivative operator from Exercise A.3.6†. The coefficients a_k are then $\Delta^k f(0)$: indeed, a straightforward shows that $f(n) = \sum_{k=0}^{n} a_k \binom{n}{k}$ for any $n \in \mathbb{N}$, so if these a_k go to 0, f must be equal to $x \mapsto \sum_{x=0}^{\infty} a_k \binom{x}{k}$ by density and continuity.

Thus, it only remains to show that $\Delta^k f(0) \to 0$. To prove this, we will show that they eventually all become divisible by p. We can then subtract $\sum_{p\nmid \Delta^k f(0)} \Delta^k f(0)\binom{x}{k}$ from $f(x)$ and divide everything by p to conclude that $p^2 \mid \Delta^k f(0)$ for large k. Iterating this process yields that $v_p(\Delta^k f(0)) \to +\infty$ as desired.

To show this, let N be such that $p \mid f(x+p^N) - f(x)$ for any x. There exists such an N since f is continuous by assumption. Then, by Exercise A.3.7†,

$$\Delta^{p^N} f(x) = \sum_{k=0}^{N} (-1)^{p^N-k} \binom{p^N}{k} f(x+k)$$

for any $x \in \mathbb{Z}_p$. Now, by Frobenius, $(1+X)^{p^N} \equiv 1 + X^{p^N} \pmod{p}$ which means that $p \mid \binom{p^N}{k}$ for any $1 \leq k \leq p^N - 1$. Hence,

$$\Delta^{p^N} f(x) \equiv f(x+p^N) + (-1)^{p^N} f(x) \pmod{p}.$$

When p is odd this is $f(x+p^N) - f(x)$ which is divisible by p by construction, and when p is even the same holds since $-1 \equiv 1$. Hence, $p \mid \Delta^{p^N} f(x)$ for all $x \in \mathbb{Z}_p$ which implies that $p \mid \Delta^n f(x)$ for all $n \geq p^N$ as well by applying Δ multiple times to $\Delta^{p^N} f(x)$. In particular, $p \mid \Delta^n f(0)$ for sufficiently large n as wanted. ■

Exercise 8.7.4†. Prove that the following power series converge if and only if for $|x|_p < 1$ and $|x|_p < p^{-1/(p-1)}$ respctively:

$$\log_p(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k-1}x^k}{k}, \quad \exp_p(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!}.$$

In addition, prove that

1. $\exp_p(x+y) = \exp_p(x)\exp_p(y)$ for $|x|_p, |y|_p < p^{-1/(p-1)}$.
2. $\log_p(xy) = \log_p(x) + \log_p(y)$ for $|x|_p, |y|_p < 1$
3. $\exp_p(\log(1+x)) = 1+x$ for $|x|_p < p^{-1/(p-1)}$.
4. $\log_p(\exp(x)) = x$ for $|x|_p < p^{-1/(p-1)}$.

Solution

We shall only prove the convergence, the claimed equalities follow from the general theory of power series: if $g(x)$, $(f \circ g)(x)$ and $f(g(x))$ all converge, we have $(f \circ g)(x) = f(g(x))$ (this is even easier over $\mathbb{Q}_p$ because we have the strong triangle inequality). The convergence for $\log_p$ follows from the fact that that $|x^k/k|_p = |x|_p^k/|k|_p$ goes to 0 when $|x|_p < 1$ since $|k|_p > 1/k$, but does not go to 0 when $|x|_p = 1$ since $|k|_p \leq 1$ for all k.

The convergence for $\exp_p$ is very similar: by Legendre's formula,

$$v_p(x^k/k!) = kv_p(x) - \frac{k}{p-1} + \frac{s_p(k)}{p-1} = k\left(v_p(x) - \frac{1}{p-1}\right) + o(k)$$

where $o(k)/k \to 0$. This forces $v_p(x) \geq \frac{1}{p-1}$, i.e. $|x|_p \leq p^{-1/(p-1)}$. Finally, we need to see that we can't have equality. This is easy: when $v_p(x) = \frac{1}{p-1}$, $v_p(x^k/k!)$ is $\frac{s_p(k)}{p-1}$ which is bounded when k is a power of p, so does not go to infinity. ■

Exercise 8.7.5†. Prove that

$$v_2\left(\sum_{k=1}^{n} \frac{2^k}{k}\right) \to \infty.$$

Solution

The problem is equivalent to showing that $\sum_{k=1}^{\infty} \frac{2^k}{k} = 0$ in $\mathbb{Q}_2$. Note that this sum is exactly $\log_2(-1)$, which is $1/2\log_2(1) = \log_2(1) = 0$ by Exercise 8.7.4†. ■

Exercise 8.7.6† (Mean Value Theorem)**.** Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$ be a p-adic power series converging for $|x|_p \leq 1$, i.e. $a_i \to 0$. Prove that

$$|f(t+h) - f(t)|_p \leq |h|_p \max_i(|a_i|_p)$$

for any $|t|_p \leq 1$ and $|h|_p \leq p^{-1/(p-1)}$.

Solution

We shall prove that $|(t+h)^n - t^n|_p \leq |h|_p$ for any $|t|_p \leq 1$ and $|h|_p \leq p^{-1/(p-1)}$. The strong triangle inequality then implies that

$$\begin{aligned}\left|\sum_{i=0}^{\infty} a_i(t+h)^i - \sum_{i=0}^{\infty} a_i t^i\right| &= \left|\sum_{i=0}^{\infty} a_i((t+h)^i - t^i)\right| \\ &\leq \max_i(|a_i((t+h)^i - t^i)|_p) \\ &\leq |h|_p \max_i(|a_i|_p)\end{aligned}$$

as wanted. Our claim is however very easy to prove: since $|h|_p \leq p^{-1/(p-1)}$, we have $|h^k/k!|_p \leq 1$ by Legendre's formula so that

$$(t+h)^n - t^n = \sum_{k=0}^{n} t^{n-k} n(n-1)\cdot\ldots\cdot(n-(k-1))h^k/k!$$

has absolute value at most $|h|_p$ by the strong triangle inequality. ■

Absolute Values

Exercise 8.7.7†. We say an absolute value $|\cdot|$ over a field K, i.e. a function $|\cdot| \to \mathbb{R}_{\geq 0}$ such that

- $|x| = 0 \iff x = 0$
- $|x+y| \leq |x| + |y|$
- $|xy| = |x| \cdot |y|$

is *non-Archimedean* if the sequence $|m| \leq 1$ for all $m \in \mathbb{Z}$ and *Archimedean* otherwise. Prove that m is non-Archimedean if and only if it satisfies the strong triangular inequality $|x+y| \leq \max(|x|, |y|)$ for all $x, y \in K$. In addition, prove that, if $|\cdot|$ is non-Archimedean, we have $|x+y| = \max(|x|, |y|)$ whenever $|x| \neq |y|$.

Solution

It is clear that $|\cdot|$ is non-Archimedean if it satisfies the strong triangle inequality. Thus, suppose that $|m| \leq 1$ for all $m \in \mathbb{Z}$. Now, notice that, for any positive integer n,

$$\begin{aligned}|x+y|^n &= |(x+y)^n| \\ &= \left|\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right| \\ &= \sum_{k=0}^{n} \left|\binom{n}{k}\right| |x|^k |y|^{n-k} \\ &\leq n \max(|x|, |y|)^n.\end{aligned}$$

Taking the limit as n goes to ∞, we get

$$|x+y| \leq n^{1/n} \max(|x|, |y|) \to \max(|x|, |y|)$$

as wanted. For the equality, if $|x| > |y|$, note that, by the same inequality, we also have $|x| \leq \max(|-y|, |x+y|)$. Since $|-y| = |y| < |x|$, we must have $\max(|x+y|, |-y|) = |x+y|$ so $|x+y| \geq |x| \geq |x+y|$ as wanted. ■

Exercise 8.7.8†. Let K be a field and let $|\cdot| : K \to \mathbb{R}_{\geq 0}$ be a multiplicative function which is an absolute value on $\mathbb{Q}$. Suppose that $|\cdot|$ satisfies the modified triangular inequality $|x+y| \leq c(|x|+|y|)$ for all $x, y \in K$, where $c > 0$ is some constant. Prove that it satisfies the triangular inequality.

Solution

The argument is very similar to our proof of Exercise 8.7.7†. Let x, y be elements of K. For any positive integer n,

$$\begin{aligned}
|x+y|^n &= |(x+y)^n| \\
&\leq c\sum_{k=0}^{n} \left| \binom{n}{k} x^{n-k} y^k \right| \\
&= c\sum_{k=0}^{n} \left| \binom{n}{k} \right| |x|^{n-k}|y|^k \\
&\leq c\sum_{k=0}^{n} \binom{n}{k} |x|^{n-k}|y|^k \\
&= c(|x|+|y|)^n.
\end{aligned}$$

Indeed, a straightforward induction shows that $|m| \leq m$ for $m \in \mathbb{N}$ since $|\cdot|$ is an absolute value on $\mathbb{Q}$ so $|m+1| \leq |m|+|1| = |m|+1$ for any $m \in \mathbb{N}$ since $|1|^2 = |1|$ and $|1| \neq 0$. Taking the nth root and letting n tend to infinity, we get

$$|x+y| \leq c^{1/n}(|x|+|y|) \to |x|+|y|$$

as wanted. ■

Exercise 8.7.9† (Ostrowski's Theorem)**.** Let $|\cdot|$ be an absolute value of $\mathbb{Q}$. Prove that $|\cdot|$ is equal to $|\cdot|_p^r$ for some prime p and some $r \geq 1$, or to $|\cdot|_\infty^r$ for some $0 < r \leq 1$ or is the trivial absolute value $|\cdot|_0$ which is 0 at 0 and 1 everywhere else.

Solution

First, note that $f(1)^2 = f(1)$ so $f(1) = 1$ since $f(x) \neq 0$. For the same reason, $f(-1) = 1$. Now, suppose that there is some $a \in \mathbb{N}$ such that $|a| > 1$ and let $b \in \mathbb{N}$ be any integer. By the previous remark, we have $a > 1$ so let $a^m = \sum_{i=0}^{\lfloor n \log_b(a) \rfloor} a_i b^i$. We get

$$|a|^m \leq \sum_{i=0}^{\lfloor n \log_b(a) \rfloor} |a_i||b|^i$$

which implies that $|b| > 1$ as well. But then,

$$|a|^m \leq \sum_{i=0}^{\lfloor m \log_b(a) \rfloor} |a_i||b|^i \leq C|b|^{\lfloor n \log_b(a) \rfloor}$$

for some constant $C = \max(|1|, |2|, \ldots, |b-1|) > 0$ which implies that $|a| \leq |b|^{\log_b(a)}$ when we take $m \to \infty$, i.e. $|a|^{1/\log a} \leq |b|^{1/\log b}$. Since the reverse inequality is true as well by symmetry, we get that $|a|^{1/\log a} = c$ is constant. This gives us $|a| = a^{\log c} := a^r$. It is then easy to see that this extends to $|a|_\infty^r$ on all of $\mathbb{Q}$ using the multiplicativity of $|\cdot|$. Finally, it is easy to check that this satisfies the triangular inequality only for $0 < r \leq 1$.

Now suppose that $|n| \leq 1$ for all $n \in \mathbb{Z}$. By Exercise 8.7.7†, $|\cdot|$ satisfies the strong triangle inequality. Without loss of generality, assume that $|\cdot|$ is non-trivial and let $p \in \mathbb{N}$ be the smallest

positive integer such that $|p| < 1$. Since $|\cdot|$ is multiplicative, p must be prime as it has no non-trivial divisor and is distinct from 1. By assumption, $|a| = 1$ for any $1 \leq a \leq p-1$. We shall prove that $|n| = 1$ for any $p \nmid n$ to conclude that, in general,

$$|n| = |p|^{v_p(n)}|n/p| = |p|^{v_p(v)} = |n|_p^{-\log_p |p|}$$

Consider any $p \nmid n$ now and express it in base p as $\sum_i a_i p^i$. Since $p \nmid n$, we have $a_0 < p$, so $1 = |a_0| > \max_{i \geq 1} |a_i p^i|$. By the previous inequality, we are in the equality case of

$$\left|\sum_i a_i p^i\right| \leq \max_i |a_i p^i| = 1$$

so $|n| = 1$ as wanted. To conclude, it is this time easy to see that $|x+y| \leq \max(|x|, |y|)$ only when $r \geq 1$. ■

Exercise 8.7.10† (Bolzano-Weierstrass Theorem)**.** Prove that a set $S \subseteq \mathbb{R}^n$ is sequentially compact if and only if it closed, meaning that any sequence of elements of S converging in $\mathbb{R}^n$ (for the Euclidean distance) converges in S, and bounded.

Solution

Clearly, if S is unbounded or not closed, one can extract a sequence which diverges to infinity or converges to an element not in S, and thus has no convergent subsequence. Now, suppose that S is closed and bounded and let $s = (s_m)_{m \geq 0}$ be a sequence of elements of S. Without loss of generality, by translating S, suppose that all its elements have coordinates in $[0, M]$. We shall proceed by dichotomy to extract a convergent in $\mathbb{R}^n$ subsequence of s, it will thus also be convergent in S since S is closed. By the (infinite) pigeonhole principle, there must some $I_1^{(1)}, \ldots, I_1^{(n)} \in \{[0, M/2], [M/2, M]\}$ such that

$$S \cap I_1^{(1)} \times \ldots \times I_1^{(n)}$$

is infinite. Pick an element r_1 in this product of intervalls and then repeat the operation: if $I_1^{(i)} = [a_1^{(i)}, b_1^{(i)}]$, there must be some $I_2^{(i)} \in \left\{ \left[a_2^{(i)}, \frac{a_2^{(i)}+b_2^{(i)}}{2}\right], \left[\frac{a_2^{(i)}+b_2^{(i)}}{2}, b_2^{(i)}\right] \right\}$ such that

$$S \cap I_2^{(1)} \times \ldots \times I_2^{(n)}$$

is infinite. Pick an element in this product of intervalls r_2, and proceed inductively that way to get chains of intervalls $I_m^{(i)} = [a_m^{(i)}, b_m^{(i)}]$ of length $M/2^m$ such that $I_{m+1}^{(i)} \subseteq I_n^{(m)}$ and

$$S \cap I_m^{(1)} \times \ldots \times I_m^{(n)}$$

is infinite and in particular contains r_m. Since the length of $I_m^{(i)}$ is $M/2^n$, the sequences $(a_m^{(i)})_{m \geq 0}$ and $(b_m^{(i)})_{m \geq 0}$ are Cauchy, say they converge to c_i. Then, the sequence $(r_m)_{m \geq 1}$ we produced converges to $(c_1, \ldots, c_n)$ as desired. ■

Exercise 8.7.11† (Extremal Value Theorem)**.** Let M be a *metric space*, i.e. a set with a distance $d : M \to \mathbb{R}_{\geq 0}$ such that $d(x, y) = 0$ iff $x = y$, $d(x, y) = d(y, x)$ (commutativity) and $d(x, y) \leq d(x, z) + d(z, y)$ (triangle inequality) for any $x, y, z \in M$ and let S be a sequentially compact subset of M. Suppose $f : S \to \mathbb{R}$ is a continuous function. Prove that f has a maximum and a minimum.

Solution

Suppose otherwise. There is a sequence $(s_n)_{n\geq 0}$ of elements of S such that

$$f(s_n) \to s \notin \operatorname{im} f$$

(s can be $\pm\infty$). Let $(r_n)_n$ be subsequence of $(s_n)_n$ converging to $r \in S$. Then, we get

$$f(r) = \lim_{n\to\infty} f(r_n) = s$$

which is a contradiction. ■

Exercise 8.7.12† (Equivalence of Norms)**.** Let $(K, |\cdot|)$ be a complete valued field in characteristic 0, i.e. a field with an absolute value $|\cdot|$ which is complete[1] for the distance induced by this absolute value. A *norm* on a vector space V over K is a function $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ such that

- $\|x\| = 0 \iff x = 0$
- $\|x + y\| \leq \|x\| + \|y\|$
- $\|ax\| = |a|\|x\|$

for all $x, y \in V$ and $a \in K$. We say two norms $\|\cdot\|_2$ and $\|\cdot\|_2$ are *equivalence of norms* if there are two positive real numbers c_1 and c_2 such that $\|x\|_1 \leq c_1\|x\|_2$ and $\|x\|_2 \leq c_2\|x\|_1$ for all $x \in V$.[2] Prove that any two norms are equivalent over a finite-dimensional K-vector space V. In addition, prove that V is complete under the induced distance of any norm $\|\cdot\|$.

Solution

Since we wish to show that all norms are equivalent, it suffices to prove that any norm is equivalent to a fixed norm we choose. A particularly simple one is the maximum norm

$$\|x\|_\infty = \max_i |a_i|$$

where $e_1, \ldots, e_n$ is a basis of V and $x = \sum_{i=1}^n a_i e_i$ for some $a_i \in K$. In other, words this is simply the maximum of the coefficients of x in the basis $(e_1, \ldots, e_n)$. Clearly, V is complete under this norm, since if $x_k = \sum_{i=1}^n a_{k,i} e_i$ is a Cauchy sequence, then so is every $(a_{k,i})_{k\geq 0}$ for the distance induced by $|\cdot|$ which means that $a_{k,i} \underset{k\to+\infty}{\longrightarrow} a_i$ for some a_i and

$$x_k \to \sum_{i=1}^n a_i e_i.$$

Since two equivalent norms induce the same topology (a sequence is Cauchy for one norm if and only if it is Cauchy for the other), we are done if we prove that any norm $\|\cdot\|$ is equivalent to $|\cdot\|_\infty$. One inequality is very easy: if $x = \sum_{i=1}^n a_i e_i$, we have

$$\begin{aligned}\|x\| &= \left\|\sum_{i=1}^n a_i e_i\right\| \\ &\leq \sum_{i=1}^n |a_i|\|e_i\| \\ &\leq \|x\|_\infty \cdot \left(\sum_{i=1}^n \|e_i\|\right).\end{aligned}$$

[1] Recall that completeness means that all Cauchy sequences converge. A Cauchy sequence $(u_n)_{n\geq 0}$ is a sequence such that, for any $\varepsilon > 0$, there is an N such that $|u_m - u_n| \leq \varepsilon$ for all $m, n \geq N$.

[2] This means that they induce the same topology on V.

For the other inequality, suppose for the sake of a contradiction that there doesn't exist a $c > 0$ such that $\|x\| \leq c\|x\|_\infty$ for all $x \in V$. In other words, for all ε, there is some x such that $\|x\| < \varepsilon\|x\|_\infty$. In particular, $x \neq 0$. Since we have infinitely many x, by the pigeonhole principle, we can assume that $\|x\|_\infty = |a_k|$ for a fixed k, where $x = \sum_{i=1}^n a_i e_i$. By dividing x by a_k, we may also assume that $a_k = 1$. This gives us a sequence

$$x_m = y_m + e_k$$

converging to 0, where y_m is in the space W spanned by $e_1, \ldots, e_{k-1}, e_{k+1}, \ldots, e_n$. In particular,

$$\|y_m - y_\ell\| \leq \|y_m + e_k\| + \|y_\ell + e_k\|$$

also converges to 0 when $\min(m, \ell) \to +\infty$. In other words, $(y_m)_{m\geq 0}$ is a Cauchy sequence. Now, we use induction on $n = \dim V$. When $n = 1$ the result is trivial since $V = K$ and $\|\cdot\| = \|1\||\cdot|$. For the inductive step, notice that W has dimension $n-1$ so, by assumption, it is complete under $\|\cdot\|$. Hence, $(y_m)_{m\geq 0}$ converges to some $y \in W$. This means that

$$\|y + e_k\| = \lim_{m\to+\infty} \|y_m + e_k\| = 0,$$

which is impossible since $y + e_k \neq 0$. ■

Exercise 8.7.13†. Let $K = \mathbb{Q}_p$ be a local field[3], where p be a prime number or ∞ and let L be a finite extension of K. Prove that there is only one absolute value of L extending $|\cdot|_p$ on K, and that it's given by $|\cdot|_p = \left|N_{L/K}(\cdot)\right|_p^{1/[L/K]}$.[4][5][6]

Solution

For simplicity purposes, we write $|\cdot|$ for $|\cdot|_p$. We first prove the uniqueness. Suppose that $|\cdot|_{(1)}$ and $|\cdot|_{(2)}$ are two absolute values extending $|\cdot|$. Then, they are norms over the K vector space L. By Exercise 8.7.12†, they must be equivalent:

$$a|x|_{(1)} \leq |x|_{(2)} \leq b|x|_{(1)}$$

for some positive real numbers a, b. In particular, if we let $x = y^n$, we get $a|y|_{(1)}^n \leq |y|_{(2)}^n \leq b|y|_{(1)}^n$. By taking nth roots and letting n tend to infinity, this gives us

$$|y|_{(1)} \leftarrow a^{1/n}|y|_{(1)} \leq |y|_{(2)} \leq b^{1/n}|y|_{(1)} \to |y|_{(1)}$$

so $|y|_{(1)} = |y|_{(2)}$ as wanted. Note that we didn't use the fact that K was a field of the form $\mathbb{Q}_p$ here.

Now, we prove the existence. Multiplicativity is obvious, and $|x| = 0$ iff $x = 0$ too. The tricky part is to prove that it satisfies the triangular inequality $|x+y| \leq |x| + |y|$. After dividing by $|y|$, this is equivalent to $|x+1| \leq |x|+1$. We will however not prove this directly, but rather that there is a constant $c > 0$ such that $|x+1| \leq c(|x|+1)$. Assuming we have proven this, Exercise 8.7.8† tells us that we can in fact pick $c = 1$, i.e. that $|\cdot|$ satisfies the triangular inequality (and is thus an absolute value).

[3] This result is true for any complete valued field $(K, |\cdot|)$, but it is harder to prove.

[4] In particular, this absolute value is still non-Archimedean if it initially was. For instance, by Exercise 8.7.7†, if p is prime, the extension of $|\cdot|_p$ still satisfies the strong triangle inequality. In fact, this is the only interesting case since it's too hard to treat the case $K = \mathbb{R}$ separately.

[5] Here is why this absolute value is intuitive: by symmetry between the conjugates, we should have $|\alpha|_p = |\beta|_p$ if α and β are conjugates. Taking the norm yields $|N_{K/\mathbb{Q}_p}(\alpha)|_p = |\alpha|_p^{[K:\mathbb{Q}_p]}$ as indicated.

[6] One might be tempted to also define a p-adic valuation for elements of K as $v_p(\cdot) = -\log(|\cdot|_p)/\log(p)$, and this is also what we will do in some of the exercises. However, we warn the reader that, if $\alpha \in \overline{\mathbb{Z}}$ is an algebraic integer and α_p is a root of its minimal polynomial in $\overline{\mathbb{Q}_p}$, $v_p(\alpha_p) \geq 1$ does not mean anymore that p divides α in $\overline{\mathbb{Z}}$, it only means that p divides α_p in $\overline{\mathbb{Z}_p} := \{x \in \overline{\mathbb{Q}_p} \mid |x|_{\leq 1}\}$.

It remains to prove that such a c exists. Let $e_1, \dots, e_n$ be a K-basis of L (for instance $e_i = \alpha^i$ for some primitive element α). Define the maximum norm as

$$\left\| \sum_i a_i e_i \right\|_\infty = \max_i |a_i|.$$

The point is that this defines a distance $d(x,y) = |x-y|^{(\infty)}$ and that the unit sphere $S = \{x \mid \|x\|_\infty = 1\}$ is sequentially compact for this distance, so that our extension of $|\cdot|$ will have a (non-zero) minimum there by the extreme value theorem from Exercise 8.7.11†.

It is also not very hard to see that the unit sphere is indeed sequentially compact: this is the Bolzano-Weierstrass theorem from Exercise 8.7.10† for $p = \infty$, i.e. $K = \mathbb{R}$, and is very easy when p is prime by an argument similar to the proof of **??**.

To conclude, our extension of $|\cdot|$, $\sqrt[n]{|N(\cdot)|}$ is continuous for the distance induced by $|\cdot|^{(\infty)}$ because $N(\sum_i a_i e_i)$ is polynomial in the a_i. Thus, there are positive a and b such that $a \leq |x| \leq b$ for $|x|^{(\infty)} = 1$ by the extremal value theorem from Exercise 8.7.11†. Note that a is positive as $|\cdot|$ doesn't vanish on S. From this we conclude that $a\|x\|_\infty \leq |x| \leq b\|x\|_\infty$ for any x. But then, we have

$$|x+1| \leq b|x+1|_\infty \leq b(|x|_\infty + 1) \leq \frac{b}{a}(|x|+1)$$

which is what we wanted to show. ■

Exercise 8.7.14†. Let $(K, \cdot)$ be a complete valued field in characteristic 0 and let $f \in K[X]$ be a polynomial. Prove that f either has a root in K, or there is a real number $c > 0$ such that $|f(x)| \geq c$ for all $x \in K$.

Solution

Suppose without loss of generality that f is irreducible and that there does not exist a $c > 0$ such that $|f(x)| \geq c$ for all $x \in K$. In other words, $|f(x)|$ takes arbitrarily small values for $x \in K$. We will produce a Cauchy sequence $(x_n)_{n\geq 0}$ such that $|f(x_n)| \to 0$. The limit x of $(x_n)_{n\geq 0}$ will then clearly be a root of f.

We use the Newton method to find such a sequence. Let $x_0 \in K$ be such that $|f(x_0)| < 1$ is small (we will specify this later). Note that $|x_0|$ is bounded since, by the triangular inequality, if $f = a_n X^n + \ldots + a_0$, we have

$$|f(x_0)| \geq |a_n||x|^n - |a_{n-1}||x|^{n-1} - \ldots - |a_0|.$$

Define the sequence $(x_n)_{n\geq 0}$ by $x_{n+1} = x_n + \varepsilon_n$, where ε_n will be chosen in the next sentences.

Given an element $x \in K$ such that $|x^2+1|$ is small, we define the sequence $(x_n)_{n\geq 0}$ as follows. Set $x_0 = x$. Then, set $x_{n+1} = x_n + \varepsilon$ for some small ε. We have, by Taylor's formula 5.3.1

$$f(x_{n+1}) = \sum_{k=0}^{n-1} \frac{\varepsilon_n^k f^{(k)}(x_n)}{k!} = f(x_n) + \varepsilon_n f(x_n) + O(\varepsilon_n^2).$$

Hence, to kill the greatest term of this sum, we choose $\varepsilon_n = -\frac{f(x_n)}{f'(x_n)}$. Let's justify a bit the notation $O(\varepsilon_n^2)$: we have shown that, if $f(x)$ is very small then x is bounded, so the derivatives $f^{(k)}(x)$ are bounded as well. We also need to ensure that $f'(x)$ is not too small when $f(x)$ is, so that $\varepsilon_n = -\frac{f(x_n)}{f'(x_n)}$ is very small. This follows from Bézout's lemma: since f is irreducible, it is coprime with its derivative f' (we are in characteristic zero) so there are $u, v \in K[X]$ such that

$$uf + vf' = 1.$$

When $f(x)$ is very small, $u(x)$ is bounded (since x is) so $|v(x)f'(x)|$ is very close to 1. Since $v(x)$ is also bounded, we get that $|f'(x)|$ is bounded below as wanted.

To conclude, we have

$$|f(x_{n+1})| = \left|\sum_{k=0}^{n-1} \frac{\varepsilon_n^k f^{(k)}(x_n)}{k!}\right| < c|\varepsilon_n|^2$$

when $f(x_n)$ is very small. Since

$$|\varepsilon_n|^2 = \frac{|f(x_n)|^2}{|f'(x_n)|^2},$$

there is some $\theta < 1$ such that

$$|f(x_{n+1})| \leq \theta |f(x_n)|$$

when $f(x_n)$ is sufficiently small (in particular, it suffices to have $f(x_0)$ sufficiently small). Hence, pick an x_0 such that $|f(x_0)|$ is sufficiently small and this inequality is true. Then, $|f(x_n)| \leq \theta^{n-1}$ by induction so that,

$$|x_{n+1} - x_n| = \frac{|f(x_n)|}{|f'(x_n)|} \leq c\theta^n$$

for some constant $c > 0$. It is not hard to see that this implies that $(x_n)_{n\geq 0}$ is Cauchy, so we are done. ■

Exercise 8.7.15† (Ostrowski)**.** Let $(K, \cdot)$ be a complete valued Archimedean field in characteristic 0[7]. Prove that it is isomorphic to to $(\mathbb{R}, |\cdot|_\infty)$ or $(\mathbb{C}, |\cdot|_\infty)$.

Solution

Without loss of generality, suppose that $\mathbb{Q} \subseteq K$. By Exercise 8.7.9†, we may also assume that $|\cdot|$ extends the usual absolute value $|\cdot|_\infty$ of $\mathbb{Q}$, by replacing $|\cdot|$ by $|\cdot|^r$ for some suitable $r \geq 1$. This new absolute value might not satisfy the triangular inequality, but in fact it does. Indeed, by the power mean inequality, we have

$$\frac{|x|^r + |y|^r}{2} \geq \left(\frac{|x| + |y|}{2}\right)^r \geq \frac{|x+y|^r}{2^r}.$$

Setting $c = 2^{r-1}$, we get that this absolute value, which we will from now one abusively denote $|\cdot|$ as well, satisfies the modified triangular inequality $|x+y| \leq c(|x|+|y|)$. Then, by Exercise 8.7.8†, $|\cdot|$ satisfies the triangular inequality as desired.

Now, note that K contains (a field isomorphic to) $\mathbb{R}$ since it is complete and $\mathbb{R}$ is the set of limits of Cauchy sequences of rational numbers. $|\cdot|$ is then the usual absolute of $\mathbb{R}$, by construction of $\mathbb{R}$. Without loss of generality, suppose also that $\mathbb{C} \subseteq K$, by extending $|\cdot|$ to $K(i)$ if necessary. By Exercise 8.7.13†, we know that we should extend $|\cdot|$ to $K(i)$ by

$$|\alpha + \beta i| = \sqrt{|\alpha^2 + \beta^2|},$$

but we don't know if it is indeed an absolute value. To show that it is, note that, if $i \notin K$, by Exercise 8.7.14† there is a constant $c > 0$ such that

$$|\alpha^2 + \beta^2| \geq c(|\alpha|^2 + |\beta|^2)$$

for all $\alpha, \beta \in K$. Indeed, if $|x^2 + 1| \geq c/2$ for all $x \in K$, we have, for any $|\beta| \geq |\alpha|$,

$$\begin{aligned} |\alpha^2 + \beta^2| &= |\beta|^2 |(\alpha/\beta)^2 + 1| \\ &\geq |\beta|^2 c/2 \\ &\geq c(|\alpha|^2 + |\beta|^2) \end{aligned}$$

[7] In fact it is quite easy to show that $\operatorname{char} K = 0$ follows from the assumption that $|\cdot|$ is Archimedean, but we add this assumption for the convenience of the reader.

Thus, for any $\alpha, \beta, \gamma, \delta \in K$,

$$\begin{aligned}|(\alpha+\beta i)+(\gamma+\delta i)|^2 &= |(\alpha+\gamma)^2+(\beta+\delta)^2| \\ &\leq 2(|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2) \\ &\leq \frac{2}{c}(|\alpha+\beta i|^2+|\gamma+\delta i|^2)\end{aligned}$$

where the third line follows from the triangular inequality and the inequality between the arithmetic and geometric mean, so $|\cdot|$ satisfies the triangular inequality by Exercise 8.7.8† (and the quadratic-geometric mean inequality).

We will now prove that any element of K is in fact in $\mathbb{C}$, thus showing that $K = \mathbb{C}$ as wanted.

Let α be an element of K and let m be the minimum of $|\alpha - x|$ for $x \in \mathbb{C}$. This minimum exists by the Bolzano-Weierstrass theorem: we have $|\alpha - x| \geq |x| - |\alpha|$ so $|\alpha - x| \to \infty$. If we choose r such that $|\alpha - x| > |\alpha|$ for $|x| > r$, we get that the minimum of $|\alpha - x|$ over $\mathbb{C}$ is also its minimum over the ball $\{x \mid |x| \leq r\}$. However, this ball is compact by the Bolzano-Weierstrass theorem, and the function $x \mapsto |\alpha - x|$ is continuous by the triangular inequality, so a minimum exists by the extremal value theorem. We wish to prove that this minimum m is zero.

The idea is now to take an x such that $|\alpha - x|$ is large, and, at the same time, $A - x$ divides a polynomial f such that $|f(\alpha)|$ is small. If we let $g = \frac{f}{A-x}$, we get that $|g(\alpha)|$ is quite small so that one of $|\alpha - z|$ where z is a root of g is small, and in particular smaller than m. Since the remainder of a polynomial f modulo $A - x$ is $f(x)$, we can relax the condition to $|f(\alpha)|$ small and $|f(x)|$ as well. With these conditions, it is natural to pick f first and then x: an obvious candidate for f is

$$f = (A - y)^n$$

where y is such that $|\alpha - y| = m$. Now, we need to estimate $|f(\alpha) - f(x)|$. By the triangular inequality, it is at most $m^n + |x - y|^n$. In particular, if $\varepsilon = |x - y| < 1$, it is at most m^n plus something very small. In addition, by definition, we know that $|g(\alpha)| \geq m^{n-1}$, where $g = \frac{f - f(x)}{A - x}$. Hence,

$$|\alpha - x| m^{n-1} \leq |g(\alpha)||\alpha - x| = |f(\alpha) - f(x)| \leq m^n + \varepsilon^n.$$

This means that, if m is non-zero, by dividing by m^n,

$$|\alpha - x| \leq m\,(1 + (\varepsilon/m)^n) \to m.$$

Thus, $|\alpha - x| = m$ for all $|x - y| < 1$. Iterating this process, we get $|\alpha - x| = m$ for all $x \in \mathbb{C}$ which is obviously a contradiction since $|\alpha - x|$ goes to ∞ when $|x| \to \infty$. Hence, $|\alpha - z| = 0$ for some $z \in \mathbb{C}$, i.e. $\alpha = z \in \mathbb{C}$ as wanted. ■

Diophantine Equations

Exercise 8.7.16† (Brazilian Mathematical Olympiad 2010)**.** Find all positive rational integers n and x such that $3^n = 2x^2 + 1$.

Solution

We proceed as in Proposition 8.6.1: working in $\mathbb{Q}(\sqrt{-2})$, we find $1 + \sqrt{-2}x = (1 \pm \sqrt{2})^n$, i.e.

$$(1 + \sqrt{-2})^n + (1 - \sqrt{-2})^n = \pm 2.$$

To solve this, we shall work in $\mathbb{Q}_{11}$. We thus consider $\alpha = 1 \pm \sqrt{-2}$ and $\beta = 1 \mp \sqrt{-2}$ as elements of $\mathbb{Q}_{11}$; Hensel's lemma gives us $\alpha \equiv 20 \pmod{121}$ and $\beta \equiv 103 \pmod{121}$. We wish to find the zeros of the linear recurrence $\alpha^n - \beta^n \pm 2$. Note that we have $\alpha^n - \beta^n \equiv \pm 2$ modulo 11 only when $n \in \{0, 1, 2\}$, so we restrict our attention to these n.

Set $a = \alpha^5 - 1 \equiv 0 \pmod{11}$ and $b = \beta^5 - 1 \equiv 0 \pmod{11}$. We shall compute the Strassmann bounds of the analytic functions

$$f_r(s) = \alpha^r(1+a)^s - \beta^r(1+b)^s$$

for $r \in \{0,1,2\}$. Modulo 11^2, we have

$$f_r(s) \equiv \alpha^r(1+as) + \beta^r(1+bs) - 2.$$

The coefficient of s is $\alpha^r a + \beta^r b$. However, for $r \in \{1,2\}$, this is respectively 44 and 88 modulo 11^2 so non-zero in both cases. Hence, the Strassmann bounds for f_1 and f_2 are 1. It remains to compute the Strassmann for f_0. This time, we have $a + b \equiv 0 \pmod{11^2}$ so we need to expand one more term. We get

$$f_0(s) = (1+a)^s + (1+b)^s - 2 \equiv 1 + as + a^2\binom{s}{2} + 1 + b^2\binom{s}{2} - 2 \pmod{11^3}.$$

The coefficient of s^2 is thus $\frac{a^2+b^2}{2}$ modulo 11^3. However, we can check with Hensel's lemma that $\alpha \equiv 587 \pmod{11^3}$ and $\beta \equiv 746 \pmod{11^3}$, which yields $a \equiv 1012 \pmod{11^3}$ and $b \equiv 317 \pmod{11^3}$. One can then verify that

$$a^2 + b^2 \equiv 847 \not\equiv 0 \pmod{11^3}.$$

Hence, the Strassmann bound for 0 is 2.

To finish, we need to find solutions: two solutions congruent to 0 modulo 5, one congruent to 1 modulo 5, and one congruent to 2 modulo 5. It is not hard to see that we indeed have

$$\begin{aligned} 3^0 &= 2 \cdot 0^2 + 1 \\ 3^1 &= 2 \cdot 1^2 + 1 \\ 3^2 &= 2 \cdot 2^2 + 1 \\ 3^5 &= 2 \cdot 11^2 + 1. \end{aligned}$$

Hence, we have found all solutions: $(n,x) \in \{(0,0),(1,1),(2,2),(5,11)\}$. ■

Exercise 8.7.19†. Solve the diophantine equation $x^2 - y^3 = 1$ over $\mathbb{Z}$.

Solution

Write this equation as $(x-1)(x+1) = y^3$. The gcd of the two factors divides 2, so we have $x - 1 = a^3$ and $x + 1 = b^3$ or $x \pm 1 = 2a^3$ and $x \mp 1 = 4b^3$ for some $a, b \in \mathbb{Z}$. The former is impossible, so we must be in the latter case. The problem thus reduces to solving the equation $a^3 - 2b^3 = \pm 1$ in rational integers. We know by Section 7.4 that

$$a - b\sqrt[3]{2} = \pm\theta^n$$

for some n, where θ is the fundamental unit of $\mathbb{Q}(\sqrt[3]{2})$. In addition, by Exercise 7.5.18†, we know that we can choose $\theta = 1 - \sqrt[3]{2} = -\frac{1}{1+\sqrt[3]{2}+\sqrt[3]{4}}$. Hence, we wish to have $a - b\sqrt[3]{2} = \pm(1-\sqrt[3]{2})^n$. As we saw in the proof of Theorem 7.4.2, for a given n, there are such a, b if and only if

$$(1-\sqrt[3]{2})^n + j(1-j\sqrt[3]{2})^n + j^2(1-j^2\sqrt[3]{2})^n = 0.$$

We work in $\mathbb{Q}_3(\alpha, j)$, where $\alpha^3 = 2$ and j is now a tryadic root of unity of order 3. Note that this has degree 6 over $\mathbb{Q}_3$ since $j \notin \mathbb{Q}_3$ and $\alpha \notin \mathbb{Q}_3(j)$ (for instance because $\mathrm{Gal}(\mathbb{Q}_3(j)/\mathbb{Q}_3)$ is abelian but $\mathrm{Gal}(\mathbb{Q}_3(\alpha)/\mathbb{Q}_3)$ isn't). In particular, $\alpha_0 = \alpha$, $\alpha_1 = j\alpha$ and $\alpha_2 = j^2\alpha$ are conjugate.

We wish to find when the linear recurrence $(1-\alpha)^n + j(1-j\alpha)^n + j^2(1-j^2\alpha)^n$ is zero. Here is the magic: this is already almost a tryadic analytic function. Indeed, we can rewrite it as

$$2^n((1+\pi_0)^n + j(1+\pi_1)^n + j^2(1+\pi_2))$$

where $\pi_k = -(1+\alpha j^k)/2$ has norm $-3/8$ and thus tryadic absolute value $3^{-1/3} < 1$. (In fact, $1+\sqrt[3]{2}$ is prime in $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Z}[\sqrt[3]{2}]$.) However, $3^{-1/3}$ is still too large: it's greater than $3^{-1/(3-1)}$. Hence, we consider the function

$$f_r(s) = (1+\pi_0)^r(1+\pi_0)^{3s} + j(1+\pi_1)^r(1+\pi_1)^{3s} + j^2(1+\pi_2)^r(1+\pi_2)^{3s}$$

for $r \in [3]$. Indeed, these converge since $(1+\pi_k)^3 = 1 + 3(-3/8 - \alpha_k/8 + \alpha_k^2/8)$ has absolute value $3^{-1} < 3^{-1/(3-1)}$. It is then straightforward to compute the Strassmann bounds: we claim that it is 1 for $r = 0$ and $r = 1$, and 0 for $r = 2$. Let us start with $r = 0$. In that case,

$$f_0(s) \equiv s\sum_{k=0}^{2} j3(-3/8 - \alpha j^k/8 + \alpha^2 j^{2k}/8) \pmod{27}.$$

It is in fact very easy to compute a sum of the form $\sum_{k=0}^{2} j^k \sum_i a_i j^{ki}$: this is a unity root filter so is the sum $3\sum_{i\equiv -1 \pmod 3} a_i\alpha^i$ (see Exercise A.3.9†). This is actually normal: it's why we considered this sum in the first place. In particular, this also explains why this congruence holds modulo 3^3 instead of simply 3^2: it's because of the additional factor of 3 added by the unity root filter. Hence, the coefficient of s of f_0 is $9\alpha^2/8$ which has tryadic valuation $2 < 3$ and 1 is thus the Strassmann bound for f_0. Conversely, it is clear that $s = 0$ is a solution (corresponding to $1 = (1-\sqrt[3]{2})^0$).

We now consider f_1. As before, we are done if the coefficient of s has tryadic valuation 2 since all the following ones have valuation at least 3. We expand f_1 modulo 27, and remember that we only care about the coefficient of α^{3n+2}:

$$\begin{aligned} f_1(s) &= \sum_{k=0}^{2} j^k(1-\alpha_k)/2 \cdot (1 + 3(-3/8 - \alpha_k/8 + \alpha_k^2/8))^s \\ &\equiv \sum_{k=0}^{2} j^k(1-\alpha_k)/2 + 3s\sum_{k=0}^{2} j^k(1-\alpha_k)/2 \cdot (-3/8 - \alpha_k/8 + \alpha_k^2/8) \pmod{27} \\ &= -9s\alpha^2/8 \end{aligned}$$

which has absolute value 3^{-2} as desired. It is again clear that $s = 0$ is a solution (corresponding to $1 - \sqrt[3]{2} = (1-\sqrt[3]{2})^1$).

Finally, we consider f_2. Here is what changes: the coefficient of s^0 is no longer zero because $(1-\alpha)^2$ now has a non-zero coefficient for some α^{3n+2}. More specifically,

$$\begin{aligned} f_2(s) &= \sum_{k=0}^{2} j^k(1-\alpha_k)^2/4 \cdot (1 + 3(-3/8 - \alpha_k/8 + \alpha_k^2/8))^s \\ &\equiv \sum_{k=0}^{2} j^k(1-\alpha_k)^2/4 \pmod{9} \\ &= -3\alpha^2/4 \end{aligned}$$

which has absolute value 3^{-1} as desired. This shows that the Strassmann bound is 0, and concludes our study of the equation $a - b\sqrt[3]{2} = \pm(1-\sqrt[3]{2})^n$: the only solutions are $a = \pm 1$, $b = 0$ as well as $a = b = \pm 1$. If we go back to the original problem, these correspond to $x \pm 1 = 2a^3 = \pm 2$, i.e. $x \in \{\pm 1, \pm 3\}$. These then yield $(x, y) \in \{(\pm 1, 0), (\pm 3, 2)\}$, which are, in conclusion, the only rational integer solutions to the equation $x^2 - y^3 = 1$. ■

Exercise 8.7.20† (Lebesgue)**.** Solve the equation $x^2+1=y^n$ over $\mathbb{Z}$, where $n\geq 3$ is an odd integer.

Solution

Suppose (x,y) is a solution. By the unique factorisation in $\mathbb{Z}[i]$, we have $xi+1=\varepsilon(a+bi)^n$ for some $a,b\in\mathbb{Z}$ and $\varepsilon\in\mathbb{Z}[i]$ a unit. Note that $y=a^2+b^2$ is odd, since x^2+1 is never divisible by 4, so one of a,b is even and the other is odd. Since the units of $\mathbb{Z}[i]$ have the form i^k for some k by Exercise 2.2.3*, they are all nth powers since n is odd, so we can assume $\varepsilon=1$.

Hence, we wish to find the $a,b\in\mathbb{Z}$ such that $(a+bi)^n+(a-bi)^n=2$. Since n is odd, this is divisible by $2a$ so a is ± 1. Since $y=a^2+b^2$ is odd, b must be even. Expanding the real part of $(a+bi)^n$ (which must be 1), we get

$$\sum_{k=0}^{\frac{n-1}{2}}\binom{n}{2k}a^{n-2k}(-1)^k b^{2k}=1.$$

Modulo b^2 we get $b^2\mid 1-a^n\in\{0,2\}$, and since b^2 is at least 4 since b is even, a must be 1. In other words, our equation becomes

$$(1+bi)^n+(1-bi)^n=2.$$

We wish to expand the LHS as a dyadic analytic function, but this is not possible because $|b|_2$ might be equal to $2^{-\frac{1}{2-1}}=2^{-1}$, i.e. b might have dyadic valuation equal to 1. To remedy this situation, we use the LTE lemma:

$$(1+bi)^2=(1+2b(i-b/2)).$$

Since n is odd, we can set $n=2m+1$ and reduce the problem to finding the zeros of the now dyadic analytic function

$$f(m)=(1+bi)(1+2b(i-b/2))^m+(1-bi)(1+2b(-i-b/2))^m-2$$

where i is now a square root of -1 in $\overline{\mathbb{Q}_2}$. Since this a root of unity filter (see Exercise A.3.9†), as in Exercise 8.7.19†, $f(m)$ is twice the "real dyadic" part of $(1+bi)(1+2b(i-b/2))^m-1$, i.e. the coefficient of 1 in this expression. Now expand this as

$$-1+(1+bi)\sum_{k=0}^{\infty}\binom{m}{k}\left(2b(i-b/2)\right)^k.$$

Suppose that $b\neq 0$, otherwise we get $x=0$ and $y=1$. Since $v_2(k!)\leq k-1$ by Legendre's formula, every term except the first two vanish modulo $2b^2$. Hence, modulo b^2, this is simply

$$-1+(1+bi)(1+2bm(i-b/2)).$$

If we expand this while focusing only on the real dyadic part, we get

$$(1-b^2m)+bi\cdot 2bim-1=-3b^2m.$$

Since $|b^2|_2>|2b^2|_2$, we conclude that the Strassmann bound is (at most) 1. Since $m=0$ is a trivial solution, we conclude that it is the only solution (corresponding to $n=1$, which is not the case). Thus, the only solution $(x,y)=(0,1)$. ■

Remark 8.7.1

We can also finish directly with a slightly ad-hoc dyadic method once we reach

$$\sum_{k=1}^{\frac{n-1}{2}} \binom{n}{2k} (-1)^k b^{2k-2} = 0.$$

Let m be the dyadic valaution of $\binom{n}{2} = \frac{n(n-1)}{2}$. We will prove that 2^{m+1} divides $\binom{n}{2}$, which is of course a contradiction. The denominator of $\binom{n}{2k}$ is $(2k)!$. By Legendre's formula, we have $v_2((2k)!) = 2k - s_2(2k) \leq 2k-1$. As a result, $\frac{b^{2k-2}}{(2k)!}$ has dyadic valuation at least -1. Since $(n-1)(n-3)$ divides $(2k)!\binom{n}{2k}$, we conclude that

$$v_2\left(\binom{n}{2k} b^{2k}\right) \geq v_2((n-1)(n-3)) + v_2(b^{2k}/(2k)!) \geq m+2-1 = m+1$$

as wanted since $m = v_2\left(\frac{n-1}{2}\right) = v_2(n-1) - 1$. Hence, 2^{m+1} divides every term of the sum

$$\sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2k+2} (-1)^k b^{2k} = 0.$$

except the first one, which means that it also divides the first one.

Exercise 8.7.21†. Solve the equation $x^2 + 1 = 2y^n$ over $\mathbb{Z}$, where $n \geq 3$ is an odd integer.

Solution

Suppose (x, y) is a solution. By factorising in $\mathbb{Z}[i]$, we get $xi + 1 = \varepsilon(1+i)(a+bi)^n$ for some $a, b \in \mathbb{Z}$ and a unit $\varepsilon \in \mathbb{Z}[i]$. Note that $y = a^2 + b^2$ is odd, since $x^2 + 1$ is never divisible by 4, so one of a, b is even and the other is odd. Since the units of $\mathbb{Z}[i]$ have the form i^k for some k by Exercise 2.2.3*, they are all nth powers since n is odd, so we can assume $\varepsilon = 1$.

By assumption,

$$\begin{aligned} 2 &= (1+ix) + (1-ix) \\ &= (1+i)(a+bi)^n + (1-i)(a-bi)^n \\ &= i(1-i)(a+bi)^n + (1-i)(a-bi)^n \\ &= (1-i)\left((\pm b \mp ia)^n + (a-bi)^n\right) \end{aligned}$$

where the ± 1 sign depends on n modulo 4. Since n is odd, this last expression is divisible by

$$\pm b \mp ia + a - bi = (a-b)(1 \mp i).$$

Thus, $(1-i)(a-b)(1 \mp i)$ divides 2. This is equivalent to $a - b \mid 1$, so $a - b = \pm 1$. Without loss of generality, suppose that a and b are non-zero since $\{|a|, |b|\} = \{0, 1\}$ yields $y = 1$ and thus $x = \pm 1$. Now we distinguish a few cases, depending on which one of a and b is even and whether $a - b$ is 1 or -1.

1. b is even and $a - b = 1$. In that case, our equation is

$$f(n) := (1+i)(1+b(1+i))^n + (1-i)(1+b(1-i))^n - 2 = 0.$$

Unlike Exercise 8.7.20†, this is already a dyadic analytic function since $|(1+i)|_2 = 2^{-1/2}$ which means that $|b(1+i)|_2 \leq 2^{-3/2} < 2^{-\frac{1}{2-1}}$ (we are working with the dyadic $i \in \overline{\mathbb{Q}_2}$). This is a unity root filter, so we are just focusing on the "real dyadic" part of $(1+i)(1+b(1+i))^n - 1$. When we expand this modulo b^3, we get

$$(1+i)(1+b(1+i)n + b^2(1+i)^2 n(n-1)/2) - 1 = i + 2bin + (1+i)2b^2 in(n-1)/2$$

since $(1+i)^2 = 2i$, which has real dyadic part $-b^2n(n-1)$. Clearly, $|b^2|_2 > |b^3|_2$ since $b \neq 0$ so the Strassmann bound is 2. The previous computation in fact shows that the first two coefficients of f are zero (when written as a Mahler series $\sum_{k=0}^{\infty} a_k \binom{x}{k}$), which means that $n = 0$ and $n = 1$ are solutions. In other words, these are the only solutions, which are ruled out by the statement.

2. b is even and $a - b = -1$. Since n is odd, we have $(-1 + b(1 \pm i))^n = -(1 - b(1 \pm i))^n$ so our equation is

$$f(n) := (1+i)(1-b(1+i))^n + (1-i)(1-b(1-i))^n + 2 = 0.$$

The same computation as before shows that the coefficient of $\binom{n}{1}$ is $-2bi + 2bi = 0$. Thus, modulo $2b^2$, we have

$$f(n) \equiv 4 + 0n$$

so the Strassmann bound is 0 since $|2b^2|_2 < |4|_2$. There are no solutions in this case.

3. a is even. Then, $a + bi = \pm i + a(1+i)$ so the equation is

$$(1+i)(\pm i + a(1+i))^n + (1-i)(\pm i + a(1-i))^n - 2 = 0.$$

Since $(\pm i + \alpha)^n = \pm i(1 + \pm i\alpha)^n$ for any $\alpha \in \mathbb{Q}_2(i)$, where the $\pm$ are independent and depend on whether $n \equiv 1 \pmod 4$ or $n \equiv -1 \pmod 4$, our equation is

$$f(n) = (1+i)(1 \pm ia(1+i))^n + (1-i)(1 \pm ia(1-i))^n \pm 2i = 0.$$

where the first two $\pm$ signs are the same and the last one is independent. We will prove that the Strassmann bound is always 0. Modulo $2a$ (this is a unity root filter so the "real dyadic" part gets doubled), we have

$$f(n) \equiv 2(1 + \pm i).$$

Since $|2a|_2 < |2(1 \pm i)|_2$, we are done.

To conclude there are no solutions to the equations $x^2 + 1 = 2y^n$ when y is not equal to 1 and $n \geq 3$, i.e. the only solutions to our equation are $(\pm 1, 1)$. ■

Linear Recurrences

Exercise 8.7.22†. Let $(u_n)_{n\geq 0}$ be a linear recurrence of rational integers given by $\sum_i f_i(n)\alpha_i^n$ such that α_i/α_j is not a root of unity for $i \neq j$. If u_n is not of the form $a\alpha^n$ for some $a, \alpha \in \mathbb{Z}$, prove that there are infinitely many prime numbers p such that $p \mid u_n$ for some integer $n \geq 0$.

Solution

Without loss of generality, suppose that u_n is not identically zero. By Corollary 8.5.2 and Corollary 8.5.1, the condition on the α_i tells us that $|u_n| \to \infty$. The idea is that we will bound the p-adic valuation of u_n over a subsequence $(u_{an+b})_{n\geq 0}$ to get a contradiction if $(u_n)_{n\geq 0}$ has finitely many prime divisors (since $(u_{an+b})_{n\geq 0}$ would then be bouded).

We shall analyze the local behaviour of $(u_n)_{n\geq 0}$ for a fixed prime p. Write $u_n = \sum_i f_i(n)\alpha_i^n$. We wish to factorise α_i by a suitable power of p so that $\max_i |\alpha_i|_p = 1$. Indeed, since $|p^{1/n}|_p^n = |p|_p = 1/p$, the absolute values of powers of p take any value which can be taken by $|\cdot|_p$. Thus, suppose that $\max_i |\alpha_i|_p = 1$ and consider the sequence $v_n = \sum_{i\in I} f_i(n)\alpha_i(n)$ where I denotes the set of i such that $|\alpha_i|_p = 1$.mb Let K_p be the field generated by the α_i. We claim that that the integers $\mathcal{O}_{K_p} := \{|x|_p \leq 1 \mid x \in K_p\}$ of K_p are finite modulo p^k, for any fixed k. This implies (by the pigenhole principle) that $(v_n)_{n\geq 0}$ is periodic modulo p^k for any k. To prove our

claim, suppose for the sake of a contradiction that there were infinitely many elements of $\mathcal{O}_{K_p}$ non-congruent modulo p^k, say f is a set of such elements. Pick a primitive element β of $K_p/\mathbb{Q}_p$ with conjugates $\beta_1, \dots, \beta_d$, and consider an element $x = \sum_{i=0}^{d-1} b_i \beta^i \in \mathcal{O}_{K_p}$. By definition of the p-adic absolute value, we also have $|x_i| \leq 1$, where x_i is the image of x under the embedding $\beta \to \beta_i$. To conclude, Cramer's rule (Exercise C.5.7) or the adjugate (Proposition C.3.7) let us express the b_i as linear combinations of the β_j^i and the x_i. Then, using the triangle inequality, we conclude that $|b_0|_p, \dots, |b_{d-1}|_p$ are bounded. As a consequence, the set

$$\{(b_0, \dots, b_{d-1}) \mid \left| \sum_{i=0}^{d-1} b_i \beta^i \right| \leq 1\} \subseteq \mathbb{Q}_p^n$$

is compact. In particular, $\mathcal{O}_{K_p}$ is as well, and thus S too. This implies that there are $s, r \in S$ such that $|s - r|_p$ is arbitrarily small, but then they will be equal modulo p^k since

$$u \equiv v \pmod{p^k} \iff \frac{u-v}{p^k} \in \mathcal{O}_{K_p} \iff |u-v|_p \leq |p^k| = p^{-k}.$$

To conclude, note that $(v_n)_{n\geq 0}$ is non-zero for large n by the Skolem-Mahler-Lech theorem. Pick any N so that v_N is non-zero, and let T_p be the period of $(v_n)_{n\geq 0}$ modulo $p^{\lfloor v_p(v_n) \rfloor + 1}$. Then, $|v_{N+kT_p}|_p$ is greater than some constant $c > 0$ for any k, and thus $|u_{n+kT_p}|_p$ as well for sufficiently large $n + kT_p$, since $u_n - v_n \to 0$. If we finally return to the global behaviour and let p vary among our finitely many prime divisors of $(u_n)_{n\geq 0}$, we get that, for any sufficiently large N, $v_p(u_{N+k\prod_p T_p})$ is bounded for any p and for any sufficiently large k. This contradicts the assumption that $|u_n| \to \infty$. ■

Remark 8.7.2

Note that, to prove that α^n is periodic modulo p for $\alpha \in \mathcal{O}_{K_p}$, we cannot simply "convert" (with the fundamental theorem of symmetric polynomials, after having introduced its conjugates) α to an element of $\overline{\mathbb{F}}_p$ and use the Frobenius morphism. Why? Because the minimal polynomial of α does not necessarily have coefficients in $\mathbb{Z}_p$. Indeed, we only consider the constant coefficient of the minimal polynmomial of α to compute its p-adic absolute value, and disregard all other coefficients. For instance, the roots of $X^2 - X/2 + 1$ over $\mathbb{Q}_2$ are in the unit ball.

As another remark, it has in fact been proven, using a generalisation of (a p-adic extension of) the Thue-Siegel-Roth theorem (see Remark 7.4.3) that u_n either has the form $c\alpha^n$, or its greater prime factor tends to infinity. See [28].

Exercise 8.7.23†. Does there exists an unbounded linear recurrence $(u_n)_{n\geq 0}$ such that u_n is prime for all n?

Solution

Suppose for the sake of a contradiction that $(u_n)_{n\geq 0}$ is such a sequence. Without loss of generality, suppose that $|u_n| \to \infty$ by replacing $(u_n)_{n\geq 0}$ by $(u_{Nn+m})_{n\geq 0}$ for some suitable N, m, as indicated after Corollary 8.5.2. Now, let m be sufficiently large so that $u_m = p$ is a prime which doesn't divide the denominator of the norm of any algebraic number appearing in the formula of u_m (so that they still make sense modulo p). Finite fields theory (e.g. Theorem 4.2.1) tells us that there exists a k $u_{np^k} \equiv u_n \pmod{p}$ for any n. Indeed, if $u_n \equiv \sum_i f_i(n)\alpha_i^n$, with $f_i \in \overline{\mathbb{F}}_p[X]$ and $\alpha_i \in \mathbb{F}_p$, it suffices to pick k so that $f_i \in \mathbb{F}_{p^k}[X]$ and $\alpha_i \in \mathbb{F}_{p^k}$, by the Frobenius morphism.

In particular, $u_{mp^{\ell k}} \equiv 0 \pmod{p}$ for any ℓ. By assumption, this means that $u_{mp^\ell} = p$, contradicting the fact that $u_n \to \infty$. ■

Miscellaneous

Exercise 8.7.24†. Which roots of unity are in $\mathbb{Q}_p$?

Solution

Let $\alpha = (a_1, a_2, \ldots)$ is a root of unity of order n in $\mathbb{Q}_p$. Suppose initially that p is odd. We first focus on the case where $p \nmid n$. We have $a_k^n \equiv 1 \pmod{p^k}$. However, the group of units modulo p^k is isomorphic to $p^{k-1}(p-1)$ by Exercise 3.5.18† (in more elementary terms: there is a primitive root) so we also have

$$a_k^{\gcd(p-1,n)} \equiv a_k^{\gcd(p^{k-1}(p-1),n)} \equiv 1.$$

Hence, α has order dividing $\gcd(p-1,n)$, which implies that $n \mid p-1$ since n is the order of α. Now suppose that $p \mid n$. We wish to reach a contradiction, so suppose without loss of generality that α has order exactly p, by replacing it by $\alpha^{n/p}$. Then, $a_k^p \equiv 1 \pmod{p^k}$ so $a_k \equiv 1 \pmod{p}$ which implies that

$$v_p(a_k^p - 1) = 1 + v_p(a_k - 1)$$

by LTE. For large k, $v_p(a_k - 1)$ stabilises since $\alpha \neq 1$, which means that this cannot be at least k.

It remains to provide a construction for $(p-1)$th roots of unity. One can do this using the structure of $(\mathbb{Z}/p^k\mathbb{Z})^\times$, or by means of Hensel's lemma: the derivative of $X^p - X$ is 1 which is never zero so we can lift all roots of $X^p - X$ modulo p to roots in $\mathbb{Q}_p$. This is called the *Teichmüller character* ω which sends $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ to the unique root of $X^{p-1} - 1$ congruent to x modulo p.

It remains to treat the case where $p = 2$. When n is odd, the same argument as before works: this time we even have $a_k^{\gcd(2^{k-2}(2-1),n)} \equiv 1 \pmod{2^k}$ for $k \geq 2$. However, unlike the previous case, there is now a root of unity of order 2: -1. Since the only root of unity of odd order is 1, the order of any root of unity must be a power of 2, since $\alpha^{2^{v_2(n)}}$ is a root of unity of odd order. Hence, we shall prove that there is no root of unity of order 4. This is easy: we use the LTE for $p = 2$ (which simply amounts to the fact that a square is always 1 modulo 4) to get

$$v_2(a_k^4 - 1) = 1 + v_2(a_k^2 - 1)$$

and this stabilises since $\alpha^2 \neq 1$ by assumption. This time, the Teichmüller character is defined as $\omega : (\mathbb{Z}/4\mathbb{Z})^\times : \mathbb{Q}_2$ sending 1 to 1 and -1 to -1.

To conclude, the roots of unity of $\mathbb{Q}_p$ are all $(p-1)$th roots of unity, as well as a root of order 2 when $p = 2$. ■

Exercise 8.7.27† (China TST 2010)**.** Let $k \geq 1$ be a rational integer. Prove that, for sufficiently large n, $\binom{n}{k}$ has at least k distinct prime factors.

Solution

The key lemma is that, for any prime p and any positive integer n, $p^{v_p\left(\binom{n}{k}\right)} \leq n$. Suppose that we have proven this. Then, if $\binom{n}{k}$ has at most $k-1$ prime factors, say $p_1, \ldots, p_m$, we have

$$\binom{n}{k} = \prod_{i=1}^{m} p_i^{v_{p_i}\left(\binom{n}{k}\right)} \leq n^m \leq n^{k-1}$$

which is impossible for large n since $\binom{n}{k}$ is a polynomial of degree k in n.

It remains to prove this key claim. We use Legendre's formula and the fact that $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ to write

$$v_p\left(\binom{n}{k}\right) = \sum_{i=1}^{\lfloor \log_p(n) \rfloor} \left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n-k}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^i} \right\rfloor.$$

The wanted result now follows from the trivial inequality $\lfloor x+y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$: each of the terms $\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n-k}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^i} \right\rfloor$ is at most 1, so the whole sum is less than or equal to $\lfloor \log_p(n) \rfloor$. This gives us $v_p\left(\binom{n}{k}\right) \leq \log_p(n)$, i.e. $p^{v_p\left(\binom{n}{k}\right)} \leq n$ as claimed. ■

Exercise 8.7.28†. Find all additive functions $f : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}$, where addition is defined componentwise. (To those who have read Section C.2, the fact that there are a nice characterisation of those functions should come off as a surprise.)

Solution

We claim that the $\mathbb{Z}$-linear functions from $\mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}$ are given by linear combinations of the coordinates, which is surprising since the vectors e_i with 1 in the ith coordinate and 0 everywhere else do not form a basis of $\mathbb{Z}^{\mathbb{N}}$: any linear combination of them has finitely many non-zero coordinates (so $(1, 1, \ldots)$ isn't one for instance)! This problem thus has two parts: proving that any such function is 0 on all but finitely many e_i, and proving that an additive function which is 0 on the e_i is identically 0. We will do the second part first.

Suppose that $f : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}$ is additive and $f(e_i) = 0$ for all i, i.e. f is 0 on the space of vectors with finitely many non-zero coordinates. The special property of $\mathbb{Z}$ is that we can use the theory of divisibility. More precisely, if the coordinates of $x \in \mathbb{Z}^{\mathbb{N}}$ eventually get all divisible by m, then $m \mid f(x)$. Indeed, if $x = (x_0, x_1, \ldots)$ is such that $m \mid x_n$ for any $n \geq N$, we have

$$f(x) = f(0, \ldots, 0, x_N, x_{N+1}, \ldots) = mf(0, \ldots, 0, x_N/m, x_{N+1}/m, \ldots).$$

Thus, if the x_i get eventually all divisible by increasingly large integers, $f(x)$ must be zero! For instance, $f(a_0, a_1 p, a_2 p^2, \ldots)$ is divisible by p^n for any n so must be zero. You should now be able to see the p-adic flavor of this problem (even if we won't really use any of the theory developped in this chapter)! In particular, x is congruent modulo p to

$$f(x_0, x_1(p+1), x_2(p+1)^2, \ldots) = 0.$$

Since this is true for abritrary p, $f(x)$ must be 0 too. Alternatively, using Bézout's lemma, there are $2^n y_n$ and $3^n z_n$ such that $2^n y_n + 3^n z_n = x_n$. Thus,

$$f(x) = f(y_0, 2y_1, 4y_2, \ldots) + f(z_0, 3z_1, 9z_2, \ldots) = 0 + 0 = 0.$$

Now we prove that any additive function $f : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}$ is 0 on all but finitely many e_i, say $i \notin I$. This implies that the function $x \mapsto f - \sum_{i \in I} f(e_i) x_i$, where x_i denotes the ith coordinate of x, is zero on every e_i so must be identically zero by the previous step. This shows that any additive function is a linear combinations of the coordinate.

The idea will again be p-adic. We will produce a sequence $x = (x_0, x_1, \ldots)$ such that $v_2(x_n)$ is increasing and grows so fast that $f(e_i)$ must be 0 for large i, since we have the congruence

$$f(x) \equiv \sum_{i=0}^{n-1} x_i f(e_i) \pmod{2^{v_2(x_n)}}.$$

We can rephrase this as saying that the series $\sum_{i=0}^{\infty} x_i f(e_i)$ converges dyadically to the **rational** integer $f(x)$. The point is that we have too many degrees of freedom for this to be always a

rational integer, unless $f(e_i) = 0$ for sufficiently large i. This follows from the fact that, if we write the dyadic expansion of a dyadic integer as $\sum_{i=0}^{\infty} a_i 2^i$ with $a_i \in \{0, 1\}$, then the dyadic integers with a finite dyadic expansion are exactly the rational integers. Indeed, this decomposition is unique for the same reason that the base 2 decomposition is: if $\sum_{i=0}^{\infty} a_i 2^i = \sum_{i=0}^{\infty} b_i 2^i$, pick the smallest n such that $a_n \neq b_n$ to get $a_n 2^n \equiv b_n 2^n \pmod{2^{n+1}}$, i.e. $a_n = b_n$, which is a contradiction. Thus, the dyadic expansion of a rational integer must be its base 2 expansion, which is indeed finite.

Hence, we pick $x_i = 2^{n_i}$ with $(n_i)_{i\geq 0}$ an increasing sequence which grows sufficiently fast. More precisely, if we write $2^{n_i} f(e_i)$ in base 2 as $\sum_{k=n_i}^{m_i} a_k 2^k$, we want n_{i+1} to be larger than m_i. That way, the base 2 expansion of $2^{n_{i+1}} f(e_{i+1})$ only adds new terms to the dyadic expansion of $f(x) = \sum_{i=0}^{\infty} 2^{n_i} f(e_i)$, unless $f(e_{i+1}) = 0$. Since the dyadic expansion of $f(x) \in \mathbb{Z}$ is finite, for sufficiently large i, $2^{n_i} f(e_i)$ cannot add new terms to it, which means $f(e_i) = 0$ as wanted. This concludes the solution. ■

Exercise 8.7.29†. Prove that the Skolem-Mahler-Lech theorem holds over any field of characteristic zero.

Solution

The idea is to reduce again the problem to sequences of algebraic numbers. More precisely, let K be the field generated by the numbers involved in the formula for u_n and pick a transcendance basis $\alpha_1, \ldots, \alpha_k$ (see Exercise B.4.9†), i.e. a maximal subset of elements which are algebraically independent over $\mathbb{Q}$. The primitive element theorem then yields $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)(\alpha)$ for some α algebraic over $\mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ with minimal polynomial $\pi(\alpha_1, \ldots, \alpha_k) \in \mathbb{Z}(\alpha_1, \ldots, \alpha_k)[X]$. The key point is that we can "replace" $\alpha_1, \ldots, \alpha_n$ by any rational integers $a_1, \ldots, a_k$ and α by any root a of $\pi(a_1, \ldots, a_k)$, since an inequality in $\mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ reduces to an equality of algebraic functions in $\mathbb{Q}(X_1, \ldots, X_k)$ modulo $\pi(X_1, \ldots, X_k)$.

Given an $A = (a_1, \ldots, a_k)$ and a root a of $\pi(a_1, \ldots, a_k)$, we shall denote the image of u_n under the substitution $\alpha_i \to a_i, \alpha \to a$ by $u_n^{[A,a]}$ (note that this only makes sense if the denominator of $u_n^[A, a]$ is non-zero). Our main claim is the following: there is a T such that, for any $u_N \neq 0$, there is an A for which $u_N^{[A,a]}$ stays non-zero and such that the common difference of the arithmetic progressions of zeros of $(u_n^{[A,a]})_{n\in\mathbb{Z}}$ divides T. It is straightforward to see that this implies the wanted theorem: if $(u_{nT+m})_{n\in\mathbb{Z}}$ is not identically zero, then pick an $N \in T\mathbb{Z}+m$ such that $u_N \neq 0$ and an A as before to get that $(u_{nT+m}^{[A,a]})_{n\in\mathbb{Z}}$ has finitely many zeros and thus $(u_{nT+m})_{n\in Z}$ as well.

It remains to prove this claim. Write $u_n = \sum_i f_i(n) r_i^n$, where $r_i = R_i(\alpha_1, \ldots, \alpha_k, \alpha)$ and let $L_i(\alpha_1, \ldots, \alpha_k)$ and $C_i(\alpha_1, \ldots, \alpha_k)$ be the leading and constant coefficients of the minimal polynomial of r_i, as seen as a polynomial $\mathbb{Z}[\alpha_1, \ldots, \alpha_k][X]$. Pick $B = (b_1, \ldots, b_k) \in \mathbb{Z}^k$ such that $L_i(B)$ and $C_i(B)$ are non-zero: this implies that the r_i are too (when evaluated at b and any root of $\pi(B)$) since their norm is. Then pick a prime p which divides none of them. Finally, we choose $(a_1, \ldots, a_k)$ such that $a_i \equiv b_i \pmod{p}$ (in particular these coefficients are still non-zero) and $u_N^{[A,a]}$ is non-zero, where $A = (a_1, \ldots, a_k, a)$ and a is always an arbitrary root of $\pi(\alpha_1, \ldots, \alpha_k)$. This is possible since if $u_N^{[A,a]}$ were always zero, then the norm of u_N is zero on $(b_1 + p\mathbb{Z}) \times \ldots \times (b_k + p\mathbb{Z})$ so is zero by Exercise A.1.7* which implies that $u_N = 0$.

Now, we consider the norm $(v_n)_{n\in\mathbb{Z}}$ of $u_n^{[A,a]}$ to get a sequence of rational numbers. We will consider $(v_n)_{n\in\mathbb{Z}}$ as a union of p-adic analytic functions to deduce information about its zero, as usual. Hence, we shall abusively consider the $r_i^{[A,a]}$ as elements of a finite extension K_p of $\mathbb{Q}_p$. Note that they have zero p-adic valuation, i.e. are units in K_p. Indeed, note that $r = L_i(A) r_i^{[A,a]}$ is a root of a monic polynomial with constant coefficient $c = C_i(A) L_i(A)^{m-1}$: if

$R_i(A) = L_i(A)X^m + \ldots + C_i(A)$, then

$$R = L_i(A)^{m-1}R_i(A)(X/L_i(A)) = X^m + \ldots + C_i(A)L_i(A)^{m-1}.$$

Since c is not divisible by p, the norm of r cannot be smaller than 1 by the strong triangle inequality, otherwise the norm of $R(r)$ would be $|c|_p = 1$. Similarly, if it has norm greater than 1, the norm of this polynomial evaluated at r would be $|r^m|_p$. Since $p \nmid L_i(A)$, we conclude that $|r_i^{[A,a]}|_p = 1$ as wanted.

Finally, we wish to transform $(v_n)_{n\in\mathbb{Z}}$ into analytic function, i.e. have $|r_i^{t[A,a]} - 1|_p \leq 1/p \leq 1/p^{\frac{1}{p-1}}$. This t will be our bound for the common period of the arithmetic progressions of zeros. For this, consider the $r_i^{[A,a]}$ as algebraic numbers again and then as elements of $\overline{\mathbb{F}}_p$. Since their degree is bounded (by $[K : \mathbb{Q}]$), their order in $\overline{\mathbb{F}}_p$ is bounded too, say divides T. Then, we have $r_i^{T[A,a]} = 1$ in $\mathbb{F}_p$, so if we return to our p-adic $r_i^{[A,a]} \in \overline{\mathbb{Q}}_p$, the fundamental theorem of symmetric polynomials shows that we also have $r_i^{T[A,a]} \equiv 1 \pmod{p}$ there. We conclude that $(v_{nT+m})_{n\in\mathbb{Z}}$ is analytic over $\mathcal{O}_K$ for any $m \in [T]$, which finishes the proof of our claim. Indeed, note that T only depends on $[K : \mathbb{Q}]$ and p, which was fixed at the beginning of the proof, so does not depend on N (our chosen index such that $u_N \neq 0$). ■

Appendix A

Polynomials

A.1 Fields and Polynomials

Exercise A.1.1*. Let K be a field. Prove that $0_K a = 0_K$ for any $a \in K$.

Solution

$0_K a = (0_K + 0_K)a = 0_K a + 0_K a$ so $0_K a = 0_K$. ■

Exercise A.1.2*. Let $\dagger$ be a binary (taking two arguments) associative operation on a set M. Suppose that M has an identity. Prove that it is unique. Similarly, prove that, if an element $g \in M$ has an inverse, then it is unique.[1]

Solution

If e and e' are identities, then $e = ee' = e'$ so $e = e'$. Similarly, if b and b' are two inverses of a, then

$$b = (b'a)b = b'(ab) = b'$$

by associativity. ■

Exercise A.1.3*. Prove that multiplication of polynomials is associative and commutative.

Solution

Let $f = \sum_i a_X^i$, $g = \sum_j b_j X^j$ and $h = \sum_k c_k X^k$ be three polynomials. We have

$$fg = \sum_{i+j=\ell} a_i b_j X^\ell = \sum_{i+j=\ell} b_j a_i X^\ell = gf$$

since multiplication is commutative in a field and

$$(fg)h = \sum_{i+j+k=\ell} (a_i b_j) c_k X^\ell = \sum_{i+j+k=\ell} a_i (b_j c_k) X^\ell = f(gh)$$

since multiplication is associative in a field. (This also works for formal power series.) ■

[1] Such a structure is called a *monoid*.

Exercise A.1.4*. Prove that the gcd of 0 and 0 is 0.

Solution

Any polynomial divides 0 and 0 if and only if it divides 0. ■

Exercise A.1.5*. Prove that the Euclidean algorithm produces the gcd. Deduce that the gcd of two polynomials in $K[X]$ is also in $K[X]$. (As a consequence, the fundamental theorem of algebra Theorem A.1.1 implies that two polynomials with rational coefficients are coprime in $\mathbb{Q}[X]$ if and only if they have a common complex root.)

Solution

We need to prove that $\gcd(f, g) = \gcd(f - gq, g)$ for any f, g. This implies that the steps in the Euclidean algorithm preserve the gcd. Since $\deg f + \deg g$ decreases at each step, we eventually reach a situation where $f = 0$, and the gcd of 0 and g is clearly g. It is however very trivial that the gcd is conserved since

$$h \mid f, g \implies h \mid f - gq, g$$

and

$$h \mid f - gq, g \implies h \mid g, (f - gq) + gq = f.$$

■

Exercise A.1.6* (Bézout's Lemma)**.** Consider two polynomials $f, g \in K[X]$. Prove that there exist polynomials $u, v \in K[X]$ such that $uf + vg = \gcd(f, g)$.

Solution

Without loss of generality, suppose that $\deg g \leq \deg f$. We proceed by induction on $\deg g$. When this is 0, i.e. g is constant, we have $0 + \cdot f + 1/g \cdot g = 1$ as wanted. For the induction step, perform the Euclidean division of f by g: $f = gq + r$. Since $\deg r < \deg g$, by the induction hypothesis, there are u and v such that $uf + vr = 1$. Then,

$$\begin{aligned} 1 &= uf + vr \\ &= uf + v(f - gq) \\ &(u + v)f - (qv)g \end{aligned}$$

as wanted. ■

Remark A.1.1

One might, at first sight, think that this proof also works for non-coprime f, g (which is impossible for obvious reasons). However, we used the assumption that they were coprime when we said the base case was $\deg g = 1$: this is only true because the gcd is 1 so the Euclidean algorithm eventually yields a pair $\{1, f\}$ with $f \neq 0$, right before the pair $\{1, 0\}$. Otherwise, we would have to do the base case when $\deg g = -\infty$ which is clearly impossible.

Exercise A.1.7*. Let $f \in K[X_1, \ldots, X_n]$ be a polynomial in n variables and suppose $S_1, \ldots, S_n \subseteq K$ are subsets of K such that $|S_i| > \deg_{X_i} f$. If f vanishes on $S_1 \times \ldots \times S_n$, prove that $f = 0$. (This is the generalisation of Corollary A.1.1 to multivariate polynomials.)

Solution

We proceed by induction on n, the base case being the previous proposition. Fix $x_n \in S_n$. Then, the polynomial

$$g(x_n) = f(X_1, \ldots, X_{n-1}, x_n) \in K[X_1, \ldots, X_{n-1}]$$

vanishes on $S_1 \times \ldots \times S_{n-1}$ and has degree less than $|S_i|$ in X_i. Hence, $g(x_n) = 0$. Finally, g is a polynomial in X_n (with coefficients in the ring $K[X_1, \ldots, X_{n-1}]$) of degree less than $|S_n|$ vanishing on S_n, which implies that it's 0 by Corollary A.1.1. (Technically, to use Corollary A.1.1 we would need to work over a field, while we are only working over a ring: $K[X_1, \ldots, X_n]$. However, this is trivial to fix: this is an integral domain so we can embed it its field of fractions, i.e. work over the field $K(X_1, \ldots, X_n)$.) ■

Exercise A.1.8*. Prove that $(fg)' = f'g + gf'$ and $(f+g)' = f' + g'$ for any $f, g \in K[X]$. Show also that $(f^n)' = nf'f^{n-1}$ for any positive integer n, where f^k denotes the kth power and not the kth iterate. More generally, show that

$$\left(\prod_{i=1}^{n} f_i\right)' = \sum_{i=1}^{n} f_i' \prod_{j \neq i} f_j.$$

Solution

Write $f = \sum_i a_i X^i$ and $g = \sum_j b_j X^j$. We have

$$(f+g)' = \sum_k k(a_k + b_k)X^{k-1} = \sum_i i a_i X^{i-1} + \sum_j j b_j X^{j-1} = f' + g'$$

which shows additivity. For the multiplication, we have

$$(fg)' = \left(\sum_{i+j=k} a_i b_j X^k\right)' = \sum_{i+j=k} k a_i b_j X^{k-1}$$

and

$$f'g + g'f = \sum_{i+j=k} i a_i b_j X^{k-1} + \sum_{i+j=k} j a_i b_j) X^{k-1} = \sum_{i+j=k} (i a_i b_j + j a_i b_j) X^{k-1} = \sum_{i+j=k} k a_i b_j X^{k-1}$$

as wanted. Finally, the last point follows from the $(fg)' = f'g + g'f$ by induction:

$$\left(\prod_{i=1}^{n} f_i\right)' = f_n' \prod_{i=1}^{n-1} f_i + f_n \sum_{i=1}^{n-1} f_i' \prod_{n \neq j \neq i} f_j = \sum_{i=1}^{n} f_i' \prod_{j \neq i} f_j.$$

The previous point follows is the case $f_1 = \ldots = f_n = f$. ■

Exercise A.1.9*. Prove that every function $f : \mathbb{F}_p \to \mathbb{F}_p$ is polynomial.

Solution

This follows from Lagrange's interpolation theorem since $\mathbb{F}_p$ is finite. ■

Exercise A.1.10*. Prove that the derivative of a rational function does not depend on its form: i.e. $(f/g)' = ((hf)/(hg))'$ for any $f, g, h \in K[X]$ with $g, h \neq 0$.

Solution

We have

$$(f/g)' = \frac{f'g - g'f}{g(X)^2}$$

and

$$(hf/hg)' = \frac{(hf)'(hg) - (hg)'hf}{g^2}(hg(X))^2$$

■

A.2 Algebraic Structures and Morphisms

Exercise A.2.1*. Prove that 1_R and 0_R are unique, and that any element has a unique additive inverse and a unique multiplicative inverse if it is non-zero.

Solution

This follows from Exercise A.2.9*. ■

Exercise A.2.2*. Let R be a ring. Prove that $0_R a = a 0_R = 0_R$ for any $a \in R$.

Solution

The proof is the same as for Exercise A.1.1*. ■

Exercise A.2.3*. Prove that $\operatorname{char} R$ is the smallest $m \geq 0$ such that R contains a copy of $\mathbb{Z}/m\mathbb{Z}$

Solution

If R contains a copy of $\mathbb{Z}/m\mathbb{Z}$ with $m \geq 1$ then R has characteristic dividing m which shows the result when $m \neq 1$. If $m = 0$, then R has characteristic zero since $n \neq 0$ for all $n \in \mathbb{Z}$. The converse is clear: the copy $\mathbb{Z}/m\mathbb{Z}$ is $a \pmod m \mapsto \underbrace{1 + \ldots + 1}_{a \text{ times}}$ for $a \in \mathbb{N}$. (This is well-defined because the characteristics are the same.) ■

Exercise A.2.4*. Prove that the characteristic of a field is either 0 or a prime number p.

Solution

Let c denote the characteristic of a given field K. If $c \neq 0$, then $c \geq 2$ since the trivial ring is not a field. Suppose that $c = ab$. Then, in K, we have $ab = 0$ which means $a = 0$ or $b = 0$ since it's an integral domain. By minimality of the characteristic, this means that $c = a$ or $c = b$. ■

Exercise A.2.5. Let R be a finite integral domain (i.e. with finitely cardinality). Prove that it is a field.

Solution

Let $a \in R$ be non-zero. Consider the powers of a: $a, a^2, \ldots$. Since R is finite, there exist $i < j$ such that $a^i = a^j$, i.e. $a^i(a^{j-i} - 1) = 0$. Since $a \neq 0$ and R is an integral domain, we get $a^{j-i} - 1 = 0$, so that a^{j-i-1} is the inverse of a. ■

Exercise A.2.6*. Prove that a subring of a field is an integral domain.

Solution

If $ab = 0$ and $a \neq 0$ then $b = a^{-1}ab = 0$. ■

Exercise A.2.7. What goes wrong if you try to construct the field of fractions of a commutative ring which isn't a domain?

Solution

Clearly, if $uv = 0$, there is something wrong with $1/u$. Indeed, we would have $1/u = v/(uv) = v/0$ which doesn't make sense (even formally: $1 \cdot 0$ is not equal toThe problem is that $a/b = c/d$ if $ad = bc$ is not an equivalence relation anymore: we can have $a/b = c/d$ and $c/d = x/y$ but $a/b \neq x/y$. Indeed, this is how the usual proof of transitivity goes: we have $ad = bc$ and $cy = dx$ so

$$ady = bcy = bdx$$

which doesn't necessarily means $ay = bx$ since d might not be invertible. Here is a concrete counterexample, if $dd' = 0$, then $1/d = d'/0$ and $d'/0 = 1/0$ but $1/d \neq 1/0$. ■

Exercise A.2.8*. Let R be an integral domain. Prove that $R[X]$ is also one.

Solution

Suppose that f and g are non-zero elements of $R[X]$ with respective leading coefficients a and b. Then, the leading coefficient of fg is ab since $ab \neq 0$ as R is an integral domain, which implies in particular that fg is non-zero. ■

Exercise A.2.9*. Prove that the identity e of a group G is unique, and that any $a \in G$ has a unique inverse. Moreover, prove that $(xy)^{-1} = y^{-1}x^{-1}$.

Solution

If e and e' are two identities then $e = ee' = e'$. The inverse of xy is $y^{-1}x^{-1}$ since $(xy)(y^{-1}x^{-1}) = xx^{-1} = e$. ■

Exercise A.2.10*. Check that $(\mathfrak{S}_n, \circ)$ is a group.

Solution

Since permutations are bijective, they are invertible. Moreover, the identity permutation is the identity of the group. Finally, it is clear that the operation is associative since composition is. ■

Exercise A.2.11*. Prove that a morphism of groups from $(G, \dagger)$ to $(H, \star)$ maps the identity of G to the identity of H.

Solution

Let φ be such a morphism and e_G, e_H be the identities of G and H respectively. We have

$$\varphi(e_G) = \varphi(e_G \dagger e_G) = \varphi(e_G) \star \varphi(e_G)$$

so $\varphi(e_G) = e_H$ as wanted (by starring both sides by its inverse).) ■

Exercise A.2.12*. Prove that the kernel of a morphism (of rings or groups) is closed under addition.

Solution

If $\varphi(a) = 0$ and $\varphi(b) = 0$ then $\varphi(a + b) = \varphi(a) + \varphi(b) = 0$. ■

Exercise A.2.13*. Prove that a morphism of groups is injective iff its kernel is trivial, i.e. consists of only the identity.

Solution

If it is injective, then the kernel is trivial. Otherwise, suppose that $\varphi(a) = \varphi(b)$ and $a \neq b$. Then $\varphi(ab^{-1}) = e$ so the kernel is non-trivial. ■

A.3 Exercises

Derivatives

Exercise A.3.1†. Let $f, g \in K[X]$ be two polynomials. Prove that the derivative of $f \circ g$ is $g' \cdot f' \circ g$.

Solution

Write $f = \sum_i a_i X^i$. Then, $(f \circ g)' = \sum_i a_i (g^i)' = \sum_i i a_i g' g^{i-1} = g' f' \circ g$. ■

Exercise A.3.2†. Let $f \in K[X]$ be a non-constant polynomial. Prove that there are a finite number of $g, h \in K[X]$ such that $g \circ h = f$, up to affine translation, meaning $(g, h) \equiv \left(g(aX + b), \frac{h-b}{a}\right)$.

Solution

By composing with an affine transformation, we may assume that $h(0) = 0$ and that h is monic. If we differentiate the equation $g \circ h = f$, we get $h' \mid f'$. There is a finite number of such h' since we fixed its leading coefficient and f is non-constant. Since $h(0) = 0$, there is also a finite number of h. Since g is uniquely determined from h, we are done. ■

Exercise A.3.4† (USA TST 2017)**.** Let $f, g \in \mathbb{R}[X]$ be non-constant coprime polynomials. Prove that there are at most three real numbers λ such that $f + \lambda g$ is the square of a polynomial.

Solution

The key point is that, if $f + \lambda g$ is a square h^2, then h divides $f + \lambda g$ as well as $f' + \lambda' g = 2hh'$ so must divide

$$g'(f + \lambda g) - g(f' + \lambda g') = fg' - g'f$$

which is independent of f. (Note that this is the determinant of $\begin{bmatrix} f & g \\ f' & g' \end{bmatrix}$ which was also used in Exercise A.3.22†. This explains why it doesn't depend on λ.)

Also, if $f + \lambda g = r^2$ and $f + \mu g = s^2$ for $\mu \neq \lambda$, r and s are coprime since they two linearly independent linear conmbinations of f and g, and we know f and g are coprime. Thus, if $f + \lambda_i g = h_i^2$ for $i = 1, \ldots, n$, we get $h_1 \cdot \ldots \cdot h_n \mid f'g - g'f$ as they all divide it and are coprime. However, when n is large (i.e. greater than 3), the degree of the LHS will be too big so this will be impossible. Indeed, from $f + \lambda_i g = h_i^2$, we deduce that $\deg h_i$ is $\max(\deg f, \deg g)/2$, except for possibly one value of λ and $\deg f = \deg g$. In the first case we are done since

$$4 \max(\deg f, \deg g)/2 > \deg f + \deg g - 1,$$

so we must have $f'g = g'f$ which is impossible as this would mean $f \mid f'$ since f and g are coprime. For the second case, if $\deg(f + \lambda g)$ is small, note that we can replace f by $f + \lambda g$ (and replace the λ_i by other real numbers μ_i) and this case is now impossible since $\deg(f + \lambda g) < \deg g = \deg f$. Note that this doesn't change the value of $f'g - g'f$ because we constructed it to be

$$g'(f + \lambda g) - g(f' + \lambda g') = fg' - g'f.$$

■

Exercise A.3.6† (Discrete Derivative)**.** Let $f \in K[X]$ be a polynomial of degree n and leading coefficient a. Define its *discrete derivative* as $\Delta f := f(X + 1) - f(X)$. Prove that, for any $g \in K[X]$ $\Delta f = \Delta g$ if and only if $f - g$ is constant, and that Δf is a polynomial of degree $n - 1$ with leading coefficient an where a is the leading coefficient of f. Deduce the minimal degree of a monic polynomial $f \in \mathbb{Z}[X]$ identically zero modulo m, for a given integer $m \geq 1$.

Solution

The discrete derivative operator is a morphism (from the space of polynomials of degree at most n to the space of polynomials of degree at most $n - 1$), thus it suffices to show that its kernel consists only of constants. This follows from the second part, that Δf is a polynomial of degree $n - 1$. For this, simply write $f = \sum_{i=0}^{n} a_i X^i$. Then,

$$\Delta f = \sum_{i=0}^{n} a_i((X + 1)^i - X^i) = \sum_{i=0}^{n} a_i \sum_{j=0}^{i-1} \binom{i}{j} X^j$$

and the term in X^{n-1} is reached only once for $i = n$, $j = n-1$, with coefficient $a_n\binom{n}{n-1} = an$. Finally, if a polynomial is identically zero modulo m and monic of degree n, $\Delta^n f = n!$ since the degree decreases by one every time we apply Δ, while the leading coefficient gets multiplied by the degree. Thus, $m \mid n!$. Conversely, if n is the minimal integer such that $m \mid n!$, the polynomial

$$f = n!\binom{X}{n} = X(X-1)\cdot\ldots\cdot(X-(n-1))$$

works. ■

Exercise A.3.7†. Let $f : R \to R$ be a function. Define its discrete derivative Δf as $x \mapsto f(x+1) - f(x)$. Prove that, for any integer $n \geq 0$,

$$\Delta^n f(x) = \sum_{k=0}^{n} (-1)^{n-k}\binom{n}{k} f(x+k).$$

Solution

We proceed by induction on n. For $n = 0$ it is of course trivial. If it's true for n, then

$$\begin{aligned}
\Delta^{n+1} f(x) &= \Delta(\Delta^n f)(x) \\
&= \sum_{k=0}^{n} (-1)^{n-k}\binom{n}{k}(f(x+k+1) - f(x+k)) \\
&= \sum_{k=0}^{n+1} ((-1)^{n+1-k}\left(\binom{n}{k+1} - \binom{n}{k}\right) f(x+k) \\
&= \sum_{k=0}^{n+1} (-1)^{n+1-k}\left(\binom{n}{k+1} + \binom{n}{k}\right) f(x+k) \\
&= \sum_{k=0}^{n+1} (-1)^{n+1-k}\binom{n+1}{k} f(x+k).
\end{aligned}$$

■

Exercise A.3.8†. Let $m \geq 0$ be an integer. Prove that there is a polynomial $f_m \in \mathbb{Q}[X]$ of degree $m+1$ such that

$$\sum_{k=0}^{n} k^m = f_m(n)$$

for any $n \in \mathbb{N}$.

Solution

We proceed by induction on m by noting that $\sum_{k=0}^{n} k^0 = n+1 := f_0(n)$ and that

$$\begin{aligned}(n+1)^{m+1} &= \sum_{k=0}^{n} (k+1)^{m+1} - k^{m+1} \\ &= \sum_{i=0}^{m} \binom{m+1}{i} \sum_{k=0}^{n} k^i \\ &= (m+1)\left(\sum_{k=0}^{n} k^m\right) + \sum_{i=0}^{m-1} \binom{m+1}{i} f_i(n)\end{aligned}$$

so that

$$f_m(n) = \sum_{k=0}^{n} k^m = \frac{(n+1)^{m+1}}{m+1} - \sum_{i=0}^{m-1} \binom{m+1}{i} \frac{f_i(n)}{m+1}$$

is a polynomial as well. Note also that its leading coefficient is $frac1m+1$. ■

Roots of Unity

Exercise A.3.9† (Root of Unity Filter)**.** Let $f = \sum_i a_i X^i \in K[X]$ be a polynomial, and suppose that $\omega_1, \ldots, \omega_n \in K$ are distinct nth roots of unity. Prove that

$$\frac{f(\omega_1) + \ldots + f(\omega_n)}{n} = \sum_{n|k} a_k.$$

Deduce that, if $K = \mathbb{C}$,

$$\max_{|z|=1} |f(z)| \geq |f(0)|.$$

(You may assume the existence of a *primitive* nth root of unity ω, meaning that $\omega^k \neq 1$ for all $k < n$, or, equivalently, every nth root of unity are powers of ω. This will be proven in Chapter 3.)

Solution

Let ω be a primitive nth root of unity. Note that, if $n \nmid m$,

$$\sum_{k=1}^{n} \omega_k^m = \sum_{k=0}^{n-1} \omega^{km} = \frac{\omega^{mn} - 1}{\omega^m - 1}$$

since the numerator is zero and the denominator isn't. When $n \mid m$, the sum is simply $\sum_{k=1}^{n} 1 = n$. Thus, we have proven the result for monomials, and the general case follows by taking linear combinations (if it's true for f and g it's also true for af and $f+g$).

For $n > \deg f$ we have $\frac{f(\omega_1)+\ldots+f(\omega_n)}{n} = f(0)$ so

$$\max_k |f(\omega_k)| \geq \left|\frac{f(\omega_1) + \ldots + f(\omega_n)}{n}\right| = |f(0)|$$

by the triangular inequality. ■

Exercise A.3.10†**.** Let $f = \sum_i a_i X^i \in \mathbb{R}[X]$ be a polynomial and $\omega_1, \ldots, \omega_n \in \mathbb{C}$ be distinct nth roots of unity with $n > \deg f$. Prove that

$$\frac{|f(\omega_1)|^2 + \ldots + |f(\omega_n)|^2}{n} = \sum_i a_i^2.$$

Denote by $S(f)$ the sum of the squares of the coefficients of f. Deduce that $S(fg) = S(fX^{\deg g}g(1/X))$ for all $f, g \in \mathbb{R}[X]$. ($X^{\deg g}g(1/X)$ is the polynomial obtained by reversing the coefficients of g.)

Solution

Note that

$$|f(\omega)|^2 = f(\omega)\overline{f(\omega)} = f(\omega)f(\overline{\omega}) = f(\omega)f(\omega^{-1})$$

for any ω on the unit circle, since $\omega\overline{\omega} = |\omega|^2 = 1$ for these ω. Thus,

$$\begin{aligned}\frac{1}{n}\sum_{k=1}^{n}|f(\omega_k)|^2 &= \frac{1}{n}\sum_{k=1}^{n}f(\omega_k)f(\omega_k^{-1})\\ &= \frac{1}{n}\sum_{k=1}^{n}\sum_{i}a_i\omega_k^i\sum_{j}a_j\omega_k^j\\ &= \frac{1}{n}\sum_{k=1}^{n}\sum_{i,j}a_ia_j\omega_k^{i-j}\\ &= \sum_{i}a_i^2\end{aligned}$$

by Exercise A.3.9† since $n \mid i-j$ iff $i = j$ for $i, j \in [\![0, \deg f]\!]$, as $n > \deg f$. For the second part, note that $|f(\omega)g(\omega)| = f(\omega)g(1/\omega)|$ for any ω on the unit circle. ■

Exercise A.3.11†. Let k be an integer. Prove that $\sum_{a\in\mathbb{F}_p}a^k$ is 0 if $p-1 \nmid k$ and -1 otherwise. Deduce that any non-constant polynomial $f \in \mathbb{F}_p[X]$ satisfying $f(a) \in \{0, 1\}$ for all $a \in \mathbb{F}_p$ must have degree at least $p-1$.

Solution

The first part is Exercise A.3.9† for $K = \mathbb{F}_p$, since non-zero elements of $\mathbb{F}_p$ are $(p-1)$th roots of unity by Fermat's little theorem. For the second, let m be the number of times $f(a) = 1$. Then, $\sum_{a\in\mathbb{F}_p}f(a) \equiv m \pmod p$. If $\deg f < p-1$, this sum is zero modulo p by the first part which is impossible since $m \in [1, p-1]$ (if f is constant over $\mathbb{F}_p$ and has degree less than p, $f - f(0)$ has more roots than its degree so is zero). ■

Exercise A.3.12†. Let $p \neq 3$ be a prime number. Suppose that a and b are integers such that $p \mid a^2 + ab + b^2$. Prove that $(a+b)^p \equiv a^p + b^p \pmod{p^3}$.

Solution

Note that we can suppose that $a, b \not\equiv 0 \pmod p$ and reduce the problem to the case where $b = 1$ by considering $x \equiv ab^{-1} \pmod p$ so that $x^2 + x + 1 \equiv 0$. In particular, x has order 3 modulo p since $x^3 - 1 \equiv (x-1)(x^2+x+1)$ but $x \not\equiv 1$ since $p \neq 3$. This implies that $p \equiv 1 \pmod 3$ by Exercise 3.3.4*. (This is a special case of Theorem 3.3.1.)

The key point is that, since $p \equiv 1 \pmod 3$, we have $(X^2+X+1)^2 \mid (X+1)^p - X^p - 1 := f$. Since $(X+1)^p - X^p - 1 \equiv 0 \pmod p$ by the binomial expansion (see **??** for more details), this means that $(X^2+X+1)^2$ divides the polynomial $\frac{f}{p}$ in $\mathbb{Q}[X]$, and hence in $\mathbb{Z}[X]$ too since it is monic. We conclude that $p(X^2+X+1)^2 \mid f$ in $\mathbb{Z}[X]$ so that

$$v_p(f(x)) \geq v_p(p(x^2+x+1)) \geq 3$$

as wanted. First, note that X^2+X+1 is irreducible over $\mathbb{Q}[X]$ and that its roots are primitive third root of unity ω, since $X^3-1=(X^2+X+1)(X-1)$. Hence, we wish to show that $f(\omega)=0$, $f'(\omega)=0$ and $f''(\omega)=0$. We have

$$f(\omega)=(\omega+1)^p-\omega^p-1=(-\omega^2)^p-\omega^p-1=0$$

since ω^p is also a primitive third root of unity. Similarly,

$$f'(\omega)=p(\omega+1)^{p-1}-p\omega^{p-1}=p\omega^{2(p-1)}-p\omega^{p-1}=p-p=0$$

since $3 \mid p-1$ and $p-1$ is even so we are done. ■

Remark A.3.1

It has been conjectured that the polynomials $\frac{(X+1)^n-X^n-1}{(X^2+X+1)^\varepsilon}$ where $\varepsilon=v_{X^2+X+1}((X+1)^n-X^n-1)$ is 2 if $n\equiv 1 \pmod 3$, 1 if $n\equiv -1 \pmod 3$ and 0 if $n\equiv 0 \pmod 3$ are irreducible. These are called the *Cauchy-Mirimanoff polynomials*.

Group Theory

Exercise A.3.14†. Given a group G and a *normal subgroup* $H\subseteq G$, i.e. a subgroup such that

$$x+H-x=H$$

for any $x\in G$,[2] we define the *quotient* G/H of G by H as G *modulo* H[3], i.e. we say $x\equiv y \pmod H$ if $x-y\in H$.[4] Prove that this indeed a group, and that $|G/H|=|G|/|H|$ for any such G,H.

Solution

G/H is clearly closed under the operation of G and has inverses and an identity. We need however to check that the operation is well defined: $x\equiv y \pmod H$ and $z\in G$, $x+z\equiv y+z \pmod H$ and $z+x\equiv z+y \pmod H$. For the former, note that $(x+z)-(y+z)=x-y\in H$ since the inverse of $y+z$ is $-z-x$, and for the latter note that $(z+x)-(z+y)=z+(x-y)-z$ is in H **because** H **is normal in** G. The second part is obvious: any $x\in G$ is equal to exactly $|H|$ elements modulo H: $x+y$ for $y\in H$. ■

Exercise A.3.15† (Isomorphism Theorems)**.** Prove the following first, second, and third isomorphism theorems.

1. Let $\varphi: A\to B$ be a morphism of groups. Then, $A/\ker\varphi\simeq \operatorname{im}\varphi$. (In particular, $\ker\varphi$ is normal in A and $|\operatorname{im}\varphi|\cdot|\ker\varphi|=|A|$.)

2. Let H be a subgroup of a group G, and N a normal subgroup of G. Then, $H/H\cap N\simeq HN/N$. (In particular, you need to show that this makes sense: HN is a group and $H\cap N$ is normal in H.)

3. Let $N\subseteq H$ be normal subgroups of a group G. Then, $(G/N)/(H/N)\simeq G/H$.

[2] In particular, when G is abelian, any subgroup is normal.

[3] This is where the notation $\mathbb{Z}/n\mathbb{Z}$ comes from! In fact this shows that, in reality, we should say "modulo $n\mathbb{Z}$" instead of "modulo n".

[4] A better formalism is to say that G/H is the set of cosets $g+H$ for $g\in G$. In fact, we will almost always use this definition in the solutions of exercises (since this is the only place where this will appear), but we introduced it that way to make the analogy with $\mathbb{Z}/n\mathbb{Z}$ clearer.

Solution

1. Note that $\ker\varphi$ is normal in A. Indeed, if $\varphi(x) = 1$, then $\varphi(yxy^{-1}) = \varphi(y)\varphi(x)\varphi(y)^{-1} = 1$ too. Second, note that every element in the image of φ has exactly one one preimage in $A/\ker\varphi$: indeed, if $\varphi(x) = \varphi(y)$, then $xy^{-1} \in \ker\varphi$ so they are equal modulo $\ker\varphi$. This shows that it is an isomorphism (it is clearly surjective, and we have shown it was injective too).

2. Note that $H \cap N$ is normal in H since N is so $hH \cap Nh^{-1} \subseteq N$ but this is also in H when $h \in H$ so must be equal to $H \cap N$. Note also that HN is indeed a group since, if $gm, hn \in HN$, then $mh = h\ell$ for some $\ell \in N$ as N is normal, so

$$gmhn = gh\ell n \in HN.$$

   Similarly, $gm = kg$ for some $k \in G$ so $(gm)^{-1} = g^{-1}k^{-1} \in HN$. Now, consider the natural map from H to HN/N, sending h to hN. Its kernel consists of the h such that $hN = N$, i.e. $h \in N$. Hence, its kernel is $H \cap N$ so we get $H/H \cap N \simeq HN/N$ by the first isomorphism theorem.

3. Consider the surjective map $G/N \to G/H$ which sends gN to gH. It is well defined since $N \subseteq H$. gN is in the kernel if $gH = H$, i.e. $g \in H$. Hence, the kernel consists of hN for $h \in H$, i.e. H/N. We conclude from the first isomorphism theorem that $G/H \simeq (G/N)/(H/N)$ as wanted.

■

Exercise A.3.16†. Let G be a finite group, $\varphi : G \to \mathbb{C}^\times$ be a non-trivial group morphism (i.e. not the constant function 1), where $(\mathbb{C}^\times, \cdot)$ is the group of non-zero complex numbers under multiplication. Prove that $\sum_{g\in G} \varphi(g) = 0$.

Solution

Note that, for any $h \in G$, $g \mapsto hg$ is a bijection so

$$\sum_{g\in G} \varphi(g) = \sum_{g\in G} \varphi(hg) = \varphi(h) \sum_{g\in G} \varphi(g)$$

which means that $\sum_{g\in G} \varphi(g) = 0$ by picking an h such that $\varphi(h) \neq 1$. ■

Remark A.3.2

Alternatively, this can be done as follows: the image of φ is a subgroup of the group of $|G|$th roots of unity by Lagrange, so must be the group of nth roots for some n, greater than 1 by assumption (this is just the fact that subgroups of cyclic groups are also cyclic). Let $\omega = \exp(2i\pi/n)$ be a primitive nth root of unity. Hence, we have

$$\sum_{x\in \operatorname{im}\varphi} x = \sum_{k=0}^{n-1} \omega^k = \frac{\omega^n - 1}{\omega - 1} = 0$$

since the numerator is zero while the denominator isn't, as $n > 1$. To conclude, by the first

isomorphism theorem from Exercise A.3.15†, we have

$$\sum_{g\in G}\varphi(g)=\frac{|G|}{\ker\varphi}\sum_{x\in\operatorname{im}\varphi}x=0.$$

Exercise A.3.17† (Lagrange's Theorem)**.** Let G be a group of cardinality n (also called the *order* of G). Prove that $g^n=e$ for all $g\in G$. In other words, the order of an element divides the order of the group. More generally, prove that the order of a subgroup divides the order of the group.

Solution

See Theorem 2.5.1 and Exercise 6.3.15*. ■

Exercise A.3.18† (5/8 Theorem)**.** Let G be a non-commutative finite group. Prove that the probability

$$p(G)=\frac{|\{(x,y)\in G^2\mid xy=yx\}|}{|G|^2}$$

that two elements commute is at most 5/8.

Solution

Denote by Z the *center* of the group, i.e. the set of elements which commute with every other one. For a given $x\in G$, denote also by $C(x)$ the *centraliser* of x, i.e. the set of y such that x and y commute. The wanted probability is $\sum_{x\in G}\frac{|C(x)|}{|G|^2}$. Note that $C(x)$ are subgroups of G (and hence Z is too): if $xy=yx$ and $xz=zx$ then

$$xyz=yxz=yzx.$$

First, let's see how big the center can be. It's a subgroup of G, so its cardinality divides $|G|$ by Lagrange's theorem Exercise A.3.17†. It can't be $|G|$ since G is non-abelian, it can't be $\frac{|G|}{2}$ since G/Z is then isomorphic to $\mathbb{Z}/2\mathbb{Z}$ so is generated by one element and hence G is generated by Z and one additional element which means that it's commutative:

$$a^mxa^ny=a^{m+n}xy=a^nya^mx$$

for $x,y\in Z$. For the same reason, it can't be $\frac{|G|}{3}$ since G/Z still has prime order so must be generated by one element by Lagrange's theorem. Thus, $\frac{|Z|}{|G|}\leq\frac{1}{4}$.

Now, if $x\notin Z$, $C(x)$ is a subgroup of G distinct from it so has cardinality at most $\frac{|G|}{2}$. To

conclude,

$$\begin{aligned}\frac{|\{(x,y)\in G^2 \mid xy=yx\}|}{|G|^2} &= \sum_{x\in G}\frac{|C(x)|}{|G|^2}\\ &= \sum_{x\in Z}\frac{|G|}{|G|^2}+\sum_{x\notin Z}\frac{|C(x)|}{|G|^2}\\ &\le \frac{|Z|}{|G|}+(|G|-|Z|)\cdot\frac{|G|/2}{|G|^2}\\ &= \frac{|Z|}{|G|}+\frac{1}{2}-\frac{|Z|}{2|G|}\\ &= \frac{|Z|}{2|G|}+\frac{1}{2}\\ &\le \frac{1}{8}+\frac{1}{2}\\ &= \frac{5}{8}.\end{aligned}$$

■

Remark A.3.3

One can check that the bound 5/8 is achieved by the quaternion group Q_8 consisting of the elements $e, b, b^2, b^3, a, ab, ab^2, ab^3$ under the presentation $a^4 = b^4 = e$, $a^2 = b^2$, and $ba = ab^3$.

Exercise A.3.19† (Fundamental Theorem of Finitely Generated Abelian Groups)**.** Let G be an abelian group which is finitely generated, i.e., if we write its operation as $+$, there are $g_1, \ldots, g_k \in G$ such that any $g \in G$ can be represented as $n_1g_1 + \ldots + n_kg_k$ for integers $n_i \in \mathbb{Z}$. Prove that there is a unique integer $n \ge 0$ (called the *rank* of the group) and a unique sequence of positive integers $d_1 \mid \ldots \mid d_m$ such that

$$(G,+) \simeq (\mathbb{Z}^n \times \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z}, +).$$

Solution

This problem has two parts: proving that a finite abelian group is isomorphic to a product of cyclic groups in the wanted way, and proving that the *torsion* T of a finitely generated abelian group, i.e. the set of elements with finite order (which is a subgroup here since G is abelian) is finite and that $G \simeq \mathbb{Z}^n \times T$ for some n.

For the first part, pick an element $h \in G$ of maximal order m. We claim that the order of any element $g \in G$ divides m. (We know that this must be true by the statement: this m is our d_k. Note however that this is false for non-abelian groups.) Indeed, suppose that $x, y \in G$ have order a, b. We will construct an element of order $\mathrm{lcm}(a, b)$. First suppose that a and b are coprime. Then, $a(x + y) = ax$ has order b since $\gcd(a, b) = 1$, and similarly $b(x + y) = by$ has order a. Thus, the order of $x + y$ is divisible by a and b, and hence by ab. Conversely, it clearly divides ab so must be exactly ab.

Now, if a and b are not necessarily coprime, let $a' = \prod_{v_p(a)\ge v_p(b)} p^{v_p(b)}$ and $b' = \prod_{v_p(a)<v_p(b)} p^{v_p(b)}$ so that a', b' are coprime and have product $\mathrm{lcm}(a, b)$. The elements $(a/a')x$ and $(b/b')y$ have respective orders a' and b' so we are done by the previous step since a' and b' are coprime.

Now, let $H = \langle h\rangle$ be the subgroup generated by g, i.e. $\{0, g, \ldots, (m-1)g\}$. This is isomorphic to $\mathbb{Z}/m\mathbb{Z}$. We claim that

$$G \simeq H \times G/H.$$

Continuing in this fashion with G/H (which has a strictly smaller cardinality unless G is already trivial) yields the wanted decomposition, since we have shown that the d_i are divisible by the

previous one (m is divisible by the order of any element). To prve that $G \simeq H \times G/H$, we will find a morphism φ from G to H which is the identity H. Indeed, $g \mapsto (\varphi(g), g \pmod H)$ will then be the wanted isomorphism between G and $H \times G/H$: if $\varphi(g) = \varphi(g')$ and $g \equiv g' \pmod H$, then $\varphi(g - g') = g - g'$ since it is the identity on H so we must have $g = g'$. Thus, our morphism is injective and hence bijective since $|G| = |H| \cdot |G/H|$.

We proceed by induction on the minimal number of elements needed to generate G from H. When $H = G$ it is trivial. Now, suppose φ is a morphism from $G' \subseteq G$ to G and let $g \in G \setminus G'$. We will extend φ to $\langle G', g\rangle$, the subgroup generated by G' and g as desired. Let n be the order of y in G/G', i.e. the smalles k such that $ny \in G'$. Then, $ky \in G \iff n \mid k$. Thus, $\varphi(g' + kg) := \varphi(g') + k\varphi(g)$ is well-defined as long as $\varphi(g)$ is such that

$$\varphi(ng) = n\varphi(g).$$

Now, note that n divides the order of g which divides $m = |H|$. Hence, it is always possible to find such a $\varphi(g)$: if $\varphi(ng) = kh$, since $mg = 0$, we have $(mk/n)h = 0$, i.e. $n \mid k$ which means that $\varphi(g) = (k/n)h$ works. Note also that this reasoning shows that the decomposition is unique too.

Now, we prove that torsion-free finitely generated abelian groups are isomorphic to $\mathbb{Z}^n$ for a unique n. But first, we show how the problem follows from these two special cases. Note that G/T is torsion-free: if $x \pmod T$ has finite order, then $nx \in T$ for some n so x has finite order, i.e. $x \in T$. Pick a basis $\alpha_1 \pmod T, \ldots, \alpha_n \pmod T$. Now, we claim that

$$G \simeq T \times (\alpha_1\mathbb{Z} + \ldots + \alpha_n\mathbb{Z}) \simeq T \times \mathbb{Z}^n$$

as wanted. This follows from the simple isomorphism $(x, y) \mapsto x + y$. This is surjective by definition, since $\alpha_1\mathbb{Z} + \ldots + \alpha_n\mathbb{Z}$ is a system of representatives of G/T. For the injectivity, note that, if $x + y = x' + y'$, then $y - y' = x - x' \in T$ so $y = y'$ and thus $x = x'$ since $\alpha_1\mathbb{Z} + \ldots + \alpha_n\mathbb{Z} \simeq G/T$ has trivial torsion. There is one last thing we need to show however: that T is finite. Pick an isomorphism $\varphi : G \mapsto T \times \mathbb{Z}^n$. Then, the first coordinates of the image of a generating family of elements of G generate T. Since they all have finite order, they generate a finite number of elements as wanted.

Hence, we only need to prove that if G has trivial torsion, it is isomorphic to $\mathbb{Z}^n$ for some n. Note that this n is unique: if we had an isomorphism from $\mathbb{Z}^m$ to $\mathbb{Z}^n$, we would have one from $(\mathbb{Z}/2\mathbb{Z})^m \to (\mathbb{Z}/2\mathbb{Z})^n$ by reducing it modulo 2, and this forces $m = n$. Pick a generating set of minimal cardinality $\alpha_1, \ldots, \alpha_n$. We wish to prove that it is linearly independent. Suppose that it is not the case, and let $N \neq 0$ be the minimum value of the absolute values of the coefficients of a non-trivial linear combination which is zero. In fact, we shall also pick the generating set to minimise N. The contradiction will then come from a construction of another generating set with zero linear combination with smaller coefficients.

Suppose that $k_1\alpha_1 + \ldots + k_n\alpha_n = 0$ and $N = |k_1| + \ldots + |k_n|$. Suppose without loss of generality that $0 < |k_1| < |k_2|$. Say we replace the family $\alpha_1, \ldots, \alpha_n$ by $\alpha_1 \pm \alpha_2, \alpha_2, \ldots, \alpha_n$. Then, $k_1\alpha_1 + \ldots + k_n\alpha_n = 0$ becomes

$$k_1(\alpha_1 \pm \alpha_2) + (k_2 \mp k_1)\alpha_2 + k_3\alpha_3 \ldots + k_n\alpha_n = 0.$$

By picking the ± 1 sign appropriately, we ensure that $|k_2 \mp k_1| < |k_2|$ thus leading to a smaller value of N, which is a contradiction. We are done. ■

Exercise A.3.20† (Burnside's Lemma)**.** Let G be a finite group, S a finite set, and $\cdot$ a *group action* of G on S, meaning a map $\cdot : G \times S \to S$ such that $e \cdot s = s$ and $(gh) \cdot s = g \cdot (h \cdot s)$ for any $g, h \in G$ and $s \in S$. Given a $g \in G$, denote by $\mathrm{Fix}(g)$ the set of elements of s fixed by g. Prove that

$$|S/G| = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}(g),$$

where $|S/G|$ denotes the number of (disjoint) orbits $\mathcal{O}_i = Gs_i$. Deduce the number of necklaces that have p beads which can be of a colours, where p is a prime number and two necklaces are considered to be the same up to rotation.

Solution

Consider the sum $\sum_{g\in G} |\operatorname{Fix}(g)|$. This is equal to the number of pairs (g, s) such that $gs = s$. Hence, this is also equal to $\sum_{s\in S} |\operatorname{Stab}(s)|$, where $\operatorname{Stab}(s)$ denotes the elements of G fixing s. Now consider the orbit Gs of s. We claim that $|Gs| = |G/\operatorname{Stab}(s)| = |G|/|\operatorname{Stab}(s)|$. Indeed, the map from the left-cosets $G/\operatorname{Stab}(s)$ to Gs sending $g\operatorname{Stab}(s)$ to gs is clearly a bijection: if $gs = hs$ then $h^{-1}g \in \operatorname{Stab}(s)$ so $g\operatorname{Stab}(s) = h\operatorname{Stab}(s)$. Hence,

$$\begin{aligned}\sum_{g\in G} |\operatorname{Fix}(g)| &= |G| \sum_{s\in S} \frac{1}{|Gs|} \\ &= \sum_{\mathcal{O}\in S/G} \sum_{x\in\mathcal{O}} \frac{1}{|\mathcal{O}|} \\ &= \sum_{\mathcal{O}\in S/G} 1 \\ &= |S/G|\end{aligned}$$

as desired.

For the second part, consider the cyclic group $\mathbb{Z}/p\mathbb{Z}$ acting on the sets of words (necklaces) in an alphabet (the set of colours) of size a. Why did we choose $\mathbb{Z}/p\mathbb{Z}$? Because we consider the necklaces up to rotation. The action of $g \in \mathbb{Z}/p\mathbb{Z}$ is of course a rotation of g beads, say to the right. Then, there is one element fixing all words: 0, and all the other ones only fix words with all letters equal, i.e. monochromatic necklaces. Indeed, if $0 \neq g \in \mathbb{Z}/p\mathbb{Z}$ fixes a necklace, then so does $\mathbb{Z}/p\mathbb{Z} = g\mathbb{Z}/p\mathbb{Z}$ which means that the necklace is invariant under all rotations, i.e. monochromatic. Hence, the number of necklaces is

$$\frac{a^p + (p-1)a}{p}$$

by Burnside's lemma. Notice that this also proves Fermat's little theorem.. ■

Miscellaneous

Exercise A.3.21† (China TST 2009)**.** Prove that there exists a real number $c > 0$ such that, for any prime number p, there are at most $cp^{2/3}$ positive integers n satisfying $n! \equiv -1 \pmod p$.

Solution

We shall prove that any set S such that $a! \equiv b! \not\equiv 0 \pmod p$ has cardinality at most $2p^{2/3}$. Consider the polynomial following polynomial

$$f_m = (X+1)\cdot\ldots\cdot(X+m) - 1 \in \mathbb{F}_p[X].$$

Since $\mathbb{F}_p$ is a field, f_m has at most m roots in $\mathbb{F}_p$. Thus, there are at most m integers n such that $n! \equiv (m+n)!$, since this is equivalent to $f_m(n) = 0$.

Let k be an integer which we will specify later on. Let N be the set of pairs of elements of S at a distance less than k, i.e.

$$N = \{\{a, b\} \subseteq S \mid a \neq b, |a-b| < k.\}$$

By our previous result,

$$|N| \leq 1 + 2 + \ldots + (k-1) < \frac{k^2}{2}.$$

Now, let $M = \{a \mid \exists b : \{a, b\} \in N\}$. Consider $S \setminus M$. By definition, for any $a, b \in S \setminus M$, we have $|a - b| \geq k$. Since the elements of S are between 0 and $p - 1$, by the pigeonhole principle, we have $|S \setminus M| \leq \frac{p}{k} + 1$. To conclude,

$$|S| \leq |S \setminus M| + |M| \leq |S \setminus M| + |N| \leq \frac{p}{k} + \frac{k^2}{2} + 1.$$

If we now pick $k = \lfloor \sqrt[3]{p} \rfloor$, we get $|S| \leq 2p^{2/3}$ as wanted. ■

Exercise A.3.22† (Mason-Stothers Theorem, ABC conjecture for polynomials)**.** Suppose that $A, B, C \in \mathbb{C}[X]$ are coprime polynomials such that $A + B = C$. Prove that

$$1 + \max(\deg A, \deg B, \deg C) \leq \deg(\operatorname{rad} ABC)$$

where $\operatorname{rad} ABC$ is the greatest squarefree divisor of ABC (in other words, $\deg(\operatorname{rad} ABC)$ is the number of distinct complex roots of ABC). Deduce that the Fermat equation $f^n + g^n = h^n$ for $f, g, h \in \mathbb{C}[X]$ does not have non-trivial solutions for $n \geq 2$.

Solution

Consider the determinant $D = \det \begin{bmatrix} A & B \\ A' & B' \end{bmatrix} = AB' - BA'$. Note that this is the same up sign when we replace A and B by two polynomials out of A, B, C: this is because the determinant is invariant up to sign under column operations (adding certain columns to other columns and exchanging columns, see Proposition C.3.4). Of course, it can also be proven by computing it explicitly: $(A + B)B' - B(A + B)' = AB' - BA'$ (and the rest follows by symmetry). Thus, r is a double root of ABC only if it is a root of D: indeed such a root must a double root of one of A, B, C since they are coprime, say A. It is then a common root of A and A' so of D too. However, a lot more holds. if v is the multiplicity of r in ABC (thus in A in our case), r is a root of multiplicity $v - 1$ of D since it's a root of multiplicity $v - 1$ of A'. Thus,

$$ABC \mid \operatorname{rad}(ABC)D,$$

which gives the wanted bound since $\deg D \leq \deg A + \deg B - 1$ and the same with B, C and C, A by symmetry.

Suppose that $A = f^n$, $B = g^n$, $C = h^n$ are non-zero and satisfy $A + B = C$. Then,

$$\begin{aligned} 1 + n \max(\deg f, \deg g, \deg h) &= 1 + \max(\deg A, \deg B, \deg C) \\ &\leq \deg(\operatorname{rad} ABC) \\ &= \deg(\operatorname{rad} fgh) \leq \deg f + \deg h + \deg h \end{aligned}$$

so $n < 3$ as wanted. ■

Exercise A.3.23†**.** Find all polynomials $f \in \mathbb{C}[X]$ which send the unit circle to itself.

Solution

As in Exercise A.3.9†, $\overline{f(z)} = f(z^{-1})$ for any z on the unit circle. Thus, $1 = |f(z)|^2 = f(z)f(z^{-1})$. Hence, $f(z)(z^n f(z^{-1})) = z^n$ for z on the unit circle, where $n = \deg f$. Note that $X^n f(1/X)$ is

indeed a polynomial: if $f = \sum_{i=0}^{n} a_i X^i$, then $X^n f(1/X) = \sum_{i=0}^{n} a_{n-i} X^i$.

Thus, the polynomials $f(X)(X^n f(1/X))$ and X^n have infinitely many roots in common, which mean that they are equal. In particular, $f \mid X^n$, which implies that $f = \varepsilon X^k$ for some ε and some k. It is clear that ε must be on the unit circle, and conversely any such ε works (in other words, the polynomials which send the unit circle to itself contract it and then rotate it). ■

Exercise A.3.26† (Gauss-Lucas Theorem)**.** Let $f \in \mathbb{C}[X]$ be a polynomial with roots $\alpha_1, \ldots, \alpha_k$. Prove that

$$\frac{f'}{f} = \sum_k \frac{1}{X - \alpha_k}.$$

Deduce the Gauss-Lucas theorem: if $f \in \mathbb{C}[X]$ is non-constant, the roots of f' are in the *convex hull* of the roots of f, that is, any root β of f' is a linear combination $\sum_i \lambda_i \alpha_i$ with $\sum_i \lambda_i = 1$ and non-negative $\lambda_i \in \mathbb{R}$.

Solution

The identity follows from Exercise A.1.8*. Let α be a root of f', without loss of generality such that $f(\alpha) \neq 0$. We have

$$0 = \sum_{i=1}^{n} \frac{1}{\alpha - \alpha_k} = \sum_{i=1}^{n} \frac{\overline{\alpha} - \overline{\alpha_k}}{|\alpha - \alpha_k|^2}$$

so that

$$\overline{\alpha} \sum_{i=1}^{n} \frac{1}{|\alpha - \alpha_k|^2} = \sum_{i=1}^{n} \frac{\overline{\alpha_k}}{|\alpha - \alpha_k|^2}.$$

If we now conjugate this equality, we get

$$\alpha = \frac{\sum_{i=1}^{n} \frac{\alpha_k}{|\alpha - \alpha_k|^2}}{\sum_{i=1}^{n} \frac{1}{|\alpha - \alpha_k|^2}}$$

which has the desired expression. ■

Remark A.3.4

You may notice that the first identity is the logarithmic derivative $(\log f)'$. This can be used to produce an analytic proof of this identity: it holds when $X > \alpha_k$ for all k (in particular they are all real), but is also a polynomial identity in X and the α_k, so it must hold polynomially. More specifically, if we fix the $\alpha_i \in \mathbb{R}$, it holds for sufficiently large X so it must hold for all X. Thus, it holds for all $\alpha_i, X \in \mathbb{R}$ which means that it always holds by Exercise A.1.7*.

Exercise A.3.27† (Sturm's Theorem)**.** Given a squarefree polynomial $f \in \mathbb{R}[X]$, define the sequence $f_0 = f$, $f_1 = f'$ and f_{n+2} is minus the remainder of the Euclidean division of f_n by f_{n+1}. Define also $V(\xi)$ as the number of sign changes in the sequence $f_0(\xi), f_1(\xi), \ldots$, ignoring zeros. Prove that the number of distinct real roots of f in the interval $]a, b]$ is $V(a) - V(b)$.[5]

[5] If we choose $a = -\infty$, $b = +\infty$, this gives an algorithm to compute the number of real roots of f, by looking at the signs of the leading coefficients of $f_0 f_1, \ldots$.

Solution

When x increases from a to b, it may pass through a zero of some f_k (otherwise, by the intermediate value theorem, $V(a) = V(b)$ and there is clearly no root in the intervall as claimed). We shall prove that this leaves $V(x)$ invariant if $k \geq 1$, and decreases it by 1 precisely when $k = 0$, i.e. x is a root of f. Before doing that, note that the important part of the definition of $(f_n)_{n\geq 0}$ is that $f_{n+1} \equiv -f_{n-1} \pmod{f}_n$ for all n. In particular, if $f_n(x)$ and $f_{n+1}(x)$ are zero, then so is $f_{n-1}(x)$, which implies, by induction that x is a root of every f_i. This is impossible since $f_0 = f$ and $f_1 = f'$ have no common root by assumption.

First, suppose that $f_i(\xi) = 0$ for some ξ and $i \geq 1$. Then, since $f_{i+1} \equiv -f_{i-1} \pmod{f_i}$, $f_{i+1}(x)$ and $f_{i-1}(x)$ have opposite signs around ξ (and are non-zero by our previous observation). This means that, before ξ, we had one sign change in $(f_{i-1}(x), f_i(x), f_{i+1}(x))$ since this has the form $(\pm 1, \varepsilon, \mp 1)$ for $\varepsilon \in \{-1, 1\}$. After ξ and at ξ, we still have one sign change for the same reason. Hence, $V(x)$ stays invariant when x passes through a root of some f_i with $i \geq 1$.

Now, suppose that $f(\xi) = 0$. Then, around ξ, $f(\xi + \varepsilon) = \varepsilon f'(\xi) + O(\varepsilon^2)$ which means that the sign of $f(x)$ flips before and after ξ, while the sign of f' does not change since ξ is a simple root. More precisely, before ξ, $f(x)$ and $f'(x)$ had opposite sign, while they have the same sign after ξ. At ξ, we do not count a sign change since $f(\xi) = 0$ so $V(\xi) = V(\xi + \varepsilon)$ for sufficiently small $\varepsilon > 0$, which finishes the proof. ■

Exercise A.3.28† (Ehrenfeucht's Criterion)**.** Let K be a characteristic zero field, let $f_1, \ldots, f_k \in K[X]$ be polynomials and define

$$f = f_1(X_1) + \ldots + f_k(X_k) \in K[X_1, \ldots, X_k].$$

If $k \geq 3$, prove that f is irreducible. In addition, prove that this result still holds if $k = 2$ and f_1 and f_2 have coprime degrees.

Solution

Let us first do the case $k = 2$. Suppose that $f(X) + g(Y)$ is reducible, say equal to uv. Let $m = \deg f$ and $n = \deg g$. Consider $f(X^n) + g(Y^m)$, which is a polynomial of degree mn in both X and Y. Let r and s be the homogeneous parts of $u(X^n, Y^m)$ and $v(X^n, Y^m)$, i.e. the polynomial formed by the monomials of highest degree of $u(X^n, Y^m)$ and $v(X^n, Y^m)$. By looking at the degrees, we must have $rs = aX^{mn} + bY^{mn}$ where a and b are the leading coefficients of u and v respectively.

Suppose without loss of generality (by symmetry) that r has at least two monomials, i.e. u has at least two monomials $X^{i_1}Y^{j_1}$ and $X^{i_2}Y^{j_2}$ such that

$$ni_1 + mj_1 = ni_2 + mj_2 \iff n(i_1 - i_2) = m(j_1 - j_2).$$

Since m and n are coprime, this implies $n \mid j_1 - j_2$ and $m \mid i_1 - i_2$. But then, $\deg_X u \geq m$ and $\deg_Y u \geq n$, which implies that s is constant in both X and Y, i.e. constant, since $f(X)+g(Y) = uv$. This is a contradiction.

Now suppose $k \geq 3$ and $f = uv$. Let $n_i = \deg f_i$ and let a_i be the leading coefficient of f_i. The same argument as before shows that

$$rs = a_1 X_1^N + \ldots + a_k X_k^N,$$

where $N = n_1 \cdot \ldots \cdot n_k$ (we replace X_i by X_i^{N/n_i} and take homogeneous parts). Thus, we have reduced the problem to the case of monomials. We can however reduce it even further: if we evaluate this at $(X, Y, 1, 0, \ldots, 0)$, we get that $aX^N + bY^N + c$ is reducible in $K[X, Y]$ (the

factorisation we get is non-trivial since r and s have degree $< N$ so still degree $< N$ when we evaluate them), say

$$aX^N + bY^N + c = (g_M X^M + \ldots + g_0)(h_{N-M} X^{N-M} + \ldots + h_0)$$

for some polynomials g_i, h_i in Y of degree $< N$. Now, substitute y a complex root of $bY^N + c$ to Y. This gives us the polynomial aX^N which can only be factored as a product of two monomials, so

$$g_0(y) = \ldots = g_{M-1}(y) = h_{N-M-1}(y) = \ldots = h_0(y).$$

But since the roots of $bY^N + c$ are distinct (there is no common root with the derivative NbY^{N-1}), g_i and h_j for $i < M$ and $j < N - M$ vanish at N distinct points, which is more than their degree. Thus, they must be zero. This leaves us with the factorisation $aX^N + bY^N + c = g_M h_{N-M} X^N$ which is clearly impossible since X^N doesn't divide the LHS. ■

Exercise A.3.29† (IMC 2007)**.** Let $a_1, \ldots, a_n$ be integers. Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is a function such that

$$\sum_{i=1}^{n} f(ka_i + \ell) = 0$$

for any $k, \ell \in \mathbb{Z}$. Prove that f is identically zero.

Solution

Consider the set I of polynomials $f = \sum_{i=0}^{m} b_i X^i \in \mathbb{Q}[X]$ such that

$$\sum_{i=1}^{m} b_i f(i + x) = 0$$

for any $x \in \mathbb{Z}$. We claim that this set is an *ideal* of $\mathbb{Q}[X]$, meaning that it's closed under addition, and closed under multiplication by any polynomial in $\mathbb{Q}[X]$. The first fact is clear. For the second, note that multiplication by X^i corresponds to a translation and that multiplication by a constant is trivial, so we can deduce it from the first fact. Thus, I is closed under gcd: by Bézout's lemma, if $f, g \in I$, there are $u, v \in \mathbb{Q}[X]$ such that

$$\gcd(f, g) = uf + vg \in I.$$

Our goal is to show that I contains the element 1: this gives $f(x) = 0$ for any $x \in \mathbb{Z}$ as wanted. The statement gives us that

$$f = \sum_{i=1}^{n} X^{ka_i + \ell} \in I$$

for any k, ℓ such that $ka_i + \ell \geq 0$ for all i. Hence, the problem reduces to proving that these polynomials are coprime, i.e., that for any algebraic number α, $\sum_{i=1}^{n} \alpha^{ka_i}$ can not always be zero. This follows from our proof of Theorem C.4.1: this is a linear recurrence, and the only linear recurrence which is identically zero is the zero recurrence. However, $\sum_{i=1}^{n} \alpha^{ka_i}$ is clearly not the zero recurrence since the coefficient before α^{ka_i} for every i. ■

Appendix B

Symmetric Polynomials

B.1 The Fundamental Theorem of Symmetric Polynomials

Exercise B.1.1. Let $f \in K(X_1, \ldots, X_n)$ be a rational function, where K is a field. Suppose f is symmetric, i.e. invariant under permutations of $X_1, \ldots, X_n$. Prove that $f = g/h$ for some symmetric polynomials $g, h \in K[X_1, \ldots, X_n]$.

Solution

Let $r = f/g$ be a symmetric rational function. We write it as

$$r = \frac{\prod_{\sigma \in \mathfrak{S}_n} f(\sigma(X_1, \ldots, X_n))}{g \prod_{\mathrm{id} \neq \sigma \in \mathfrak{S}_n} f(\sigma(X_1, \ldots, X_n))}.$$

The numerator is a symmetric polynomial so the denominator must be too since the quotient is. ■

Exercise B.1.2. Prove that the decomposition of a symmetric polynomial f as $g(e_1, \ldots, e_n)$ is unique.

Solution

This accounts to proving that $f(e_1, \ldots, e_n) = 0$ if and only if $f = 0$. This is clear by induction on n (trivial when $n = 1$). Let f be such a polynomial and suppose for the sake of a contradiction that $e_n \mid f$. If we set $X_n = 0$ we get

$$f(e_1, \ldots, e_{n-1}, 0) = 0$$

where the e_i are now the elementary symmetric polynomials in $X_1, \ldots, X_{n-1}$. By the induction hypothesis, this means that $f(X_1, \ldots, X_{n-1}, 0) = 0$, i.e. $X_n \mid f$. By symmetry, $e_n = X_1 \cdot \ldots \cdot X_n \mid f$, a contradiction. ■

B.2 Newton's Formulas

Exercise B.2.1*. Prove Corollary B.2.1.

Solution

We have $K(p_1, \ldots, p_n) \subseteq K(e_1, \ldots, e_n)$ by the fundamental theorem of symmetric polynomials, and the reverse inclusion comes from the Newton formulas by induction, as explained before. (We need the assumption that K is a field because the LHS of the Newton's formulas has a factor of k which we need to divide by in the inductive step, and we need K to have characteristic zero so that $k \neq 0$.) ■

B.3 The Fundamental Theorem of Algebra

Exercise B.3.1*. Prove Proposition B.3.2.

Solution

By the quadratic formula (or completing the square), solving quadratic equations is equivalent to finding square roots. Thus, let $a + bi \in \mathbb{C}$ be a complex number, with $a, b \in \mathbb{R}$. We wish to find a square root $x + iy$ or $a + bi$, i.e.

$$x^2 - y^2 + 2ixy = (x + iy)^2 = a + bi.$$

This means $x^2 - y^2 = a$ and $2xy = b$. This is equivalent to x^2 and $-y^2$ being roots of $X^2 - aX - b^2/4$ by Vieta's formulas. Since the constant coefficient is negative, the roots are real (e.g. by the intermediate value theorem), and since the product is negative, one is positive and one negative. Label the positive one as x^2 and the negative one as $-y^2$, take the square roots to find x and y and adjust the sign to have $2xy = b$. ■

B.4 Exercises

Newton's Formulas

Exercise B.4.2† (Hermite's Theorem)**.** Prove that a function $f : \mathbb{F}_p \to \mathbb{F}_p$ is a bijection if and only if $\sum_{a \in \mathbb{F}_p} f(a)^k$ is 0 for $k = 1, \ldots, p-2$ and -1 for $k = p-1$.

Solution

If f is a bijection, then this is Exercise A.3.11†. Now suppose that this condition holds. Newton's formulas (note $k \neq 0$ for $k < p$ so Corollary B.2.1 still holds) tell us that there is only one possible value of $e_k(f(0), \ldots, f(p-1))$ for any fixed k. Hence, we must have

$$e_k(f(0), \ldots, f(p-1)) = e_k(0, \ldots, p-1)$$

since $0, \ldots, p-1$ satisfy the condition. This implies that

$$(X - f(0)) \cdot \ldots \cdot (X - f(p-1)) = (X - 0) \cdot \ldots \cdot (X - (p-1))$$

so f is a bijection as wanted. ■

Exercise B.4.3†. Suppose that $\alpha_1, \ldots, \alpha_n$ are such that $\alpha_1^k + \ldots + \alpha_k^n$ is an algebraic integer for all n. Prove that $\alpha_1, \ldots, \alpha_k$ are algebraic integers.

Solution

Newton's formulas give us $k!e_i(\alpha_1,\dots,\alpha_k) \in \overline{\mathbb{Z}}$ for any i. Thus, $k!\alpha \in \overline{\mathbb{Z}}$ for any $\alpha = \alpha_i$, by Exercise 1.5.22†. In particular, since the statement is also true when we replace the α_i by α_i^m for any fixed m, we get $k!\alpha^m \in \overline{\mathbb{Z}}$ for any m.

Thus, the problem reduces to showing that, if $\alpha \in \overline{\mathbb{Q}}$ is algebraic and such that $N\alpha^n \in \overline{\mathbb{Z}}$ (i.e. powers of α have bounded denominator) for some non-zero $N \in \mathbb{Z}$ and any positive integer n, then $\alpha \in \overline{\mathbb{Z}}$. For large n, the degree of α^{2^n} is constant, since the sequence

$$[\mathbb{Q}(\alpha^{2^n}) : \mathbb{Q}] = [\mathbb{Q}(\alpha^{2^n}) : \mathbb{Q}(\alpha^{2^{n-1}})][\mathbb{Q}(\alpha^{2^{n-1}}) : \mathbb{Q}]$$

is a non-increasing sequence of integers. By replacing α by α^{2^m} for some large m, we may assume that this is true for any $n \geq 0$. Let $\beta_1,\dots,\beta_\ell$ be the conjugates of α. Consider the minimal polynomial

$$f_{2^k} = \prod_{i=1}^{\ell} X - \beta_i^{2^k}$$

of α^{2^k} and let $N_k = 1/c(f_{2^k}))$ be the smallest positive integer such that $N_k f_{2^k} \in \mathbb{Z}[X]$. By assumption N_k is bounded. However, we have

$$\begin{aligned} N_k^2 f_{2^{k+1}}(X^2) &= N_k^2 \prod_{i=1}^{\ell} X^2 - \beta_i^{2^{n+1}} \\ &= \left(N_k \prod_{i=1}^{\ell} X - \beta_i^{2^n}\right)\left(N_k \prod_{i=1}^{\ell} X + \beta_i^{2^n}\right) \\ &= \pm(N_k f_{2^k})(N_k f_{2^k}(-X)) \end{aligned}$$

which is primitive by Gauss' lemma 5.1.2. Hence, $N_{k+1} = N_k^2$ so N_1 must be 1 otherwise $N_k = N_1^{2^{n-1}} \to \infty$. This means that the minimal polynomial of α has integral coefficients, i.e. α is an algebraic integer. ■

Remark B.4.1

It is necessary to mention that the key claim admits a very short and intuitive proof if we allows ourself some ideal theory. The idea is that, if $\alpha \in \mathbb{Q}$, we can simply look at the p-adic valuations to get $nv_p(\alpha) + v_p(N) \geq 0$ which gives us $v_p(\alpha) \geq 0$ for large enough n. Hence, α is an integer. For arbitrary algebraic integers, the same proof works almost verbatim: a number field K is not always a UFD but always has ideal factorisation. This means that we can this time consider prime ideals $\mathfrak{p}$ of K to get $nv_\mathfrak{p}(\alpha) + v_\mathfrak{p}(N) \geq 0$ which implies $v_\mathfrak{p}(\alpha) \geq 0$ again. Finally, since this is true for any prime ideal $\mathfrak{p}$, we get $\alpha \in \mathcal{O}_K$.

Algebraic Geometry

Exercise B.4.4† (Resultant)**.** Let R be a commutative ring, and $f, g \in R[X]$ be two polynomials of respective degrees m and n. For any integer $k \geq 0$, denote by $R_k[X]$ the subset of $R[X]$ consisting of polynomials of degree less than k. The *resultant* $\mathrm{Res}(f,g)$ is defined as the determinant of the linear map

$$(u, v) \mapsto uf + vg$$

from $R_m[X] \times R_n[X]$ to $R_{m+n}[X]$. Prove that, if $f = \sum_i a_i X^i$ and $g = \sum_i b_i X^i$, we have[1]

$$\operatorname{Res}(f,g) = \begin{vmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \cdots & 0 & b_1 & b_0 & \cdots & 0 \\ a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 \\ a_m & a_{m-1} & \cdots & \vdots & b_n & b_{n-1} & \cdots & \vdots \\ 0 & a_m & \ddots & \vdots & 0 & b_n & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_{m-1} & \vdots & \vdots & \ddots & b_{n-1} \\ 0 & 0 & \cdots & a_m & 0 & 0 & \cdots & b_n \end{vmatrix},$$

and, if $f = a\prod_i X - \alpha_i$ and $g = b\prod_j X - \beta_j$, then[2]

$$\operatorname{Res}(f,g) = a^m b^n \prod_{i,j} \alpha_i - \beta_j.$$

In addition, prove that $\operatorname{Res}(f,g) \in (fR[X] + gR[X])$.[3] Finally, prove that if $f, g \in \mathbb{Z}[X]$ are monic and $uf + vg = 1$ for some $u, v \in \mathbb{Z}[X]$, $\operatorname{Res}(f,g) = \pm 1$. (It is not necessarily true that $(fR[X]+gR[X]) \cap R = \operatorname{Res}(f,g)R$ for specific polynomials f, g, but we always have $\operatorname{Res}(f,g) \in fR[X]+gR[X]$ by the previous point.)

Solution

The determinant form of the resultant simply follows from considering the matrix of the linear function corresponding to the basis $1, X, \ldots, X^{m+n-1}$. To prove the explicit formula, consider the case where $A = a$, $B = b$, $\alpha_i = A_i$ and $\beta_j = B_j$ are indeterminates. Working over a field K, the resultant vanishes when $A_i = B_j$ for some i, j since the map is not surjective: it never reaches 1. Thus, the resultant is divisible by $A_i - B_j$ for all i, j. Looking at the determinant formula, we see that the degree of $\operatorname{Res}(f,g)$ in A_1 is n and its leading coefficient is $A^m B^n$, which proves the wanted formula.

For the second part, write the equation $uf+vg = r$ in the monomial basis as $RV = (r, 0, \ldots, 0) := re_1$, where R is the matrix corresponding to the linear map $(u, v) \mapsto uf + vf$. Hence, we wish to have $rR^{-1}e_1 \in R^n$. **??** tells us that $r = \det R = \operatorname{Res}(f,g)$ works.

Now let f and g be generic polynomials with integer coefficients of respective degree m and n.

Suppose finally that $(f\mathbb{Z}[X] + g\mathbb{Z}[X]) \cap \mathbb{Z} = \mathbb{Z}$. Write f and g as $\prod_{i=1}^m X - \alpha_i$ and $\prod_{j=1}^n X - \beta_i$. We have $u(\beta_i)f(\beta_i) = 1$ for each i, so

$$\prod_{i=1}^{f}(\beta_i) = \pm \operatorname{Res}(f,g)$$

divides 1 as desired. ■

Exercise B.4.6† (Hilbert's Nullstellensatz)**.** Let K be an algebraically closed field. Suppose that $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ have no common zeros in K. Prove that there exist polynomials $g_1, \ldots, g_m$ such that

$$f_1 g_1 + \ldots + f_m g_m = 1.$$

[1] This is an $(m+n) \times (m+n)$ matrix, with n times the element a_0 and m times the element b_0.

[2] In particular, the discriminant of f is $\frac{(-1)^{\frac{n(n-1)}{2}}}{a} \cdot \operatorname{Res}(f, f')$.

[3] In other words, the resultant provides an explicit value of a possible constant in Bézout's lemma for arbitrary rings (such as $\mathbb{Z}$).

Deduce that, more generally, if f is a polynomial which is zero at common roots of polynomials $f_1, \dots, f_m$ (we do not assume anymore that they have no common roots), then there is an integer k and polynomials $g_1, \dots, g_m$ such that

$$f^k = f_1 g_1 + \dots + f_m g_m.$$

Solution

We proceed by induction on the number n of variables. When $n = 1$ this is just Bézout's lemma. Now, if $n \geq 1$, we will eliminate one variable with the resultant. Consider the polynomial

$$g = \mathrm{Res}_{X_n}(f_m, U_1 f_1 + \dots + U_{m-1} f_{m-1}) \in K[U_1, \dots, U_{m-1}][X_1, \dots, X_{n-1}],$$

where $U_1, \dots, U_{m-1}$ are formal variables. By Exercise B.4.4†, $(x_1, \dots, x_{n-1})$ is a root of g if and only if f_m and $U_1 f_1 + \dots + U_{m-1} f_{m-1}$ have a common root x_n at $(x_1, \dots, x_{n-1})$, i.e. $(x_1, \dots, x_n)$ is a common root of $f_1, \dots, f_m$, or if the leading coefficient in X_n of f_m and $U_1 f_1 + \dots + U_{m-1} f_{m-1}$ vanish at $(x_1, \dots, x_{n-1})$, i.e. the leading coefficient in X_n of $f_1, \dots, f_m$ vanish at $(x_1, \dots, x_{n-1})$ (we say $(x_1, \dots, x_{n-1})$ is a common root at infinity). We wish to rule out the second case. This is not very hard: perform the change of coordinates $X_i \to X_i + c_i X_n$ for $i = 1, \dots, n-1$ and some c_i to get constant leading coefficients in X_n (thus sharing no common root).

Hence, g has no root by assumption since $f_1, \dots, f_m$ have no common root. However, a root of g is simply a common root of its coefficients g_i when g is seen as a polynomial in $U_1, \dots, U_{m-1}$. This implies that a linear combination of the g_i is 1, by the induction hypothesis. Finally, notice that

$$g = \mathrm{Res}_{X_m}(f, U_1 f_1 + \dots + U_{m-1} f_{m-1}) = uf + v(U_1 f_1 + \dots + U_{m-1} f_{m-1})$$

for some $u, v \in K[X_1, \dots, X_n][U_1, \dots, U_{m-1}]$, by Exercise B.4.4†. Hence, the coefficients g_i of g are linear combinations of the f_i (with coefficients in $K[X_1, \dots, X_n]$). We conclude that a linear combination of the f_i is 1 as wanted.

For the second part, suppose without loss of generality that $f \neq 0$. Use the first part on $f_1, \dots, f_m, 1 - X_{n+1} f$ which have no common root by assumption (this is known as Rabinowitsch's trick). Thus, there are $g_1, \dots, g_m, g \in K[X_1, \dots, X_{n+1}]$ such that

$$g_1 f_1 + \dots + g_m f_m + g(1 - X_{n+1} f) = 1.$$

Now, evaluate this at $X_{n+1} = 1/f$ and multiply by a large enough power of f to get the wanted equality. ■

Exercise B.4.7† (Weak Bézout's Theorem)**.** Prove that two coprime polynomials $f, g \in K[X, Y]$ of respective degrees m and n have at most mn common roots in K. (Bézout's theorem states that they have exactly mn common roots counted with multiplicity, possibly at infinity.[4])

Solution

We can assume without loss of generality that K has as many elements as we want by iteratively adding new elements to K using Exercise 4.2.1*.)

We shall proceed as in Exercise B.4.6†. Consider the resultant $h = \mathrm{Res}_Y(f, g)$. This is a polynomial of degree at most mn by its matrix expression of Exercise B.4.4†. By the same exercise, if (x, y) is a common root of f, g, then x is a root of h. Thus, we would be done if there was at most one possible value of y for each x, since h has degree at most mn and thus

[4] This requires some care: we need to define the multiplicity of common roots as well as what infinity means. See any introductory text to algebraic geometry, e.g. Sharevich [**shafarevich**]. See also the appendix on projective geometry of Silverman-Tate [26].

has at most mn roots. Note that we already get that there are finitely many common roots (although that's already a consequence of Bézout's lemma). Here is how we can achieve that: do a change of coordinates $X \to X + c'Y$ for some c chosen so that each x appears at most once as a common root (x, y) of f and g: this is possible because the common roots in this new system of coordinates are $(\alpha + c'\beta, \beta)$ and there are finitely many c' for which

$$\alpha + c'\beta = \alpha' + c'\beta' \iff c = \frac{\alpha - \alpha'}{\beta' - \beta}.$$

■

Exercise B.4.8†. Prove that $n+1$ polynomials $f_1, \dots, f_{n+1} \in K[X_1, \dots, X_n]$ in n variables are *algebraically dependent*, meaning that there is some non-zero polynomial $f \in K[X_1, \dots, X_{n+1}]$ such that

$$f(f_1, \dots, f_{n+1}) = 0.$$

Solution

We present two solutions: one with linear algebra and one with resultants.

For the first solution, consider the linear system of equations in $(N+1)^{n+1}$ variables

$$\sum_{i_1, \dots, i_{n+1} \leq N} a_{i_1, \dots, i_{n+1}} f_1^{i_1} \cdot \dots \cdot f_{n+1}^{i_{n+1}} = 0. \tag{$*$}$$

We wish to find a non-trivial solution to this system. Let us count the number of equations we have. Set $M = \max_i(\deg f_i)$. Then, the LHS of $(*)$ is a polynomial of degree $(n+1)MN$, when we consider the $a_{i_1, \dots, i_{n+1}}$ as formal variables. Hence, we have $(N+1)^{n+1}$ unknowns and

$$\sum_{k=0}^{N} ((n+1)MN)^k = \frac{((n+1)MN)^{n+1} - 1}{(n+1)MN - 1}$$

equations, one for each coefficient. For large N, $(N+1)^{n+1} > \frac{((n+1)MN)^{n+1}-1}{(n+1)MN-1}$, which means that there is a non-trivial solution as wanted (the kernel is non-trivial by e.g. the rank-nullity theorem **??**, or Proposition C.1.2).

To make the idea of the second solution clearer, we treat the case $n = 1$ first. If $f, g \in K[X]$ are polynomials, the resultant $h = \mathrm{Res}_X(f - S, g - T)$ is a non-zero polynomial in S, T with coefficients in K. Indeed, it is non-zero since when $S - f$ and $T - g$ are coprime it takes a non-zero value (we can choose $T = 0$ and $S \in K$ to be a large constant for instance). However, when $S = f$ and $T = g$, the polynomials $f - S$ and $g - T$ are not coprime anymore so $h(f, g) = 0$ as wanted.

Now, we construct by backwards induction on k a polynomial with coefficients in $K[X_1, \dots, X_k]$ vanishing at $f_1, \dots, f_{n+1}$. In other words, we eliminate one variable each time. Here is how we do it: at first, $f_{n,i} = f_i$. Then, we define the polynomials

$$f_{k-1,i} = \mathrm{Res}_{X_k}(f_{k,k+1} - T_{k,k+1}, f_{k,i} - T_{k,i})$$

for $i = 1, \dots, k$. At each step we get rid of X_k and introduce $k+1$ new variables. Thus, $f_{0,1} \in K[\{T_{i,j} \mid i \leq j - 1\}$. It is clear that it is zero when evaluated at $T_{n,i} = f_i$ for every i and $T_{k,i}$ constant for $i \leq k - 1 \leq n - 2$. Indeed, note that $\mathrm{Res}(A, B)(t)$ is not in general equal to $\mathrm{Res}(A(t), B(t))$, since $A(t), B(t)$ do not have the same degree as A, B. If we consider constant polynomials as polynomials of degree $\deg(f_{k,i} - T_{k,i}) > 0$, then

$$\mathrm{Res}_{X_k}(f_{k,k+1} - T_{k,k+1}, f_{k,i} - T_{k,i}) = 0,$$

as can be seen from the matrix expression of Exercise B.4.4†. It remains to prove that there is some choice of such $T_{k,i}$ for which $f_{0,1}$ is not the zero polynomial. This is easy to see: we can choose $T_{k,k+1} = 0$ for all k and at each step we pick $T_{k,i}$ so that $f_{k,k+1}$ and $f_{k,i} + T_{k,i}$ are coprime. Indeed, if $f_{k,k+1}$ has ℓ irreducible prime factors, if we pick $\ell + 1$ values of $T_{k,i}$ one of them must work, as otherwise we would have

$$\pi \mid (f_{k,i} + T_{k,i}) - (f_{k,i} - T'_{k,i}) = T_{k,i} - T'_{k,i}$$

for some irreducible $\pi \mid f_{k,k+1}$ and distinct $T_{k,i}, T'_{k,i} \in K$ by the pigeonhole principle. This is impossible sine it implies $T_{k,i} = T'_{k,i}$. There is still one slight technicality: we could have $\ell \geq |K|$. However, we can simply add elements to K to get a sufficiently large K as in Exercise B.4.7†, and then consider the norm of the polynomial f we obtain (i.e. take the product over each of its conjugates, exactly like we did in the solution of Exercise 1.5.22†). ■

Exercise B.4.9† (Transcendence Bases)**.** Let L/K be a field extension. Call a maximal set of K-algebraically independent elements of L a *transcendence basis*. Prove that, if L/K has a transcendence basis of cardinality n, then all transcendence bases have cardinality n. This n is called the *transcendence degree* $\operatorname{trdeg}_K L$. Finally, show that, if $L = K(\alpha_1, \ldots, \alpha_n)$ any maximal algebraically independent subset of $\alpha_1, \ldots, \alpha_n$ is a transcendence basis. (In particular $\operatorname{trdeg}_K L \leq n$.)

Solution

We prove a result analogous to Proposition C.1.2: if $\alpha_1, \ldots, \alpha_m \in L$ are K-algebraically independent and $\beta_1, \ldots, \beta_n \in L$ are such that any element of L is algebraic over $K(\beta_1, \ldots, \beta_n)$, then $m \leq n$. Since transcendence bases satisfy both conditions, this shows that $\operatorname{trdeg}_K L$ is well-defined. This almost Exercise B.4.8†: any family of $n+1$ elements algebraic over $K(\beta_1, \ldots, \beta_n)$ is algebraically dependent over K. The only difference is that, in our case $\alpha_1, \ldots, \alpha_m$ are not necessarily in $K(\beta_1, \ldots, \beta_n)$. However, the first argument still works perfectly fine, the only difference is that, if α_i has degree d_i over $K(\beta_1, \ldots, \beta_n)$, we get (at most)

$$\prod_{i=1}^{m} d_i \frac{(mMN)^{n+1} - 1}{mMN - 1}$$

equations this time, which is still less than $(N+1)^m$ for large N if $m > n$.

For the second part, note that, by the same argument as Theorem 1.3.2 or by Chapter 6, any element of $K(\alpha_1, \ldots, \alpha_n)$ is algebraic over $K(S)$, where $S \subseteq \{\alpha_1, \ldots, \alpha_n\}$ is a maximal subset of K-algebrically independent element. ■

Exercise B.4.10†. Let K be an algebraically closed field which is contained in another field L. Suppose that $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ are polynomials with a common root in L. Prove that they also have a common root in K.

Solution

We present two solutions, one based on Hilbert's Nullstellensatz from Exercise B.4.6† and one in characteristic 0 based on transcendence basis from Exercise B.4.9†. For the first sol, note that $f_1, \ldots, f_m$ have a common root in L if and only if there are no $g_1, \ldots, g_m \in L[X_1, \ldots, X_n]$ such that $f_1 g_1 + \ldots + f_m g_m = 1$. In that case, there are no such g_i in $K[X_1, \ldots, X_n]$ either, so $f_1, \ldots, f_m$ also have a common root in K.

We new present the second solution, which is perhaps more intuitive as it "lifts" (or "reduces" in our case) the common root over L to a common root over K. Thus, suppose that $\operatorname{char} K = 0$

and let $\alpha_1, \dots, \alpha_k$ be a K-transcendence basis for the field generated by K and the common root. Then, let α be such that this field is equal to $K(\alpha_1, \dots, \alpha_k, \alpha)$, there exists such an α by the primitive element theorem 6.2.1. Let

$$r_1(\alpha_1, \dots, \alpha_k)(\alpha), \dots, r_n(\alpha_1, \dots, \alpha_k)(\alpha))$$

be the common root, with $r_i \in K(X)$. The equality

$$f_i(r_1(\alpha_1, \dots, \alpha_k)(\alpha), \dots, r_n(\alpha_1, \dots, \alpha_k)(\alpha)) = 0$$

is an equality modulo the minimal polynomial $\pi(\alpha_1, \dots, \alpha_k)$ of α. Thus, if we replace α_i by $a_i \in K$ and α by a root $a \in K$ of $\pi(a_1, \dots, a_k)$, we get a common root in K. We just need to check that the $r_i(a_1, \dots, a_k)(a)$ are well-defined, i.e. their denominator is non-zero. This follows from Exercise A.1.7*: the denominator is non-zero so it stays non-zero infinitely many times in K^n. Note that $r_i(\alpha)$ is not necessarily a polynomial, instead it is algebraic over $K(\alpha_1, \dots, \alpha_k)$, but by considering its norm (the product with its conjugates over $K(\alpha_1, \dots, \alpha_k)$) we can get a polynomial. Indeed, if the norm of $r_i(\alpha)$ is non-zero then so is $r_i(\alpha)$. (We also need to be careful with the leading coefficient of π: if it vanishes α has too few conjugates and things can get weird, but we can simply pick $a_1, \dots, a_k$ so that it doesn't vanish either.) ■

Miscellaneous

Exercise B.4.11† (ISL 2020 Generalised)**.** Let $n \geq 1$ be an integer. Find the maximal N for which there exists a monomial f of degree N which can not be written as a sum

$$\sum_{i=1}^{n} e_i f_i$$

with $f_i \in \mathbb{Z}[X_1, \dots, X_n]$.

Solution

The answer is $N = \frac{n(n-1)}{2}$. First, we prove that $X_2 X_3^2 \cdot \ldots \cdot X_n^{n_1}$ can not be written in the desired form. Suppose for the sake of a contradiction that $X_2 X_3^2 \cdot \ldots \cdot X_n^{n_1} = \sum_i e_i f_i$ for some polynomials f_i, which we suppose without loss of generality to be homogeneous of degree $\frac{n(n-1)}{2} - i$ (by ignoring all other monomials). Then, we sum $\varepsilon(\sigma) X_{\sigma(2)}^1 \cdot \ldots \cdot X_{\sigma(n)}^{n-1}$ over all permutations $\sigma \in \mathfrak{S}_n$ of $[n]$, where ε denotes the signature (see Definition C.3.2). Since the e_i are symmetric, we have

$$\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) X_{\sigma(2)}^1 \cdot \ldots \cdot X_{\sigma(n)}^{n-1} = \sum_i e_i \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) f_i(X_{\sigma(1)}, \dots, X_{\sigma(n)}).$$

Here is the key point: if f has degree less than $\frac{n(n-1)}{2}$, $\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = 0$. This is an obvious contradiction as the LHS is a sum of distinct monomials so is non-zero. To prove this claim, suppose without loss of generality that f is a monomial $\prod_{i=1}^n X_i^{a_i}$. Since $\sum_{i=1}^n a_i < \sum_{i=1}^n (i-1)$, two a_i must be equal, say $a_i = a_j$. Denote by τ the transposition $i \leftrightarrow j$. Then, by grouping permutations of $[n]$ by orbits $\sigma, \sigma \circ \tau$, the sum is zero since

$$f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = f(X_{\sigma \circ \tau(1)}, \dots, X_{\sigma \circ \tau(n)})$$

but $\varepsilon(\sigma \circ \tau) = -\varepsilon(\sigma)$ by Exercise C.3.11* so the sum over each orbits cancels out.

It remains to prove that $X_1^{a_1} \cdot \ldots \cdot X_n^{a_n}$ works when $a_1 + \ldots + a_n > \frac{n(n-1)}{2}$. When $a_1, \dots, a_n \geq 1$ it is trivial since the monomial is divisible by e_1. We proceed by induction on $a_1^2 + \ldots + a_n^2$, with the following base case: $a_1, \dots, a_n \geq 1$ the monomial is divisible by e_1.

Now suppose that $a_1 + \ldots + a_n > \frac{n(n-1)}{2}$ and, without loss of generality, $0 = a_1 \leq a_2 \leq \ldots \leq a_n$. There must exist some k such that $e_{k+1} \geq e_k + 2$, since otherwise $e_k \leq k-1$ for all k contradicting our initial assumption on the sum. Now consider

$$X_1^{a_1} \cdot \ldots \cdot X_n^{a_n} - X_1^{a_1} \cdot \ldots \cdot X_{k-1}^{a_{k-1}} X_k^{a_k - 1} \cdot \ldots \cdot X_n^{a_n - 1} e_{n-k}.$$

We claim that the sum of the squares of the exponents in any monomial appearing in this polynomial is less than $a_1^2 + \ldots + a_n^2$, thus concluding the inductive step. To see this, express a monomial of $X_1^{a_1} \cdot \ldots \cdot X_{k-1}^{a_{k-1}} X_k^{a_k - 1} \cdot \ldots \cdot X_n^{a_k} e_{n-k}$ as

$$X_1^{a_1 + b_1} \cdot \ldots \cdot X_{k-1}^{a_{k-1} + b_{k-1}} X_k^{a_k + b_k - 1} \cdot \ldots \cdot X_n^{a_n + b_n - 1}$$

for some $b_i \in \{0, 1\}$ with $b_1 + \ldots + b_n = n - k$. The wanted result then follows from the convexity of the square function: if $b_i = 1$ for some $i < k$ and $b_j = 0$ for some $j \geq k$, then $(a_i + 1)^2 + (a_j - 1)^2 < a_i^2 + a_j^2$. Iterating this process to "push" all the ones to the positions greater than or equal to k, we get

$$(a_1 + b_1)^2 + \ldots + (a_{k-1} + b_{k-1})^2 + (a_k + b_k - 1)^2 + \ldots + (a_n + b_n - 1)^2 \leq a_1^2 + \ldots + a_n^2$$

with equality if and only if we already had equality in the beginning, i.e. if the monomial is $X_1^{a_1} \cdot \ldots \cdot X_n^{a_n}$. However, we have ruled that case out by subtracting precisely this monomial, so we are done. ■

Exercise B.4.12† (Lagrange)**.** Given a rational function $f \in K[X_1, \ldots, X_n]$, we denote by G_f the set of permutations $\sigma \in \mathfrak{S}_n$ such that

$$f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Let $f, g \in K(X_1, \ldots, X_n)$ be two rational functions. If $G_f \subseteq G_g$, prove that there exists a rational function $r \in K[e_1, \ldots, e_n](X)$ such that

$$g = r \circ f.$$

Solution

We present the proofs in Prasolov [21]. Partition G_g into disjoint cosets $G_f = h_1 G_f, h_2 G_f, \ldots, h_k G_f$ and write $f_i = h_i f$ and $g_i = h_i f$ for each i, where σf means $f(X_{\sigma(1)}, \ldots, f(X_{\sigma(n)})$ (we say the group of permutations $\mathfrak{S}_n$ *acts* on the field $K(X_1, \ldots, X_n)$). (This is where we use the assumption that $G_f \subseteq G_g$.)

For the first proof, notice that

$$\sum_{i=1}^{k} \frac{g_i}{T - f_i}$$

is, by definition, symmetric in $X_1, \ldots, X_n$. Since $\Omega = \prod_{i=1}^{k} T - f_i$ is as well, we get

$$\sum_{i=1}^{k} \frac{g_i}{T - f_i} = \frac{F(T)}{\Omega(T)}$$

for some $F \in K(e_1, \ldots, e_n)[T]$ by the fundamental theorem of symmetric polynomials. Notice that $F'(f) = \prod_{i=2}^{k} f - f_i$ is $F/(T - f)$ evaluated at $T = f$ by Exercise 3.2.2*. Hence, we conclude that

$$\frac{F(f)}{\Omega'(f)} = \sum_{i=1}^{k} g_i \left(\frac{\Omega}{(T - f_i)\Omega'} \right)(f) = g$$

since $\frac{\Omega}{(T - f_i)\Omega'}$ vanishes at $f \neq f_i$.

The second proof is perhaps more intuitive. We consider the system of equations

$$\sum_{i=1}^{k} f_i^s g_i = T_s,$$

where the exponent represents powers and not iterates. Cramer's rule from Exercise C.5.7 and the Vandermonde determinant from Appendix C and tell us that

$$g = \frac{D}{\Delta}$$

where

$$\Delta = \begin{vmatrix} 1 & \cdots & 1 \\ f_1 & \cdots & f_n \\ \vdots & \ddots & \vdots \\ f_1^{k-1} & \cdots & f_k^{k-1} \end{vmatrix} = \prod_{i<j} f_i - f_j$$

and

$$D = \begin{vmatrix} T_0 & 1 & \cdots & 1 \\ T_1 & f_2 & \cdots & f_k \\ \vdots & \vdots & \ddots & \vdots \\ T_{k-1} & f_2^{k-1} & \cdots & f_k^{k-1} \end{vmatrix}.$$

Write this as $g = \frac{D\Delta}{\Delta^2}$. Notice that Δ^2 is symmetric, while D and Δ both change sign when two f_i are switched, so $D\Delta$ is symmetric in $f_2, \ldots, f_k$. However, it is easy to see that, for any i, $e_i(f_2, \ldots, f_k)$ can be expressed polynomially in terms of f_1 and $e_j(f_1, \ldots, f_k)$. Hence, this $\frac{D\Delta}{\Delta^2}$ is a rational function in f with symmetric coefficients by the fundamental theorem of symmetric polynomials. ■

Exercise B.4.13† (Iran Mathematical Olympiad 2012)**.** Prove that there exists a polynomial $f \in \mathbb{R}[X_0, \ldots, X_{n-1}]$ such that, for all $a_0, \ldots, a_{n-1} \in \mathbb{R}$,

$$f(a_0, \ldots, a_{n-1}) \geq 0$$

is equivalent to the polynomial $X^n + a_{n-1}X^{n-1} + \ldots + a_0$ having only real roots, if and only if $n \in \{1, 2, 3\}$.

Solution

If $n \leq 3$, the discriminant satisfies the condition. Indeed, the discriminant of $f = \prod_i X - \alpha_i$ is the square of $\prod_{i<j} \alpha_i - \alpha_j$ so is positive if all α_i are positive. It remains to prove that, for these n, $\prod_{i<j} \alpha_i - \alpha_j$ is real if and only if all α_i are (its square is real so it must be real or purely imaginary). For $n = 1$, it is trivial since any polynomial of degree 1 with real coefficients splits in $\mathbb{R}$. For $n = 2$, if the roots of f are $\alpha \neq \overline{\alpha}$, then $\alpha - \overline{\alpha}$ is not real since complex conjugation negates it. For $n = 3$, if the roots of f are $\alpha \neq \overline{\alpha}$ and $\beta \in \mathbb{R}$, then complex conjugation also negates

$$(\alpha - \overline{\alpha})(\beta - \alpha)(\beta - \overline{\alpha})$$

so it isn't real as desired.

Now, if there exists such a polynomial for $n \geq 4$, there exists one for $n = 4$ by setting $g(a, b, c, d) = f(a, b, c, d, 0, \ldots, 0)$. Thus, it only remains to prove that there doesn't exist such a polynomial for $n = 4$. For this, consider the special polynomial $f(0, b, 0, d)$ since we know precisely when the roots of $X^4 + bX^2 + d$ are real. For convenience, we shall in fact consider the polynomial $g(r, s) = f(0, -r - s, 0, rs)$ which is non-negative iff the roots of

$$X^4 - (r + s)X^2 + rs = (X^2 - r)(X^2 - s)$$

are all real, In other words, $g(r, s)$ is non-negative if and only if r and s are. This implies that

$$0 \geq \lim_{s \to 0^-} g(r, s) = g(r, 0) = \lim_{s \to 0^+} g(r, s) \geq 0,$$

i.e. $g(r, 0) = 0$ for any non-negative r. But then, the polynomial $g(R, 0)$ must be zero since it has infinitely many roots, so $g(r, 0)$ is also zero (and in particular non-negative) for negative r which is a contradiction. ■

Appendix C

Linear Algebra

C.1 Vector Spaces

Exercise C.1.1*. Prove Proposition C.1.3.

Solution

Let $u_1, \dots, u_k$ be linearly independent elements of the n-dimensional vector space V. Proceed as follow to complete it into a basis: as long as it does not generate everything, add one element that is not generated (and thus linearly independent with the previous ones). This process must stop since $n+1$ vectors are always linearly dependent by Proposition C.1.2.

For the second part, let $u_1, \dots, u_k$ be a generating family of elements and suppose without loss of generality that $u_1, \dots, u_m$ is a maximal subset of linearly independent elements. This is a basis, since every other u_k can be represented as a linear combination of them (and thus all of V too). Indeed, since $u_1, \dots, u_m, u_k$ are linearly dependent for $k > m$, we have $au_m + \sum_{i=1}^{m} a_i u_i = 0$ for some $a_i \in K$. Since $u_1, \dots, u_m$ are linearly independent, a must be non-zero and we get

$$u_m = -\sum_{i=1}^{m} \frac{a_i}{a} u_i$$

as wanted. ■

C.2 Linear Maps and Matrices

Exercise C.2.1*. Prove that $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ but $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.

Solution

We have

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1\cdot 1 + 0\cdot 0 & 1\cdot 1 + 0\cdot 0 \\ 0\cdot 1 + 0\cdot 0 & 0\cdot 1 + 0\cdot 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1\cdot 1 + 1\cdot 0 & 1\cdot 0 + 1\cdot 0 \\ 0\cdot 1 + 0\cdot 0 & 0\cdot 0 + 0\cdot 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

■

Exercise C.2.2*. Prove that matrix multiplication is *distributive* over matrix addition, i.e. $A(B+C) = AB + AC$ and $(A+B)C = AC + BC$ for any A, B, C of compatible dimensions.

Solution

Let $A = (a_{i,j})$, $B = (b_{i,j})$ and $C = (c_{i,j})$. Then, the (i,j) coordinate of $A(B+C)$ is

$$\sum_k a_{i,k}(b_{k,j} + c_{k,j})$$

which is equal to $\sum_k a_{i,k}b_{k,j} + \sum_k a_{i,k}c_{k,j}$, i.e. the (i,j) coordinate of $AB + AC$. The right-distributivity is completely analogous by symmetry of the left and right multiplication. ■

C.3 Determinants

Exercise C.3.1. Prove that an $m \times n$ matrix can only have a right-inverse if $m < n$, and only a left-inverse if $m > n$. When does such an inverse exist?

Solution

By symmetry, it suffices to consider right-inverses. Suppose that a matrix A has dimensions $m \times n$ and is right-invertible. Consider the surjective linear map from $K^{n\times m}$ to $K^{m\times m}$ defined by $B \mapsto AB$. By surjectivity, $mn \geq m^2$, i.e. $n \geq m$ as wanted.

For the converse, we shall refine a bit our original argument. Note that each column of AB is the sum of linear combinations of the columns of A: if $A^1, \ldots, A^n$ are the columns of A and $B = (b_{i,j})$, then

$$\sum_i b_{i,k}A^i$$

is the kth column of AB. Hence, A has a right-inverse if and only if $n \geq m$ and its columns are linearly independent. ■

Exercise C.3.2*. Prove that $(AB)^\mathsf{T} = B^\mathsf{T}A^\mathsf{T}$ for any $n \times n$ matrices A, B.

Solution

Let $A = (a_{i,j})$ and $B = (b_{i,j})$. The (i,j) coordinate of AB is $\sum_k a_{i,k}b_{k,j}$ so the (i,j) coordinate of its transpose is $\sum_k a_{j,k}b_{k,i} = \sum_k b_{k,i}a_{j,k}$ which is also the (i,j) coordinate of $B^\mathsf{T}A^\mathsf{T}$. ■

Exercise C.3.3. Prove this identity.

Solution

We have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} ad + b(-c) & a(-b) + ba \\ cd + d(-c) & c(-b) + da \end{bmatrix} = \begin{bmatrix} ad - bc & 0 \\ 0 & ad - bc \end{bmatrix} = (ad - bc)I_2.$$

■

Exercise C.3.4*. Prove that $\det I_n = 1$.

Solution

As always, by induction. From the definition of the determinant, we have $\det I_n = 1 \cdot \det I_{n-1} + 0 \cdot \ldots = \det I_{n-1}$ and $\det I_1 = 1$. ■

Exercise C.3.5*. Prove that the determinant of a matrix with a zero column is zero.

Solution

Suppose that the kth column M^k of M is zero. By Proposition C.3.1 (with $t = 0$), we have

$$\det M = \det_0^k(A) = 0 \det_0^k(M) = 0.$$

■

Exercise C.3.6. Prove that the determinant of a non-invertible matrix is 0.

Solution

Suppose that the columns of M are linearly dependent, i.e. $\sum_i a_i M^i = 0$ for some $a_i \in K$ with $a_k \neq 0$. Then,

$$0 = \det_0^k(M) = \sum_i a_i \det_{M^i}^k(M)$$

by Exercise C.3.5* and Proposition C.3.1. Now, by Proposition C.3.3, all the determinants vanish except the one with $i = k$. Thus, we get $0 = a_k \det M$ which means $\det M = 0$ as wanted. ■

Exercise C.3.7*. Prove that an upper triangular matrix is invertible if and only if its determinant is non-zero, i.e. if the elements on its diagonal are non-zero.

Solution

Let α_i denote the ith element on the diagonal (i.e. the (i, i) coordinate). First, suppose that $\alpha_i \neq 0$ for every i and that

$$\sum_{i=1}^{n} a_i M^i = 0$$

for some $a_i \in K$ not all zero. Consder the least k such that $a_k \neq 0$ and let α denote the (k, k) coordinate of M. The kth coordinate of $\sum_{i=1}^n a_i M^i$ is $\sum_{i=1}^k a_i \alpha_i = a_k \alpha_k$ since the $a_i = 0$ for $i < k$. This means that $a_k = 0$ which contradicts our assumption.

For the converse, let k be such taht $\alpha_k = 0$. Then, the columns $M^k, M^{k+1}, \ldots, M^n$ all have the top k coordinates zero. Thus, we can view them as vectors with $n - k$ coordinates. We have $n - k + 1$ vectors in a space of dimension $n - k$ so they must be linearly dependent. ■

Exercise C.3.8. Prove that $\overline{\mathbb{Z}}$ is *integrally closed*, meaning that, if f is a monic polynomial with algebraic integer coefficients, then any of its root is also an algebraic integer. (This is also Exercise 1.5.22†.)

Solution

Let $f = X^n + \alpha_{n-1}X^{n-1} + \ldots + \alpha_0$ be a monic polynomial with algebraic integer coefficients and let β be one of its roots. Then,

$$M = \mathbb{Z}[\alpha_{n-1}, \ldots, \alpha_0, \beta]$$

is a finitely generated $\mathbb{Z}$-module such that $\beta M \subseteq M$, so β is an algebraic integer. ■

Exercise C.3.9*. Prove Lemma C.3.1.

Solution

By induction:

$$\begin{aligned}\det A &= \sum_{i=1}^{n}(-1)^{i-1}a_{i,1}\det A_{i,1}\\ &= \sum_{i=1}^{n}(-1)^{i-1}a_{i,1}\sum_{\sigma}\varepsilon(\sigma)a_{2,\sigma(2)}\cdot\ldots\cdot a_{n,\sigma(n)}\\ &= \sum_{i=1}^{n}\sum_{\sigma}(-1)^{i-1}\varepsilon(\sigma)a_{i,1}a_{\sigma(2),2}\cdot\ldots\cdot a_{\sigma(n),n}\end{aligned}$$

where the sum is over the bijections $\sigma : [n] \setminus \{1\} \to [n] \setminus \{i\}$. This has the desired form. Finally, note that the sign of $a_{1,1}\cdot\ldots\cdot a_{n,n}$ is $(-1)^{1-1}$ times the sign of $a_{2,2}\cdot\ldots\cdot a_{n,n}$ which is 1 as wanted. ■

Exercise C.3.10*. Prove that the number of derangements of $[m]$ is

$$\sum_{i=0}^{m}\frac{(-1)^i m!}{i!}$$

and that this number is odd if m is even and even if m is odd.

Solution

We shall instead count the number of permutations with at least one fixed point. We use the principle of *inclusion-exclusion*. For a fixed k, there are $(n-1)!$ permutations σ satisfying $\sigma(k) = k$. Thus, we count $n \cdot (n-1)! = n!$ permutations. However, we have counted some permutations twice: the ones which have at least two fixed points. Thus, we remove $\binom{n}{2}\cdot(n-2)!$ from our count (we need to choose two fixed points and then permute the remaining $n-2$ elements arbitrarily). But now, we have removed some permutations too many times: the ones with at least three fixed points, so we must add $\binom{n}{3}\cdot(n-3)!$ to our count, etc. At the end, we get

$$\sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}(n-k)! = \sum_{k=1}^{n}(-1)^{k-1}\frac{n!}{k!}.$$

If we subtract this from $n!$ (the total number of permutations), we get exactly the wanted formula. ■

Exercise C.3.11*. Prove that the signature is negated when one exchanges two values of σ (i.e. compose a transposition with σ).

Solution

Say that we exchange $\sigma(i)$ with $\sigma(j)$, i.e. we apply the transposition $\tau = \tau_{\sigma(i),\sigma(j)}$. We have

$$\begin{aligned}\varepsilon(\sigma)/\varepsilon(\tau\circ\sigma) &= \frac{\frac{\sigma(i)-\sigma(j)}{j-i}\cdot\prod_{k\neq i}\frac{\sigma(k)-\sigma(j)}{k-i}\cdot\prod_{k\neq j}\frac{\sigma(k)-\sigma(i)}{k-j}}{\frac{\sigma(j)-\sigma(i)}{j-i}\cdot\prod_{k\neq i}\frac{\sigma(k)-\sigma(i)}{k-i}\cdot\prod_{k\neq j}\frac{\sigma(k)-\sigma(j)}{k-j}}\\ &= \frac{\frac{\sigma(i)-\sigma(j)}{j-i}}{\frac{\sigma(j)-\sigma(i)}{j-i}}\\ &= -1\end{aligned}$$

as wanted. ■

Exercise C.3.12*. Prove that transpositions $\tau_{i,j} : i \leftrightarrow j$ and $k \mapsto k$ for $k \neq i, j$ generate all permutations (through composition).

Solution

By induction: we start with $\tau_{n,\sigma^{-1}(n)}$ so that $\sigma \circ \tau_{n,\sigma^{-1}(n)}(n) = n$. Then, ignoring the last element of $\sigma \circ \tau_{1,\sigma^{-1}(1)}$, it is a permutation of $[n-1]$ so a composition of transpositions. We get the wanted result by applying $\tau_{n,\sigma^{-1}(n)} = \tau^{-1}_{n,\sigma^{-1}(n)}$ to both sides. ■

Exercise C.3.13*. Prove Theorem C.3.3.

Solution

We proceed as in Exercise C.3.9*: we have

$$\det(a_{i,j}) = \sum_{i=1}^{n}\sum_{\sigma}(-1)^{i-1}\varepsilon(\sigma)a_{i,1}a_{\sigma(2),2}\cdot\ldots\cdot a_{\sigma(n),n}$$

where the sum is over the bijections $\sigma : [n]\setminus\{1\} \to [n]\setminus\{i\}$. It remains to prove that $\varepsilon(\sigma) = (-1)^{\sigma(1)-1}\varepsilon(\sigma')$ where σ' denotes the bijection $[n]\setminus\{1\} \to [n]\setminus\{\sigma(1)\}$ obtained by forgetting the first element. This is easy: we want to count the number of inversions of σ which are not inversions of σ'. This is exactly the number of inversions $(k, 1)$ since 1 is the only difference bewteen σ and σ'. Since $k > 1$ for each $k \neq 1$, the number of such inversions is the number of $\sigma(k) < \sigma(1)$, i.e. $\sigma(1) - 1$ as wanted. ■

Exercise C.3.14*. Prove that $\det A = \det A^{\mathsf{T}}$ for any square matrix A.

Solution

Our formula from Theorem C.3.3 is symmetric in rows and columns:

$$\begin{aligned}\det A &= \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{\sigma(1),1}\cdot\ldots\cdot a_{\sigma(n),n}\\ &= \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma^{-1}) a_{1,\sigma^{-1}(1)}\cdot\ldots\cdot a_{n,\sigma^{-1}(n)}\\ &= \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) a_{1,\sigma(1)}\cdot\ldots\cdot a_{n,\sigma(n)}\\ &= \det A^{\mathsf{T}}.\end{aligned}$$

■

Exercise C.3.15*. Prove that $D_k(I_{n-1}) = (-1)^{k-1}$.

Solution

Consider the $n\times n$ matrix I we defined D_k with and substitute $A = I_{n-1}$. We will exchange $k-1$ columns to transform it into I_n, thus getting a determinant of $(-1)^{k-1}\det I_n = (-1)^{k-1}$ as wanted.

Note that I is already almost equal to I_n: its first column should be kth and the 1 to k ones should be shifted to the left. Here is how we do this shift using transpositions.

We first exchange the first column of the with the second one so that $a_{1,1}=1$ becomes the $(1,1)$ coordinate of I, then we exchange the (new) second column with the third one so that $a_{2,2}=1$ becomes the $(2,2)$ coordinate of I, etc., until we exchange the $k-1$th column with the kth one so that $a_{k,k}=1$ becomes the (k,k) coordinate of I. Thus, the $k-1$th column, which was originally the first one, becomes the kth one as wanted. ■

Exercise C.3.16. Prove that the determinant is multiplicative by using the explicit formula of Theorem C.3.3.

Solution

Write $C = AB$, so that

$$C^k = b_{1,k}A^1 + \ldots + b_{n,k}A^n.$$

Then, by multilinearity of the determinant,

$$\begin{aligned}\det C &= \det(b_{1,1}A^1+\ldots+b_{n,1}A^n,\ldots,b_{1,n}A^1+\ldots+b_{n,n}A^n)\\ &= \sum_{\sigma\in\mathfrak{S}_n} b_{\sigma(1),1}\cdot\ldots\cdot b_{\sigma(n),n}\det(A^{\sigma(1)},\ldots,A^{\sigma(n)})\\ &= \sum_{\sigma\in\mathfrak{S}_n} \sigma(\varepsilon) b_{\sigma(1),1}\cdot\ldots\cdot b_{\sigma(n),n}\det(A^1,\ldots,A^n)\\ &= \det B\det A\end{aligned}$$

where the second-to-last equality comes from Remark C.3.4. ■

Exercise C.3.17. Let L/K be a finite extension. Prove that the determinant of the K-linear map $L\to L$ defined by $x\mapsto x\alpha$ is the norm of α defined in Definition 6.2.3.

Solution

We first treat the case where $L = K(\alpha)$. Consider the basis $1, \alpha, \ldots, \alpha^{n-1}$ of L and let $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ be the minimal polynomial of α. The matrix corresponding to $x \mapsto x\alpha$ in this basis is

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & -a_0 \\ 1 & 0 & 0 & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ 0 & 0 & 1 & \cdots & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -a_{n-1} \end{bmatrix}.$$

Using Theorem C.3.3, we see that this is $-\varepsilon(\sigma)a_0$, where σ is the cycle $(1, 2, \ldots, n)$. Hence, we need to prove that $\varepsilon(\sigma) = (-1)^{n-1}$ since the product of the conjugates of α is $(-1)^n a_0$ by Vieta's formulas. This follows from the fact that

$$\sigma = (1, n) \cdot \ldots \cdot (1, 3)(1, 2)$$

is a product of $n - 1$ transpositions.

Now here is what we can do for the general case. Note that the norm is multiplicative. Indeed, for any linear maps φ and ψ,

$$\det \varphi \cdot \det \psi = \det \varphi \circ \psi$$

since the determinant is multiplicative. Since the composite of $x \mapsto \alpha x$ and $x \mapsto \beta x$ is $x \mapsto \alpha\beta x$, the norm of $\alpha\beta$ is the norm of α times the norm of β. Then, pick a primitive element γ of L/K such that α/γ is also a primitive element. We can do this since

$$\sigma(\alpha)/\sigma(\gamma) = \alpha/\gamma \iff \sigma(\gamma) = \gamma \cdot \frac{\sigma(\alpha)}{\alpha}$$

is false for $\gamma = a\delta + b$ for well-chosen $a, b \in K$ and a fixed primitive element δ. Thus, from the first observation, we get

$$\begin{aligned} N_{L/K}(\alpha) &= N_{L/K}(\gamma) N_{L/K}(\alpha/\gamma) \\ &= \prod_{\sigma \in \mathrm{Emb}_K(L)} \sigma(\gamma) \prod_{\sigma \in \mathrm{Emb}_K(L)} \sigma(\alpha/\gamma) \\ &= \prod_{\sigma \in \mathrm{Emb}_K(L)} \sigma(\alpha) \end{aligned}$$

as wanted. ■

Exercise C.3.18*. Prove that $\operatorname{adj} AA = (\det A) I_n$.

Solution

Set $(b_{i,j}) = \operatorname{adj} AA$. This time, we have

$$b_{i,j} = \sum_{k=1}^{n} (-1)^{i+k} \det(A_{k,i}) a_{k,j}.$$

When $i = j$ this is the column expansion of the determinant of A which is $\det A$, and when $i \neq j$ this is $(-1)^{i+j}$ times the determinant of the matrix obtained by replacing the ith column of A by its jth column. This matrix has two identical columns so its determinant is zero as wanted. ■

C.4 Linear Recurrences

Exercise C.4.1. Prove that Theorem C.4.1 holds in a field K of characteristic $p \neq 0$ as long as the multiplicities of the roots of the characteristic polynomial are at most p. In particular, for a fixed characteristic equation, it holds for sufficiently large p.

Solution

The only thing to check is that if $f_i(n) = 0$ for all $n \in \mathbb{Z}$ and f_i has less than the multiplicity of α_i so less than p then $f_i = 0$. This is true because $\mathbb{Z}$ reduces to p elements in a field of characteristic $p \neq 0$ so f_i has p roots which is more than its degree and is thus zero. ■

C.5 Exercises

Vector Spaces and Bases

Exercise C.5.1 (Grassmann's Formula)**.** Let U be a vector space and V, W be two finite-dimensional subspaces of U. Prove that

$$\dim(V + W) = \dim V + \dim W - \dim(V \cap W).$$

Solution

Let $u_1, \ldots, u_k$ be a basis of $V \cap W$. Complete it to a basis $u_1, \ldots, u_k, v_1, \ldots, v_m$ of V and a basis $u_1, \ldots, u_k, w_1, \ldots, w_n$ of W. We claim that

$$u_1, \ldots, u_k, v_1, \ldots, v_m, w_1, \ldots, w_n$$

is a basis of $V + W$. It clearly spans all of $V + W$ so it remains to check that it's linearly independent. If

$$\sum_{i=1}^{k} a_i u_i + \sum_{i=1}^{m} b_i v_i + \sum_{i=1}^{m} c_i w_i = 0,$$

then $\sum_{i=1}^{m} b_i v_i$ is both in V and W so is in $V \cap W$. This means that it's a linear combination of the u_i, but by construction this implies $b_1 = \ldots = b_m = 0$ since the u_i and v_i are linearly independent (they form a basis of V together). By symmetry, $c_1 = \ldots = c_n = 0$. Finally, this forces $a_1 = \ldots = a_k = 0$ too.

We conclude that

$$\dim(V + W) = k + m + n = (k + m) + (k + n) - k = \dim V + \dim W - \dim V \cap W.$$

■

Exercise C.5.3† **.** Given a vector space V of dimension n, we say a subspace H of V is a *hyperplane* of V if it has dimension $n - 1$. Prove that H is a hyperplane of K^n if and only if there are elements $a_1, \ldots, a_n \in K$ not all zero such that

$$H = \{(x_1, \ldots, x_n) \in K^n \mid a_1 x_1 + \ldots + a_n x_n = 0\}.$$

Solution

Clearly, if H is defined as the zero set of $a_1 X_1 + \ldots + a_n X_n$ then H has dimension $n - 1$ since,

assuming without loss of generality that $a_n \neq 0$, we get a bijective map $K^{n-1} \to H$ given by

$$(x_1, \ldots, x_{n-1}) \mapsto \left(x_1, \ldots, x_{n-1}, -\frac{a_1 x_1 + \ldots + a_n x_n}{a_1}\right).$$

For the converse, pick a linear map φ mapping H to 0 without being identically 0. Then,

$$(x_1, \ldots, x_n) = x \in H \iff \varphi(x) = 0 \iff \sum_{i=1}^{n} x_i \varphi(e_i) = 0$$

where e_i is the canonical basis of K^n: 0 everywhere except in its ith coordinate where there is a 1. ■

Determinants

Exercise C.5.6. Let $a_0, \ldots, a_{n-1}$ be elements of K and ω a primitive nth root of unity. Prove that the *circulant determinant*

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{bmatrix}$$

is equal to

$$f(\omega) f(\omega^2) \cdot \ldots \cdot f(\omega^{n-1})$$

where $f = a_0 + \ldots + a_{n-1} X^{n-1}$. Deduce that this determinant is congruent to $a_0 + \ldots + a_{p-1}$ modulo p when $n = p$ is prime and $a_1, \ldots, a_p$ are integers.

Solution

Let A be the circulant matrix. We shall imitate the proof of Theorem C.3.2: we need to prove that $\det A$ is zero when $a_0 = -(a_1\omega + \ldots + a_{n-1}\omega^{n-1})$ for any root of unity ω. This shows that the product $f(\omega)$ divides the determinant as a polynomial in a_0. Then, by looking at the coefficient of a_0^n, we can conclude that they are in fact equal. To show that the determinant vanishes for these a_0, note that the following linear combination of the columns is zero

$$\sum_{i=1}^{n} \omega^i A^i = 0.$$

Alternatively, one could note that $A = f(J)$, where is the circulant matrix with $a_1 = 1$ and $a_0 = a_2 = a_3 = \ldots = a_{n-1} = 0$. We can check that all nth roots of unity are eigenvalues of J. To finish, Exercise C.5.15 implies that the eigenvalues of $f(J)$ are the $f(\omega)$, and the determinant is their product as wanted. ■

Exercise C.5.7 (Cramer's Rule)**.** Consider the system of equations $MV = X$ where M is an $n \times n$ matrix and $V = (v_i)_{i \in [\![1,n]\!]}$ and $X = (x_i)_{i \in [\![1,n]\!]}$ are column vectors. Prove that, for any $k \in [\![1, n]\!]$, v_k is equal to $\det M / \det M_{k,X}$, where $M_{k,X}$ denotes the matrix $[M^1, \ldots, M^{k-1}, X, M^{k+1}, \ldots, M^n]$ obtained from M by replacing the kth column by X.

Solution

Note that this formula is linear in XX since the determinant is multilinear. Since the kth coordinate of the formula $M^{-1}V$ is also linear in X, we just need to check that both formulas

agree on a basis of K^n. This is easy: when $X = M^k$ we get $v_k = 1$ and $v_i = 0$ for $i \neq k$ which is indeed the solution to $MV = M^k$. Since these form a basis of K^n as M is invertible, we are done. ■

Exercise C.5.8†. Let $(u_n)_{n\geq 0}$ be a sequence of elements of a field K. Suppose that the $(m+1)\times(m+1)$ determinant $\det(u_{n+i+j})_{i,j\in[\![0,m]\!]}$ is 0 for all sufficiently large n. Prove that there is some N such that $(u_n)_{n\geq N}$ is a linear recurrence of order at most m.

Solution

We proceed by induction on m (it's trivial when $m = 1$). More precisely, we prove that, under the assumptions of the problem, if the $(m-1)\times(m-1)$ determinant $\det(u_{n+i+j})_{i,j\in[\![0,m-1]\!]}$ vanishes for one value of n, then it vanishes for all the next ones which means that there exists some N for which $(u_n)_{n\geq N}$ is a linear recurrence of order at most $m-1 \leq m$. If it doesn't vanish for $n \geq N$, then $(u_{n+i+j})_{i,j\in[\![0,m]\!]}$ has rank $m-1$ by definition of the rank (see Exercise C.5.26†), and, more precisely, its first m rows as well as its first last rows are linearly independent and generate the same hyperplane H. Notice that the last m rows of $(u_{n+i+j})_{i,j\in[\![0,m]\!]}$ are the first m rows of $(u_{n+1+i+j})_{i,j\in[\![0,m]\!]}$ so this hyperplane H is always the same. Finally, with Exercise C.5.3†, we conclude that

$$a_0u_n + a_1u_{n+1} + \ldots + a_{n+m}u_{n+m} = 0$$

for all $n \geq N$, i.e. $(u_n)_{n\geq N}$ is a linear recurrence of order at most m as claimed.

It remains to prove that, if $\det(u_{n+i+j})_{i,j\in[\![0,m-1]\!]} = 0$, then $\det(u_{n+1+i+j})_{i,j\in[\![0,m-1]\!]} = 0$ as well. Hence, suppose that the first determinant is 0, i.e. that there is a linear dependence between the rows. If this dependence does not involve the first row, then it also creates a linear dependence in the rows of the second matrix which implies that its determinant is 0 as wanted. Otherwise, the first row is a linear combination of the $m-1$ next ones. This implies that the first row of $(u_{n+i+j})_{i,j\in[\![0,m]\!]}$ is a linear combination of the $m-1$ next ones as well as a vector of the form $(0,\ldots,0,a)$ for some $a \in K$. Then, by performing row operations, we find

$$0 = (u_{n+i+j})_{i,j\in[\![0,m]\!]} = \pm\begin{vmatrix} 0 & \cdots & 0 & a \\ u_{n+1} & \cdots & u_{n+m} & u_{n+m+1} \\ \vdots & \vdots & \ddots & \vdots \\ u_{n+m} & \cdots & u_{n+2m-1} & u_{n+2m} \end{vmatrix} = \pm a \det\det(u_{n+1+i+j})_{i,j\in[\![0,m-1]\!]}$$

by expanding with respect to the first row. We are done. ■

Exercise C.5.9†. Let $f_1,\ldots,f_n : \mathbb{N} \to \mathbb{C}$ be functions which grow at different rates, i.e.

$$\frac{f_1(m)}{f_2(m)}, \frac{f_2(m)}{f_3(m)}, \ldots, \frac{f_{n-1}(m)}{f_n(m)} \underset{m\to\infty}{\longrightarrow} 0$$

Prove that there exists n integers $m_1,\ldots,m_n$ such that the tuples

$$(f_1(m_1),\ldots,f_n(m_1)),\ldots,(f_1(m_n),\ldots,f_n(m_n))$$

are linearly independent over $\mathbb{C}$.

Solution

We proceed by induction on n. It is of course trivial when $n = 1$. Fix $m_1,\ldots,m_{n-1}$ such that

$$(f_1(m_1),\ldots,f_{n-1}(m_1)),\ldots,(f_1(m_{n-1}),\ldots,f_{n-1}(m_{n-1}))$$

are linearly independent, i.e. such that the determinant

$$C = \begin{bmatrix} f_1(m_1) & \cdots & f_{n-1}(m_1) \\ \vdots & \ddots & \vdots \\ f_1(m_{n-1}) & \cdots & f_{n-1}(m_{n-1}) \end{bmatrix}$$

is non-zero. We wish to show that there is some m_n such that

$$\begin{bmatrix} f_1(m_1) & \cdots & f_n(m_1) \\ \vdots & \ddots & \vdots \\ f_1(m_{n-1}) & \cdots & f_n(m_n) \end{bmatrix}$$

is non-zero. Expand it with respect to the last column to get

$$\sum_{i=1}^{n} C_i f_i(m_n)$$

where C_i are constants and $C_n = C$. Since f_n dominates all other f_i and C_n is non-zero by construction, this is non-zero for sufficiently large m as wanted. ■

Algebraic Combinatorics

Exercise C.5.12†. Let $A_1, \ldots, A_{n+1}$ be non-empty subsets of $[n]$. Prove that there exist disjoint subsets I and J of $[n+1]$ such that

$$\bigcup_{i \in I} A_i = \bigcup_{j \in J} A_j.$$

Solution

Identity each subset $A_i \subseteq [n]$ with the vector $v_i \in \mathbb{R}^n$ whose ith coordinate is 1 if $i \in S$ and 0 otherwise. This makes the set of subsets of $[n]$ into a subset of a $\mathbb{R}$-vector space of dimension n. (It's not a vector space itself, though it would be if we chose $\mathbb{F}_2$ instead of $\mathbb{R}$. $\mathbb{F}_2$ is usually very useful in algebraic combinatorics but doesn't work here.) We have $n+1$ vectors in a space of dimension n so they must be linearly dependent, say

$$\sum_{i=1}^{n+1} c_i v_i = 0.$$

Now consider the set I of indices of positive c_i, and the set J of indices of negative c_i. We have

$$\sum_{i \in I} |c_i| v_i = \sum_{j \in J} |c_j| v_j$$

which gives us $\bigcup_{i \in I} A_i = \bigcup_{j \in J} A_j$ as wanted. In addition, I and J are disjoint by construction. ■

The Characteristic Polynomial and Eigenvalues

Exercise C.5.15 (Characteristic Polynomial)**.** Let K be an algebraically closed field. Let $M \subseteq K^{n \times n}$ be an $n \times n$ matrix. Define its *characteristic polynomial* as $\chi_M = \det(M - XI_n)$. Its roots (counted with multiplicity) are called the *eigenvalues* $\lambda_1, \ldots, \lambda_n \in K$ of M. Prove that $\det M$ is the product of the eigenvalues of M, and that $\operatorname{Tr} M$ is the sum of the eigenvalues. In addition, prove that λ is an eigenvalue of M if and only if there is a non-zero column vector V such that $MV = \lambda V$ (in other words, M acts like a homothety on V). Conclude that, if $f \in \mathbb{C}[X]$ is a polynomial, the eigenvalues of

$f(M)$ are $f(\lambda_i)$ (with multiplicity). (We are interpreting $1 \in K$ as I_n for $f(M)$ here, i.e., if $f = X+1$, $f(M)$ is $M + I_n$.) In particular, the eigenvalues of $M + I\alpha$ are $\lambda_1 + \alpha, \dots, \lambda_n + \alpha$, and the eigenvalues of M^k are $\lambda_1^k, \dots, \lambda_n^k$.[1]

Solution

The first part follow simply from expanding the determinant and using Vieta's formulas. For the second one, there is a non-zero vector V such that $MV = \lambda V \iff (M - \lambda I_n)V$ if and only if $\ker(M - \lambda I_n)$ is non-trivial, which is equivalent to $\det(M - \lambda I_n) = 0$. Now, note that $MV = \lambda V$ gives $M^k V = \lambda^k V$ and thus, by taking linear combinations, $f(M)V = f(\lambda)V$. This shows that the $f(\lambda)$ are eigenvalues of M. To account for the multiplicity, note that we have established the result when χ_M has simple roots, and that the general results follows by density, analytical or algebraic. We present the proof by algebraic density (more technically, *Zariski density*) since it works over any field, which is similar to Remark C.3.7.

Note that the equality $\chi_{f(M)} = \prod_{k=1}^n f(\lambda_i) - X$ is a polynomial equality in the coefficients of f and the coordinates of M by the fundamental theorem of symmetric polynomials. Let Δ_f by the discriminant of $\prod_{k=1}^n f(\lambda_i) - X$, i.e. $\pm \prod_{i \neq j} f(\lambda_i) - f(\lambda_j)$ which is again polynomial in the coefficients of f and the coordinates of M. We have shown that

$$(\chi_{f(M)} - \prod_{k=1}^n f(\lambda_i) - X)\Delta_f$$

always takes the value zero. Hence, it must be the zero polynomial. If we show that Δ_f is non-zero, we are hence done. Choosing $f = X$, this amounts to finding a matrix with distinct eigenvalues. This is not very hard: we can fix all coordinates of M except one and let it vary. The determinant then varies affinely in this coordinates, say it is $ua + v$, where a is the varying coordinate. By induction, we can choose u to have simple roots. A multiple root of $ua + v$ would also be a root of u', but this is impossible for large a unless this root is a common root of u and v, which must thus have multiplicity one: this is a contradiction. (Alternatively, we can consider the matrix J from Exercise C.5.6.) ■

Exercise C.5.16 (Cayley-Hamilton Theorem)**.** Prove that, for any $n \times n$ matrix M, $\chi_M(M) = 0$ where χ_M is the characteristic polynomial of M and $0 = 0I_n$. Conclude that, if every eigenvalue of M is zero, M is *nilpotent*, i.e. $M^k = 0$ for some k.[2]

Solution

Using Proposition C.3.7, we get

$$(M - XI_n)\operatorname{adj}(M - XI_n) = \operatorname{adj}(M - XI_n)(M - XI_n) = \chi_M I_n. \qquad (*)$$

We wish to substitute M for X in $M - XI_n$, but we can only do that if M commutes with the coefficients of $\operatorname{adj}(M - XI_n)$ (which are matrices). Note that this is the case since

$$XI_n \operatorname{adj}(M - XI_n) = \operatorname{adj}(M - XI_n)XI_n$$

(X is a formal variable so commutes with everything, and I_n does as well) so $M \operatorname{adj}(M - XI_n) = \operatorname{adj}(M - XI_n)M$ by $(*)$. The second part is obvious: if all eigenvalues of M are zero, then $\chi_M = \pm X^n$ so $M^n = 0$. ■

[1] One of the advantages of the characteristic polynomial is that we are able to use algebraic number theory, or more generally polynomial theory, to deduce linear algebra results, since the eigenvalues say a lot about a matrix (if we combine this with the Cayley-Hamilton theorem). See for instance Exercise C.5.18 and the third solution of Exercise C.5.19.

[2] Note that if, in the definition of χ_M, we replace det by an arbitrary multilinear form in the coordinates of M, such as the *permanent*) $\operatorname{perm}(A) = \sum_{\sigma \in \mathfrak{S}_n} a_{1,\sigma(1)} \cdot \ldots \cdot a_{n,\sigma(n)}$, the result becomes false, so we cannot just say that "$\chi_M(M) = \det(M - MI_n) = \det 0 = 0$" (this "proof" is nonsense because the scalar 0 is not the matrix 0, but the point is that this intuition is fundamentally incorrect).

Exercise C.5.19. Let p be a prime number, and G be a finite (multiplicative) group of $n \times n$ matrices with integer coordinates. Prove that two distinct elements of G stay distinct modulo p. What if the elements of G only have algebraic integer coordinates and p is an algebraic integer with all conjugates greater than 2 in absolute value?

Solution

We will present three solutions, in increasing order of non-elementariness, and of generality. Suppose that the reduction modulo p (group) morphism φ is not injective, i.e. has non-trivial kernel (see Exercise A.2.13* – this is really trivial, I'm only using this language so that you familiarise with it), say $I := I_n \neq A \subseteq \in \ker \varphi$, i.e. $A = I + pB$ for some non-zero B. Since G is a finite group, we have $A^m = I$ for $m = |G|$ by Lagrange's theorem Exercise A.3.17†. We will show that this is impossible (if fact it is equivalent to the problem: if it were possible, the group generated by M would be a counterexample). (Note that all solutions will use the assumption that $p \neq 2$ somewhere, and for a good reason: $-I \equiv I \pmod 2$.)

Here is the first solution, which works only for the first part of the problem. Let k be the greatest integer such that B/p^k has integer coordinates. Suppose first that $p \nmid m$. Then, modulo p^{k+2}, using the binomial expansion (which we can use since I and pB commute), we have

$$(I + pB)^m \equiv I + mpB \not\equiv I \pmod{p^{k+2}}$$

which is a contradiction. We will now replace B by C such that $(I + pB)^p = I + pC$. That, way, m gets replaced by m/p, and by iterating this process we will eventually reach a $p \nmid m$ which is a contradiction. However, we need to prove that $C \neq 0$ too. Thus, suppose that $(I + pB)^p = I$. We then have

$$(I + pB)^m \equiv I + mpB + \frac{m(m-1)}{2} p^2 B^2 equiv I + p^2 B \not\equiv I \pmod{p^{k+3}}$$

since p is odd, which is also a contradiction.

We now present the second solution. Let $|M|$ denote the maximum of the absolute value of the coordinates of a matrix M. Since $A^m = I$ for some m, $|A^k|$ is bounded when k varies, say by C. We have

$$|(pB)^r = |(I - A)^r| \leq \sum_{k=0}^{r} \binom{r}{k} |A^r| \leq C 2^r.$$

However, the left hand side is divisible by p^n so is at least p^n unless it is 0. Since $p > 2$, by taking r sufficiently large, we get $|B^r| = 0$, i.e. $B^r = 0$: B is nilpotent. When p is only an algebraic integer with all conjugates greater than 2, the same argument works: the coordinates of B^r/p^r are algebraic integers with absolute value less than $C2^r/p^r$ so less than 1 for large r. However, the same goes for their conjugates by assumption. Since the only algebraic integer whose conjugates are all strictly in the unit disk is 0 (by looking at the constant coefficient of its minimal polynomial), we get $B^r = 0$ for large r as wanted.

Consider k such that $B^k \neq 0$ but $B^{k+1} = 0$. Since $B \neq 0$, we have $k \geq 1$. By expanding $(I + pB)^m = I$, we get

$$pmB + p^2 \frac{m(m-1)}{2} B^2 + \ldots = 0.$$

Finally, by multiplying this equation by B^{k-1}, we get $pmB^k = 0$ which implies $m = 0$ and is a contradiction.

Finally, the third solution uses more advanced linear algebra. Let β be an eigenvalue of B. Then, $\alpha = 1 + p\beta$ is an eigenvalue of A which is congruent to 1 modulo p. Further, since A^m, we have $\alpha^m = 1$ so it is a root of unity. This implies that $\beta = \frac{\alpha - 1}{p}$ has module less than 1 since $p > 2$. This is also true for all its conjugates. Thus, the constant coefficient of its minimal polynomial must be 0, i.e. $\beta = 0$. Hence, all eigenvalues of B are zero, which implies that B is nilpotent by Exercise C.5.16. We finish as in the previous solution. ■

Miscellaneous

Exercise C.5.20 (USA TST 2019)**.** For which integers n does there exist a function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ such that

$$f, f + \mathrm{id}, f + 2\mathrm{id}, \ldots, f + m\mathrm{id}$$

are all bijections?

Solution

There exists such a function if and only if all prime factors of n are greater than $m+1$. In that case, it is clear that $f = \mathrm{id}$ works. Now suppose that f has a prime factor $p \leq m+1$. Pick p to be minimal, and suppose without loss of generality that $m = p-1$. For $1 \leq k \leq m$, since f and $f + k\mathrm{id}$ are both bijections, we have

$$\sum_{x=1}^{n} g(x)^m \equiv \sum_{x=1}^{n} (g(x) + kx)^m = \sum_{i=0}^{m} \binom{m}{i} k^{m-i} \sum_{x=1}^{n} g(x)^i x^{m-i},$$

i.e.

$$\sum_{i=0}^{m-1} \binom{m}{i} k^{m-i} \sum_{x=1}^{n} g(x)^i x^{m-i} \equiv 0.$$

Thus, we have a linear system in the k^{m-i} with solution $x_i = \binom{m}{i} \sum_{x=1}^{n} g(x)^i x^{m-i}$. By Vandermonde, the determinant of the matrix $M = (k^{m-i})_{k,i}$ is

$$\prod_{1 \leq i < j \leq m} i - j$$

which is invertible modulo n since p is the smallest prime factor of n by assumption and $m = p-1$. Thus, by Exercise C.3.18*, M is invertible modulo n which implies that our system has exactly one solution. Since $x_0 \equiv \ldots \equiv x_{m-1} = 0$ is of course the trivial solution, this must in fact be the case. In particular,

$$x_0 = \sum_{x=1}^{n} x^{p-1}$$

is zero. We will prove that this is impossible. If $p = 2$, this sum is $\frac{n}{n-1}2$ so $n \mid \frac{n(n-1)}{2}$ which implies that n is odd and is a contradiction.

Now suppose that p is odd. Let $k = v_p(n)$. Since this sum is congruent to

$$\frac{n}{p^k} \sum_{x=1}^{p^k} x^{p-1}$$

modulo p^k, it suffices to prove that $p^k \nmid \sum_{x=1}^{p^k} x^{p-1}$. Let g be a primitive root modulo p^k, there exists one by Exercise 3.5.18†. Then,

$$\sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} x^{p-1} \equiv \sum_{k=1}^{p^k - 1} g^{k(p-1)} = \frac{g^{p^{k-1}(p-1)^2} - 1}{g^{p-1} - 1}.$$

By LTE 3.4.3, the p-adic valuation of this is $k - 1 < k$. To take care of the terms of the sum which are divisible by p, simply note that

$$v_p \left(\sum_{v_p(x) = \ell, x \in \mathbb{Z}/p^k\mathbb{Z}} x^{p-1} \right) = (p-1)\ell + v_p \left(\sum_{x \in (\mathbb{Z}/p^{k-\ell})^\times} x^{p-1} \right) = (p-1)\ell + k - \ell - 1 \geq k$$

by our previous computation. ∎

Exercise C.5.21 (Finite Fields Kakeya Conjecture, Zeev Dvir)**.** Let $n \geq 1$ an integer and $\mathbb{F}$ a finite field. We say a set $S \subseteq \mathbb{F}^n$ is a *Kakeya set* if it contains a line in every direction, i.e., for every $y \in \mathbb{F}^n$, there exists an $x \in \mathbb{F}^n$ such that S contains the line $x + y\mathbb{F}$. Prove that any polynomial of degree less than $|\mathbb{F}|$ vanishing on a Kakeya set must be zero. Deduce that there is a constant $c_n > 0$ such that, for any finite field $\mathbb{F}$, any Kakeya set of $\mathbb{F}^n$ has cardinality at least $c_n p^n$.

Solution

Let q be the cardinality of $\mathbb{F}$. The proof will be in two steps. Suppose that f is a polynomial of degree $d < q$ vanishing on a Kakeya set S. Fix any $y \in \mathbb{F}^n$. Then, for some $x \in \mathbb{F}^n$, $f(x+ty) = 0$ for any $t \in \mathbb{F}$. The polynomial $f(x+Ty)$ has more roots than its degree so is zero. Let g be the homogeneous part of f, i.e. the polynomial formed by the monomials of degree d of f. Notice that the coefficient of T^d in $f(x+Td)$ is exactly $g(y)$. Hence, $g(y) = 0$ for any $y \in \mathbb{F}^n$, which implies that $g = 0$ by Exercise A.1.7*. This contradicts the assumption that f had degree d.

For the second step, note that the dimension of the vector space V of polynomials of degree at most $q-1$ is $\binom{n+q-1}{n}$. Indeed, the monomials $X_1^{d_1} \cdot \ldots \cdot X_n^{d_n}$ for $d_1 + \ldots + d_n \leq q-1$ form a basis of this space. However, the number of such tuples is the same as the number of ways to choose n elements from $[n+q-1]$: choose $a_1 < \ldots < a_n$ and decide that $d_1 = a_1$, $d_1 + d_2 = a_2$, etc., until $d_1 + \ldots + d_n = a_n$ (this technique is usually called *stars and bars* because you have $q-1$ stars and n bars used to separate them). Now consider the linear map $T : V \to \mathbb{F}^{|S|}$ defined by $T(f) = (f(s))_{s \in S}$. If $|S| < \dim V$, it must have a non-trivial kernel by Proposition C.1.2 (or the rank-nullity theorem). This contradicts the first step.

We conclude that

$$|S| \geq \binom{n+q-1}{n} = \frac{q(q+1) \cdot \ldots \cdot (n+q-1)}{n!} \geq \frac{q^n}{n!}$$

so we can take $c_n = \frac{1}{n!}$. ■

Exercise C.5.22 (Siegel's Lemma)**.** Let $a = (a_{i,j})$ be an $m \times n$ matrix with integer coordinates. Prove that, if $n > m$, the system

$$\sum_{j=1}^{n} a_{i,j} x_j = 0$$

for $i = 1, \ldots, n$ always has a solution in integers with

$$\max_i |x_i| \leq \left(n \max_{i,j} |a_{i,j}| \right)^{\frac{m}{n-m}}.$$

Solution

Let $M = \max_{i,j} |a_{i,j}|$. Fix a constant N to be chosen later. Suppose that the integers $a_1, \ldots, a_k$ are negative while $a_{k+1}, \ldots, a_n$ are positive. Then, for any $(x_1, \ldots, x_n) \in [N]^n$, we have

$$N(a_1 + \ldots + a_k) \leq a_1 x_1 + \ldots + a_n x_n \leq N(a_{k+1} + \ldots + a_n).$$

Thus, the expression $a_1 x_1 + \ldots + a_n x_n$ can take at most $1 + N(|a_1| + \ldots + |a_n|)$ values.

Now, we return to the problem. Set $A = (a_{i,j})$. We have shown that, when $X \subseteq [N]^n$, each rows of AX can take at most $1 + NnM$ values. Thus, when X ranges through $[N]^n$, AX takes at most $(1+NnM)^m < (1+N)^m (nM)^m$ values. Since X can take $(1+N)^n$ values, if

$$(1+N)^n > (1+N)^m (nM)^m \iff (1+N)^{n-m} > (nM)^m \iff 1 + N > (nM)^{\frac{m}{n-m}}$$

then one value will be taken twice by the pigeonhole principle, say $AX = AY$. This yields

$A(X-Y)=0$ for some $Z=X-Y\subseteq[\![-N,N]\!]^n$ as wanted. It is clear that $N=\left\lfloor (nM)^{\frac{m}{n-m}}\right\rfloor$ works and gives us what we want. ■

Exercise C.5.24. How many invertible $n\times n$ matrices are there in $\mathbb{F}_p$? Deduce the number of (additive) subgroups of cardinality p^m that $(\mathbb{Z}/p\mathbb{Z})^n$ has.

Solution

We proceed inductively to determine the number of tuples of linearly independent vectors of cardinality k. At first, we can pick any non-zero vector in $\mathbb{F}_p^n$, there are thus p^n-1 choices. Then, we can pick any vector which is not a linear combination of the first one, there are thus p^n-p possible choices. Continuing like that, if we have picked k vectors, their linear combinations generate p^k elements so we have p^k elements to avoid and thus p^n-p^k possibilities for the next vector. In conclusion, the number of invertible $n\times n$ matrices with coefficients in $\mathbb{F}_p$ is

$$(p^n-1)(p^n-p)\cdot\ldots\cdot(p^n-p^{n-1}).$$

For the second part, note that a subgroup of $(\mathbb{Z}/p\mathbb{Z})^n$ is a $\mathbb{F}_p$-vector space, and the fact that it has p^m elements means that its dimension is m. Thus, we want to count the subspaces of $\mathbb{F}_p^n$ of dimension m. Here is how we will proceed: we count the number of tuples of m linearly independent elements, and divide this by the number of tuples which represent a fixed subspace. We have already computed the first one: it is

$$(p^n-1)\cdot\ldots\cdot(p^n-p^{m-1}).$$

We have also determined the second: if we fix a subspace of dimension m, it has

$$(p^m-1)\cdot\ldots\cdot(p^m-p^{m-1})$$

bases. We conclude that $(\mathbb{Z}/p\mathbb{Z})^n$ has

$$\frac{(p^n-1)\cdot\ldots\cdot(p^n-p^{m-1})}{(p^m-1)\cdot\ldots\cdot(p^m-p^{m-1})}$$

subgroups of cardinality p^m. ■

Exercise C.5.25†. Let K be a field, and let $S\subseteq K^2$ be a set of points. Prove that there exists a polynomial $f\in K[X,Y]$ of degree at most $\sqrt{2n}$ such that $f(x,y)=0$ for every $(x,y)\in S$.

Solution

Write $f=\sum_{i,j}a_{i,j}X^iY^j$ where the sum is over the i,j such that $i+j\leq\sqrt{2n}$. By stars and bars, there are $\binom{2+\lfloor\sqrt{2n}\rfloor}{2}$ such pairs: we choose the two values i and $i+j+1$ in $[\![0,\lfloor\sqrt{2n}\rfloor+1]\!]$. Since

$$\binom{2+\lfloor\sqrt{2n}\rfloor}{2}=\frac{(1+\lfloor\sqrt{2n}\rfloor)(2+\lfloor\sqrt{2n}\rfloor)}{2}>\frac{\sqrt{2n}\cdot\sqrt{2n}}{2}=n,$$

we have more unknowns then equations so there is a solution. ■

Exercise C.5.26†. Given an $m\times n$ matrix M, we define its *row rank* as the maximal number of linearly independent rows of M. Similarly, its *column rank* is the maximal number of linearly independent columns of M. Prove that these two numbers are the same, called the rank of M and denoted $\operatorname{rank}M$.

Solution

Without loss of generality, by removing some rows if necessary, suppose that all m rows of M are linearly independent. We will prove that M has at least m linearly independent columns, which implies that the column rank is greater than or equal to the row rank (if we add rows the linearly independent columns stay linearly independent). Taking the transpose then yields the reverse inequality, so they are in fact both equal.

Suppose for the sake of a contradiction that M has at most $m-1$ linearly independent columns, say $M^1, \dots, M^k$. If we consider the m vectors corresponding to the rows of $[M^1, \dots, M^k]$, they are linearly dependent by Proposition C.1.2. Now, if we add a column M^{k+1} which is a linear combination of $M^1, \dots, M^k$, the vectors corresponding to the rows of $[M^1, \dots, M^{k+1}]$ stay linearly dependent. Indeed, if

$$M^{k+1} = \sum_{i=1}^{k} a_i M^i$$

and the linear dependence of the rows of $[M^1, \dots, M^k]$ is

$$\sum_{i=1}^{m} b_i m_{i,j}$$

for any $j \in [k]$, then

$$\begin{aligned} \sum_{i=1}^{m} b_i m_{i,k+1} &= \sum_{i=1}^{m} b_i \sum_{j=1}^{k} a_j m_{i,j} \\ &= \sum_{j=1}^{k} a_j \sum_{i=1}^{m} b_i m_{i,j} \\ &= 0. \end{aligned}$$

In other words, a linear dependence between the rows extends to a linear dependence with the same coefficients between the rows when we add a linearly dependent column. Continuing like that shows that, finally, the rows of $[M^1, \dots, M^m] = M$ are linearly dependent, contradicting our initial assumption. ■

Exercise C.5.28 (Nakayama's Lemma)**.** Let R be a commutative ring, I an *ideal* of a R, i.e. an *R-module* inside R[3], and M a finitely-generated R-module. Suppose that $IM = M$, where IM does not mean the set of products of elements of I and M, but instead the R-module it generates (i.e. the set of linear combinations of products). Prove that there exists an element $r \equiv 1 \pmod{I}$ of R such that $rM = 0$.

Solution

Let $\alpha_1, \dots, \alpha_n$ be generators of M. We have a system of equation as follows:

$$\alpha_i = \sum_{j=1}^{n} \beta_{i,j} \alpha_j$$

for $i = 1, \dots, n$ and $\beta_{i,j} \in I$. Let $B = (\beta_{i,j})$ and $A = (\alpha_i)$ (as a colum vector), so that $BA = A$, i.e. $(I_n - B)A = 0$. We claim that $r = \det(I_n - B)$ works. First, note that $r \equiv 1 \pmod{I}$ since $I_n - B \equiv I_n \pmod{I}$. By Proposition C.3.7, we have

$$rI_n = \operatorname{adj}(I_n - B)(I_n - B)$$

[3]See also Proposition C.3.5. A module is like a vector space but the underlying structure is not necessarily a field (in this case it's R).

so, after right-multiplying by A, we get $rA = 0$. This implies that $rM = 0$ as wanted. ■

Further Reading

Here are some books I like[4]. As said in the foreword, I particularly recommend Andreescu-Dospinescu [1, 2], Ireland-Rosen [11], and Murty [19].

For classical algebraic number theory, I suggest Murty [19]. I'll just define ideals here because they are not defined in the book (but no prior exposure to them is assumed, so a wikipedia search would also do). An ideal I of a commutative ring R is simply a set which is closed under addition, and closed under multiplication by elements of R. In number fields, ideals are all *finitely generated*, i.e. $I = a_1R + \ldots + a_nR$ for some $a_1, \ldots, a_n$ (see chapter 5 of Murty). As an exercise you can prove that the ideals of $\mathbb{Z}$ have the form $n\mathbb{Z}$ for some n. Milne [18] (pages 7–10) has good motivation on why to consider ideals.

For p-adic analysis, I wholeheartedly recommend the addendum 3B of SFTB first, and then the excellent book by Cassels [7], which, although a bit old[5], is full of number-theoretic applications like the one in Section 8.6. Robert [23] is also very good, but focuses a lot more on analysis than on number theory, and assumes a fair amount of topology.[6] Also, Borevich-Shafarevich [6] has a great proof of Thue's theorem 7.4.3 using local methods (p-adic methods).

The elementary theory of elliptic curves is also of similar flavour to the topics of the present book, see Silverman-Tate [26] for a wonderful introduction.

For more on polynomials, see Prasolov [21] (things like Appendix A). See also Rosen [24] for number theory in function fields, i.e. algebraic number theory but with polynomials over $\mathbb{F}_q$ instead of rational integers!

For abstract algebra (including Galois theory), I recommend Lang [15]. For even more advanced algebra, see his other book [13].

For linear algebra, I also recommend Lang [14] because I like everything I read by him. For applications of linear algebra to combinatorics, see chapter 12 of PFTB [1], which assumes approximately Appendix C as background, and Stanley [27], which assumes approximately Lang's book as background.

[4] Disclaimer: I haven't finished reading all of them.

[5] It's not typeset in LaTeX!

[6] The first chapter is particularly topologically heavy but it gets better afterwards. I would suggest to skip it at first since it just defines the p-adic numbers, and have a look at the other chapters if you're interested in the analytical theory.

Further Reading

[1] T. Andreescu and G. Dospinescu. *Problems from the Book*. 2nd ed. XYZ Press, 2010.

[2] T. Andreescu and G. Dospinescu. *Problems from the Book*. XYZ Press, 2012.

[6] Z. I. Borevich and I. Shafarevich. *Number Theory*. Academic Press, 1964.

[7] J. W. S. Cassels. *Local fields*. Cambridge University Press, 1986.

[11] S. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. 2nd ed. Vol. 84. Graduate Texts in Mathematics. Springer-Verlag, 1990.

[13] S. Lang. *Algebra*. 5th ed. Vol. 211. Graduate Texts in Mathematics. Springer-Verlag, 2002.

[14] S. Lang. *Linear Algebra*. 3rd ed. Undergraduate Texts in Mathematics. Springer-Verlag, 1987.

[15] S. Lang. *Undergraduate Algebra*. 3rd ed. Undergraduate Texts in Mathematics. Springer-Verlag, 1987.

[18] J. S. Milne. *Algebraic Number Theory*. URL: https://www.jmilne.org/math/CourseNotes/ant.html. (accessed: 26.09.2021).

[19] M. R. Murty and J. Esmonde. *Problems in Algebraic Number Theory*. 2nd ed. Vol. 190. Graduate Texts in Mathematics. Springer-Verlag, 2005.

[21] V. V. Prasolov. *Polynomials*. Vol. 11. Algorithms and Computation in Mathematics. Springer-Verlag, 2004.

[23] A. M. Robert. *A Course in p-adic Analysis*. Vol. 198. Graduate Texts in Mathematics. Springer-Verlag, 2000.

[24] M. Rosen. *Number Theory in Function Fields*. Vol. 210. Graduate Texts in Mathematics. Springer-Verlag, 2002.

[26] J. H. Silverman and J. T. Tate. *Rational Points on Elliptic Curves*. 2nd ed. Undergraduate Texts in Mathematics. Springer-Verlag, 2015.

[27] R. Stanley. *Algebraic Combinatorics*. 2nd ed. Undergraduate Texts in Mathematics. Springer-Verlag, 2018.

Bibliography

[3] G. M. Bergman. *Luroth's Theorem and some related results, developed as a series of exercises.* URL: https://math.berkeley.edu/~gbergman/grad.hndts/. (accessed: 26.09.2021).

[4] Y. Bilu, Y. Bugeaud, and M. Mignotte. *The Problem of Catalan.* Springer-Verlag, 2014.

[5] A. B. Block. *The Skolem-Mahler-Lech Theorem.* URL: http://www.columbia.edu/~abb2190/Skolem-Mahler-Lech.pdf. (accessed: 26.09.2021).

[8] E. Chen. *A trailer for p-adic analysis, first half: USA TST 2003.* URL: https://blog.evanchen.cc/2018/10/10/a-trailer-for-p-adic-analysis-first-half-usa-tst-2003/. (accessed: 26.09.2021).

[9] E. Chen. *Napkin.* URL: https://web.evanchen.cc/napkin.html. (accessed: 26.09.2021).

[10] K. Conrad. *Kummer's lemma.* URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/kummer.pdf. (accessed: 26.09.2021).

[12] M. Klazar. *Størmer's solution of the unit equation $x - y = 1$.* URL: https://kam.mff.cuni.cz/~klazar/stormer.pdf. (accessed: 26.09.2021).

[16] P-S. Loh. *Algebraic Methods in Combinatorics.* URL: https://www.math.cmu.edu/~ploh/docs/math/mop2009/alg-comb.pdf. (accessed: 26.09.2021).

[17] D. Masser. *Auxiliary Polynomials in Number Theory.* Cambridge Tracts in Mathematics. Cambridge University Press, 2016.

[20] M. R. Murty and N. Thain. "Primes in Certain Arithmetic Progressions". In: *Functiones et Approximatio* 35 (2006), pp. 249–259. DOI: 10.7169/facm/1229442627.

[22] P. Ribenboim. *13 Lectures on Fermat's Last Theorem.* Springer-Verlag, 1979.

[25] A. Schinzel. "On Primitive Prime Factors of $a^n - b^n$". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 58 (4 1962), pp. 556–. DOI: 10.1017/s0305004100040561.

[28] C. L. Stewart. "On the greatest prime factor of terms of a linear recurrence sequence". In: *Rocky Mountain Journal of Mathematics* 35 (2 1985), pp. 599–608. DOI: 10.1216/RMJ-1985-15-2-599.

[29] R. Thangadurai. *On the Coefficients of Cyclotomic Polynomials.* URL: https://www.bprim.org/sites/default/files/th.pdf. (accessed: 26.09.2021).

[30] N. Tsopanidis. "The Hurwitz and Lipschitz Integers and Some Applications". PhD thesis. Faculdade De Ciências da Universidade do Porto, 2020.

[31] S. Weintraub. *Galois Theory.* 2nd ed. Universitext. Springer-Verlag, 2009.

Index

D

E

N

O

P

Q