MA3A6
ALGEBRAIC NUMBER THEORY

SAMIR SIKSEK

Abstract. This is an incomplete set of lecture notes for for Algebraic Number Theory. I do not know yet if it will be completed, so you are advised to continue taking notes in the lectures. Please send comments, misprints and corrections to siksek@maths.warwick.ac.uk

Contents

Date: September 26, 2006.

1. Orientation

Algebraic number theory arose out of the study of Diophantine equations. A Diophantine equation is a polynomial equation in several variables with integer coefficients and one desires the solutions in integers. The study of Diophantine equations seems as old as human civilization itself; they are however named after Diophantus of Alexandria who lived in the 3rd century BC. Soon we will give our motivating example for algebraic number theory. Before that we look at three methods for attacking Diophantine equations which should be close to the heart of every student of number theory: *Local Methods*, *Infinite Descent*, *Descent*.

1.1. **Local Arguments.** This means that we look at the equation modulo some positive integer m and try to get information about integral solutions.

Example 1.1. Show that the equation

$$x^2 + 1 = 4y^2$$

does not have solutions in integers.
Answer: Suppose x, y is an integer solution. Reducing the equation modulo 4 we get

$$x^2 + 1 \equiv 0 \pmod 4.$$

However, the squares modulo 4 are $x^2 \equiv 0$ or $1 \pmod 4$. So

$$x^2 + 1 \equiv 1 \text{ or } 2 \pmod 4,$$

giving a contradiction.

Included in 'local arguments' is the idea that if an equation does not have real solutions then it does not have integeral solutions. For example, the equation $x^2 + 5 = -2z^2$ does not have integral solutions because it does not have real solutions.

1.2. **Infinite Descent.** 'infinite descent' is used to show that equations do not have solutions, or that they do not have non-trivial solutions. The idea is to suppose that a Diophantine equation has solutions, take the smallest one and show that there must be a smaller one, giving a contradiction.

Example 1.2. Show that the equation $X^2 = 2Y^2$ does not have non-trivial solutions in integers.

You will recognize this as essentially the proof that $\sqrt{2}$ is irrational. Suppose that we have non-trivial solutions. Let (x, y) be a non-trivial solution with the value of $|x|$ minimal. Since $x^2 = 2y^2$ we get that x is even. So $x = 2x_1$ for some

$x_1 \in \mathbb{Z}$. So $2x_1^2 = y^2$ and we show that $y = 2y_1$. Now (x_1, y_1) is a non-trivial solution to $X^2 = 2Y^2$ and $|x_1| < |x|$, giving a contradiction.

The name 'infinite descent'comes from the original way in which the method is applied. We start with a non-trivial solution (x, y) and construct another one (x_1, y_1), and then from (x_1, y_1) we get another one (x_2, y_2) and so on. We get an infinite list of non-trivial solutions satisfying

$$|x| > |x_1| > |x_2| > \cdots > 0;$$

but we cannot squeeze infinitely many integers between $|x|$ and 0 and we have a contradiction.

Here is another example due to Euler.

Example 1.3. Show that the equation

$$X^2 + 2Y^3 + 4Z^3 = 0 \tag{1}$$

has no non-trivial solutions.

Answer: Suppose it has non-trivial solutions. Let (x, y, z) be a non-trivial solution with the value of $|x|$ minimal. We see that x^3 is even and so x is even. Write $x = 2x_1$. Then

$$4x_1^3 + y^3 + 2z^3 = 0.$$

Thus $y = 2y_1$ and applying the same trick again $z = 2z_1$. We see that (x_1, y_1, z_1) is a non-trivial solution to equation (1) with $|x_1| < |x|$ giving a contradiction.

In both the above examples, we could have obtained a contradition by explaining that we may assume that x, y are coprime. Then the argument shows that x, y are not coprime. This is not always the case with infinite descent examples.

1.3. **Descent.** Descent is not the same as infinite descent. It is a technique invented by Fermat. It uses variants of the following very simple Lemma:

Lemma 1.1. *Suppose that U, V, W are non-zero integers, with U, V coprime. Suppose also that $UV = W^n$ where n is a positive integer. Then $U = \pm W_1^n$ and $V = \pm W_2^n$ for some integers W_1, W_2. Moreover, if n is odd, we can take $U = W_1^n$ and $V = W_2^n$.*

Proof. Let $p_1, \dots p_r$ be the distinct prime divisors of U and $q_1, \dots, q_s$ the distinct prime divisors of V. Since U, V are coprime, these lists are disjoint (this is a very important point). Notice that

$$p_1, \dots, p_r, q_1, \dots, q_s$$

are the distinct prime divisors of W. By the Fundamental Theorem of Arithmetic, we can write

$$U = \pm p_1^{a_1} \dots p_r^{a_r}, \qquad V = \pm q_1^{b_1} \dots q_s^{b_s}, \qquad W = \pm p_1^{c_1} \dots p_r^{c_r} q_1^{d_1} \dots q_r^{d_s}.$$

Substituting in $UV = W^n$ we get

$$p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_s^{b_s} = \pm p_1^{nc_1} \dots p_r^{nc_r} q_1^{nd_1} \dots q_r^{nd_s}.$$

From the uniqueness of factorization we deduce that

$$a_i = nc_i, \qquad b_j = nd_j;$$

it is here that we need the fact that the ps and qs are distinct. Hence

$$U = \pm \left(p_1^{c_1} \dots p_r^{c_r}\right)^n, \qquad V = \pm \left(q_1^{d_1} \dots q_s^{d_s}\right)^n.$$

This completes the proof for n even. For n odd, simply absorb the $\pm$ inside the n-th power. $\square$

We are ready to give a first example of descent.

Example 1.4. Show that the equation

$$4X^2 - 1 = Y^3$$

has no solutions in integers apart from $(X, Y) = (0, -1)$.
Answer: First notice that if (X, Y) is a solution then so is $(-X, Y)$. So we may suppose that we have a solution with $X \geq 0$. Write

$$(2X + 1)(2X - 1) = Y^3.$$

Let d be the gcd of $2X+1$ and $2X-1$. Since d divides them both, it must divide their difference; thus $d \mid 2$ and so $d = 1$ or $d = 2$. However, d divides $2X + 1$ which is odd, so d is odd and so $d = 1$. In other words, $2X + 1$ and $2X - 1$ are coprime. Applying Lemma 1.1 we see that

$$2X + 1 = Y_1^3, \qquad 2X - 1 = Y_2^3, \tag{2}$$

where $Y = Y_1 Y_2$ (this step is called 'descent'). Subtracting we get

$$2 = Y_1^3 - Y_2^3 = (Y_1 - Y_2)(Y_1^2 + Y_1 Y_2 + Y_2^2).$$

Recall our assumption that $X \geq 0$. Hence $2X + 1 > 2X - 1$ which gives $Y_1 > Y_2$; i.e. $Y_1 - Y_2 > 0$. We deduce that either

$$Y_1 - Y_2 = 1, \qquad Y_1^2 + Y_1 Y_2 + Y_2^2 = 2,$$

or

$$Y_1 - Y_2 = 2, \qquad Y_1^2 + Y_1 Y_2 + Y_2^2 = 1.$$

But, from (2) we know that Y_1, Y_2 are both odd, and so $Y_1 - Y_2$ is even. Hence we have only to deal with the last case: $Y_1 - Y_2 = 2$. Write $Y_1 = Y_2 + 2$ and substitute in to $Y_1^2 + Y_1 Y_2 + Y_2^2 = 1$. We get $Y_2^2 + 2Y_2 + 1 = 0$. Thus $Y_2 = -1$ and $Y_1 = Y_2 + 2 = 1$. Hence $Y = Y_1 Y_2 = -1$ and we see that $X = 0$ as required.

2. Beginnings of Algebraic Number Theory

The following example is the beginning of algebraic number theory. Fermat claimed that he has shown that the only solutions to the equation

$$X^2 + 2 = Y^3$$

is $(X, Y) = (\pm 5, 3)$. Euler 'proved'Fermat's assertion in 1770. The 'proof' mimics the standard factorization or descent argument used in the above example. We say 'proof' in quotes because what Euler wrote down was not rigorous, but can be made rigorous. Let us see Eulers argument: simply factor the left-hand side to get:

$$(X + \sqrt{-2})(X - \sqrt{-2}) = Y^3.$$

We leave the usual integers $\mathbb{Z}$ and work with $\mathbb{Z}[\sqrt{-2}]$. Now the 'integers' $X + \sqrt{-2}$, $X - \sqrt{-2}$ are 'coprime'and so each must be a cube. So

$$X + \sqrt{-2} = (a + b\sqrt{-2})^3,$$

where a, b are in $\mathbb{Z}$. Once we get past the dodgy step above, the rest of the argument is respectable. Expand the brackets to get

$$X + \sqrt{-2} = (a^3 - 6ab^2) + (3a^2 b - 2b^3)\sqrt{-2}.$$

Comparing the coefficients of $\sqrt{-2}$ we get

$$X = a^3 - 6ab^2, \qquad 1 = 3a^2b - 2b^3.$$

Hence $b \mid 1$ and so $b = \pm 1$ which gives $3a^2 - 2 = \pm 1$. Therefore $a = \pm 1$ and we get $X = a^3 - 6ab^2 = \pm 5$. Hence $(X, Y) = (\pm 5, 3)$ as required.

Is this argument respectable? It turns out that it is because $\mathbb{Z}[\sqrt{-2}]$ is a unique factorization domain, and so we have an analogue of the Fundamental Theorem of Arithmetic and can prove the needed analogue of Lemma 1.1.

This and other Diophantine equations have lead us to reconsider what integers are. In $\mathbb{Q}$ we have rational (or usual) integers $\mathbb{Z}$. But in other fields such as $\mathbb{Q}(\sqrt{d})$ we have an extension of the concept of integer. Unfortunately unique factorisation does not always hold. For example, in $\mathbb{Q}(\sqrt{-5})$, the 'integers'is the ring $\mathbb{Z}[\sqrt{-5}]$. Here we do not have unique factorization (i.e. there is no analogue of the Fundamental Theorem of Arithmetic); for example, 6 can be factorized as a product of irreducibles in two different ways,

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Thus the analogue of our Lemma 1.1 does not hold for this ring.

In this course we cover the following ideas:

(1) The correct generalization of the concept of integer.
(2) Whilst uniqueness of factorization fails for elements (as above), it holds for ideals; every ideal can be expressed as a product of powers of distinct prime ideals in a unique way.
(3) *Minkowski's Theorem.* Essentially this tells us that whilst unique factorization fails, it is not by too much.
(4) *Dirichelet's Unit Theorem.*

3. Preliminaries on Rings and Ideals

We begin by revising some ideas that you have met in previous algebra courses.

3.1. **Rings.** By a *ring* we shall always mean a commutative ring with a unit element 1. Examples of rings that you are familiar with are $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{Z}[i]$ (the Gaussian integers), $\mathbb{Q}[x]$, $\mathbb{Z}[x]$. Another important ring is $\mathbb{Z}/n\mathbb{Z}$ (the integers modulo n). You probably called this ring $\mathbb{Z}_n$ in your earlier courses, but we will stick with the notatin $\mathbb{Z}/n\mathbb{Z}$.

Definition. *Let R be a ring. A non-zero element $x \in R$ is called a* zero-divisor *if there is some other non-zero element y such that $xy = 0$. A ring that* does not *have zero-divisors is called an integeral domain.*

Example 3.1. $\mathbb{Z}$, $\mathbb{Q}[x]$ do not have zero-divisors and are therefore integral domains.

Example 3.2. In the ring $\mathbb{Z}/6\mathbb{Z}$ (integers modulo 6) the elements 2 and 3 are zero-divisors, because $2 \times 3 \equiv 0 \pmod 6$ but $2 \not\equiv 0 \pmod 6$ and $3 \not\equiv 0 \pmod 6$. Thus $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain.

Exercise 3.3. Suppose $n > 1$ is an integer. Show that $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is prime.

3.2. **Ideals.**

Definition. *Let R be a ring. A non-empty subset I is an* ideal *if*

- *$a - b \in I$ for every a, $b \in I$ (this really says that I is an additive subgroup of R);*
- *if $a \in I$ and $r \in R$ then $ra \in I$.*

Example 3.4. R is an ideal of R. Every other ideal of R is called a proper ideal.

Example 3.5. Suppose R is an ring and $a \in R$. We define

$$aR = \{ar \ : \ r \in R\}.$$

It is easy to show that aR is an ideal of R (just check the definition). We call aR the principal ideal generated by a. Another common notation for aR is (a).

The ideal $(0) = \{0\}$ is called the zero ideal.

3.3. **Quotient Rings.** Let I be an ideal of the ring R. A coset of I is of the form

$$x + I = \{x + a \ : \ a \in I\}.$$

Recall that two cosets are equal $x + I = y + I$ if and only if $x - y = I$. We define the *quotient*

$$R/I = \{x + I \ : \ x \in R\}.$$

A priori R/I is just the set of cosets of R, but we can make it into a ring by defining addition and multiplication as follows:

$$(x + I) + (y + I) = (x + y) + I, \qquad (x + I)(y + I) = xy + I.$$

Exercise 3.6. Prove that these operations are well-defined and that they do give us a ring structure on R/I.

3.4. **Units.**

Definition. *An element u of a ring R is called a* unit *(or an* invertible element*) if there is some other element $v \in R$ such that $uv = 1$. If R is an integral domain, then v is unique and we call it the inverse of u and write $v = u^{-1}$.*

The set of units in R is denoted by R^* or $U(R)$.

Example 3.7. The units of $\mathbb{Z}$ are ± 1. Thus $\mathbb{Z}^* = \{1, -1\}$.

Example 3.8. The units of $\mathbb{Z}[i] = \{a + bi \ : \ a, b \in Z\}$ are ± 1, $\pm i$. It is clear that these are units. Let us prove that they are the only ones. Suppose $u \in \mathbb{Z}[i]$ is a unit and let $v = u^{-1}$. Then $u = a + bi$ and $v = c + di$ for some integers $a,\ldots,d$ such that

$$(a + bi)(c + di) = 1.$$

Conjugating we get

$$(a - bi)(c - di) = 1.$$

Multiplying the last two equalities

$$(a^2 + b^2)(c^2 + d^2) = 1.$$

Now noting that $a^2 + b^2$, $c^2 + d^2$ are in $\mathbb{Z}$ and non-negative we deduce

$$a^2 + b^2 = c^2 + d^2 = 1.$$

Hence $(a, b) = (\pm 1, 0)$ or $(0, \pm 1)$ giving the $u = \pm 1$ or $\pm i$.

Exercise 3.9. Determine the units of $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \ : \ a, b \in \mathbb{Z}\}$ and of

$$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{-3}}{2}\right) \ : \quad a, b \in \mathbb{Z}\right\}.$$

Exercise 3.10. If R is a ring then R^* is a group under multiplication (it is called the unit group of R).

Example 3.11. Note that $(\sqrt{2}+1)(\sqrt{2}-1) = 1$. Thus $\sqrt{2}+1$ is a unit in the ring $\mathbb{Z}[\sqrt{2}]$. Since the units form a group under multiplication, we see immediately that $(\sqrt{2}+1)^n$ is a unit for all integers n. In fact, it can be shown that

$$\mathbb{Z}[\sqrt{2}]^* = \{\pm(\sqrt{2}+1)^n \ : \ n \in \mathbb{Z}\}.$$

Dirichelet's Units Theorem, which we will hopefully meet at the end of this course, describes unit groups R^* for certain rings called rings of integers of number fields.

Exercise 3.12. If R is a ring then $R[x]^* = R^*$.

3.5. **Fields.**

Definition. *A* field *is a non-zero ring where every non-zero element is a unit.*

Example 3.13. $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

Theorem 1. *Every finite integral domain is a field.*

Proof. Suppose R is a finite integral domain. We want to show that every non-zero element is invertible. Suppose x is a non-zero element, and consider the map

$$\phi_x \ : \ R \to R, \qquad \phi_x(a) = x\,a.$$

We want to show first that ϕ_x is one-to-one. So suppose that a, $b \in R$ and $\phi_x(a) = \phi_x(b)$. Thus $x\,a = x\,b$, or in other words

$$x\,(a-b) = 0.$$

But R is an integral domain, and so x is not a zero-divisor. Hence $a - b = 0$, which gives $a = b$ showing indeed that ϕ_x is one-to-one.

Here is where we use the fact that R is finite: recall that a one-to-one map from a finite set to itself must be onto. Hence ϕ_x is onto. In particular, there is some element $y \in R$ such that $\phi_x(y) = 1$. We can re-write this as $xy = 1$, clearly showing that x is invertible.

This show that R is a field. □

Example 3.14. Suppose p is a prime. We denote $\mathbb{Z}/p\mathbb{Z}$ (the integers modulo p) by $\mathbb{F}_p$. We know from Exercise 3.3 that $\mathbb{F}_p$ is an integral domain. Since $\mathbb{F}_p$ is finite, Theorem 1 tells us that it is a field.

Note that the proof of Theorem 1 is non-constructive. It shows that if x is a non-zero element then it has an inverse, but it does not tell us how to find it. For $\mathbb{F}_p$ we can actually give a constructive proof. Suppose x is an integer satisfying $x \not\equiv 0 \pmod{p}$. This means that $p \nmid x$ and (as p is prime), the integers x and p are coprime. By Euclid's algorithm we know that there are integers y, z such that

$$y\,x + z\,p = 1.$$

Recuding modulo p we get

$$y\,x \equiv 1 \pmod{p},$$

showing that x is invertible. Euclid's algorithm is actually a recipe that will write down for us y (and z). Thus we can calculate the inverse of any non-zero element.

Exercise 3.15. Use Euclid's algorithm to find the inverse of 14 in $\mathbb{F}_{101}$.

3.6. **Fields of Fractions.**

Definition. *Let R be an integral domain. A field K is said to be the* field of fractions *if*

- *K contains R as a subring;*
- *every element $\alpha \in K$ is expressible as a/b for some a, $b \in R$ and $b \neq 0$.*

Example 3.16. $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$. $\mathbb{Q}(x)$ is the field of fractions of $\mathbb{Q}[x]$ and of $\mathbb{Z}[x]$.

Theorem 2. *Every integral domain has a field of fractions (that is unique up to isomorphism).*

3.7. **Prime and Maximal Ideals.**

Definition. *Let R be a ring. An ideal $\wp$ of R is said to be a prime ideal if, $ab \in \wp$ implies $a \in \wp$ or $b \in \wp$ for all a, $b \in R$.*

An ideal $\mathfrak{m}$ of R is said to be maximal if it is a proper ideal and is not contained in any other proper ideal.

Exercise 3.17. Show that the zero ideal (0) is prime if and only R is an integral domain.

Exercise 3.18. Suppose p, q are distinct prime numbers. Let $R = \mathbb{Z}/pq\mathbb{Z}$ (the integers modulo pq). Show that pR and qR are prime ideals.

The proof of the following theorem is an easy exercise.

Theorem 3. *Let R be a ring. An ideal $\wp$ is a prime ideal if and only if $R/\wp$ is an integral domain. An ideal $\mathfrak{m}$ is maximal if and only if $R/\mathfrak{m}$ is a field.*

3.8. **Unique Factorization Domains.**

Definition. *Let R be a ring. A non-zero element x is called* irreducible *if x is not a unit and whenever $x = ab$ with a, $b \in R$, one of a, b must be a unit.*

Example 3.19. In $\mathbb{Z}$ the irreducible elements are of the form $\pm p$ where p is prime. The composite elements are of the form $\pm n$ where n is composite.

Example 3.20. 2 is irreducible in $\mathbb{Z}$ but not in $\mathbb{Z}[i]$, since $2 = (1+i)(1-i)$ and neither $(1+i)$ nor $(1-i)$ is a unit.

Definition. *Two elements x, $y \in R$ are called* associates *(written $x \sim y$) if there is a unit $u \in R$ such that $x = uy$.*

Definition. *A ring R is a* unique factorization domain *if it satisfies the following three conditions:*

- *R is an integral domain;*
- *Every non-zero, non-unit $x \in R$ can be written as a product $x = q_1 \dots q_r$ of irreducible elements;*
- *The decomposition of x into irreducibles is unique up to units and permutation of factors. This means that if $x = q'_1 \dots q'_s$ is another factorization into irreducibles then $r = s$ and after possibly relabeling we have $q_i \sim q'_i$ for all $i = 1, \dots, r$.*

4. Algebraic Numbers and Algebraic Integers

We now introduce the main objects of study of algebraic number theory.

Definition. *Let $\alpha \in \mathbb{C}$. We say that α is an algebraic number if there is some non-zero polynomial $f(x) \in \mathbb{Q}[x]$ (i.e. it has rational coefficients) such that $f(\alpha) = 0$.*

We say that $\alpha \in C$ is an algebraic integer if there is some monic polynomial $f(x) \in \mathbb{Z}[x]$ (i.e. with integral coefficients) such that $f(\alpha) = 0$.

Clearly every algebraic integer is an algebraic number. We will see that the converse need not hold. We denote the set of algebraic numbers by $\overline{\mathbb{Q}}$ and the set of algebraic integers by $\mathcal{O}$. Thus

$$\mathcal{O} \subset \overline{\mathbb{Q}} \subset \mathbb{C}.$$

Lemma 4.1. *$\mathbb{Z} \subset \mathcal{O}$ and $\mathbb{Q} \subset \overline{\mathbb{Q}}$.*

Proof. If $\alpha \in \mathbb{Z}$ then α is the root of $X - \alpha$ which is a monic polynomial in $\mathbb{Z}[X]$, and so $\alpha \in \mathcal{O}$. Thus $\mathbb{Z} \subset \mathcal{O}$, and similarly $\mathbb{Q} \subset \overline{\mathbb{Q}}$. □

Example 4.1. $\sqrt{-2}$ is an algebraic integer because it is a root of the monic polynomial with integral coefficients $X^2 + 2$.

Let $\alpha = \sqrt{2} + \sqrt{3}$. We will show that α is also an algebraic integer. Note

$$\alpha^2 = 5 + 2\sqrt{6}.$$

Hence

$$(\alpha^2 - 5) = 24.$$

In other words, $\alpha = \sqrt{2} + \sqrt{3}$ is a root of

$$f(X) = (X^2 - 5)^2 - 24 = X^4 - 10X^2 + 1.$$

Since $f(X)$ is monic with integral coefficients, it follows that α is an algebraic integer.

Example 4.2. Not every complex number is algebraic. Complex numbers that are not algebraic numbers are called **transcendental**. Examples of transcendental numbers are e and π. We shall not prove this as we do not need it. For proofs, see Stewart's *Galois Theory*.

The elements of $\mathbb{Z}$ are called the *rational integers*. The reason is found in the following theorem which says that any algebraic integer which is also a rational number must belong to $\mathbb{Z}$.

Theorem 4. *(Gauss) $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$.*

Proof. We know that $\mathbb{Z} \subset \mathbb{Q}$ and $\mathbb{Z} \subset \mathcal{O}$ so $\mathbb{Z} \subset \mathcal{O} \cap \mathbb{Q}$. It is enough to prove that $\mathcal{O} \cap \mathbb{Q} \subset \mathbb{Z}$. Suppose $\alpha \in \mathcal{O} \cap \mathbb{Q}$; we want to show that $\alpha \in \mathbb{Z}$. Thus there some polynomial $f(X)$, monic with coefficients in $\mathbb{Z}$ such that $f(\alpha) = 0$. Write

$$f(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0, \qquad c_i \in \mathbb{Z}.$$

Since α is rational, we may write $\alpha = a/b$ where a, b are integers, $b > 0$ and $\gcd(a, b) = 1$. Substituting we get

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots c_0 = f(\alpha) = 0.$$

Multiplying by b^n we obtain

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_0 b^n = 0.$$

Rearranging we get

$$b \underbrace{\left(-c_{n-1}b^{n-2} - \cdots - c_0\right)}_{\text{in } \mathbb{Z}} = a^n.$$

We deduce that $b \mid a^n$. Recall $b > 0$. We want to show that $\alpha = a/b$ is in $\mathbb{Z}$ and for this it is enought to show that $b = 1$. Suppose that $b \neq 1$ and we will derive a contradiction. Then some prime p must divide b. So $p \mid a^n$ which implies $p \mid a$. This contradicts the assumption that $\gcd(a, b) = 1$. Hence $b = 1$ and $\alpha \in \mathbb{Z}$ as required. □

Example 4.3. All the examples of algebraic numbers that we have seen so far have been algebraic integers. Thanks to the above theorem, we can now give examples of algebraic numbers that are not algebraic integers: $1/2$, $-3/4$, etc. Any rational number that is not an integer is an algebraic number that is not an algebraic integer.

Exercise 4.4. Show that the following are algebraic numbers: $\sqrt{3}$, $\sqrt{3} + \sqrt{-3}$, $e^{2\pi i/7}$, $\cos(2\pi i/3)$.

Eventually we will show that $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$ and that $\mathcal{O}$ is a subring of $\mathbb{C}$. For this we need symmetric polynomials which we will cover soon. In the meantime we content with proving the following Lemma.

Lemma 4.2. *Suppose $\alpha \in \overline{\mathbb{Q}}$ and $\alpha \neq 0$. Then $\alpha^{-1} \in \overline{\mathbb{Q}}$.*

Proof. Suppose $\alpha \in \overline{\mathbb{Q}}$ and $\alpha \neq 0$. Then α is a root of some non-zero polynomial $f(X)$ with rational coefficients. Write

$$f(X) = c_n X^n + c_{n-1}X^{n-1} + \cdots + c_0.$$

Then

$$c_n\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0.$$

Dividing by α^n we get

$$c_n + c_{n-1}\alpha^{-1} + \cdots + c_0\alpha^{-n} = 0.$$

Hence α^{-1} is the root of the non-zero polynomial

$$g(X) = c_0 X^n + \cdots + c_{n-1}X + c_n$$

which has rational coefficients; implying $\alpha^{-1} \in \overline{\mathbb{Q}}$. □

5. Minimal Polynomials

We recall the definition of an algebraic number: $\alpha \in \mathbb{C}$ is said to be algebraic if there is some non-zero polynomial $f \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. For any algebraic α there are of course infinitely many such f. For example, if $\alpha = i$, we may take f to be any of

$$x^2 + 1, \quad (x^2 + 1)(x - 7), \quad (x^2 + 1)^3, \ldots.$$

It turns out that the 'best' choice for f is the one with least degree. By 'best' here we mean the choice which most closely reflects the properties of α. To such an f we give a special name:

Definition. *Suppose $\alpha \in \mathbb{C}$ is an algebraic number. We define the* **minimal polynomial** *of α, which we denote by f_α to be the monic polynomial with rational coefficients and least possible degree satisfying $f_\alpha(\alpha) = 0$.*

As with any other definition in Mathematics, we must be concerned with existence and uniqueness. If α is an algebraic number, there is by definition some non-zero polynomial f with rational coefficients satisfying $f(\alpha) = 0$. We can make f monic simply by dividing f by the leading coefficient. Out of all such polynomials we take f_α to be the one of least possible degree, which will be the minimal polynomial. Of course here we run into the problem of uniqueness, for there may be two or more such polynomials of minimal degree. We prove below that minimal polynomials are unique, so until then read 'let f_α be a minimal polynomial for α' when you see the phrase 'let f_α be the minimal polynomial for α'.

Lemma 5.1. *Let α be an algebraic number and $f_\alpha \in \mathbb{Q}[x]$ be its minimal polynomial. Then*

(i) *f_α is irreducible* [1]*;*
(ii) *if $g \in \mathbb{Q}[x]$ satisfies $g(\alpha) = 0$ then $g \mid f_\alpha$.*

Proof. For (i) suppose otherwise. Then $f_\alpha(x) = g(x)h(x)$ where g, h are polynomials with rational coefficients and $\deg(g)$, $\deg(h) < \deg(f_\alpha)$; as f_α is monic we can suppose that g and h are monic (check this). Since $f_\alpha(\alpha) = 0$ we see that either $g(\alpha) = 0$ or $h(\alpha) = 0$. This contradicts that fact that f_α is the monic polynomials of least degree satisfying $f_\alpha(\alpha) = 0$. This prove (i).

We now turn to (ii). Suppose that $g \in \mathbb{Q}[x]$ satisfies $g(\alpha) = 0$. By Euclid's algorithm we know that

$$g(x) = q(x)f_\alpha(x) + r(x), \qquad q(x),\, r(x) \in \mathbb{Q}[x],$$

where either $r = 0$, or otherwise $\deg(r) < \deg(f)$. We want to show that $r = 0$; in this case $g(x) = q(x)f_\alpha(x)$ showing that $f_\alpha \mid g$ and this is what we desire to prove. So let us assume that $r \neq 0$, and hence r is a non-zero polynomial with rational coefficients of degree strictly less than f. Substituting α for x in the above and recalling that $g(\alpha) = f_\alpha(\alpha) = 0$ leads us at once to conclude that $r(\alpha) = 0$. We now divide r by its leading coefficient to obtain a monic polynomial $s \in \mathbb{Q}[x]$ with degree strictly less than f_α and satisfying $s(\alpha) = 0$. This is a contradiction and proves (ii).

There is a slightly different way of proving (ii). We know from (i) that f_α is irreducible. Suppose $f_\alpha \nmid g$. Then the polynomials f_α and g are coprime. By Euclid there are polynomials u, $v \in \mathbb{Q}[x]$ such that

$$u(x)f_\alpha(x) + v(x)g(x) = 1.$$

Substituting α for x we obtain $0 = 1$ which is a contradiction. □

We now prove the uniqueness of the minimal polynomial.

Corollary 5.2. *Suppose α is an algebraic number. The minimal polynomial f_α is unique.*

[1] Of course we mean here that f_α is irreducible over $\mathbb{Q}$. Over $\mathbb{C}$ we know by the Fundamental Theorem of Algebra that we may factorize it as a product of linear factors.

Proof. Suppose there are two minimal polynomials f, g for α. By part (ii) of the above Lemma we know that $f \mid g$ and $g \mid f$. Hence $f = \lambda g$ for some non-zero rational number λ. But f and g are both monic, and so $\lambda = 1$. □

Theorem 5. *Suppose α is an algebraic number. A polynomial $f \in \mathbb{Q}[x]$ is the minimal polynomial of α if and only if f is monic and irreducible and satisfies $f(\alpha) = 0$.*

Proof. If f is the minimal polynomial of α then f is monic and satisfies $f(\alpha) = 0$ by definition, and f is irreducible by part (i) of Lemma 5.1.

Conversely suppose that f is monic and irreducible and satisfies $f(\alpha) = 0$. By part (ii) Lemma 5.1 we see that $f_\alpha \mid f$. As f is irreducible, f_α is a constant or $f_\alpha = \lambda f$ for some non-zero rational λ. Since f_α is monic and $f_\alpha(\alpha) = 0$ we see that f_α is non-constant. Hence $f_\alpha = \lambda f$ for some non-zero rational λ. But f_α and f are both monic, so $\lambda = 1$ proving that $f = f_\alpha$ as desired. □

Example 5.1. Let $f(X) = X^2 - 2$; it is monic, has rational coefficients, is irreducible and satisfies $f(\sqrt{2}) = 0$. By the above theorem, f is the minimal polynomial of $\sqrt{2}$. Notice that it would not have been straightforward to deduce this fact from the definition of minimal polynomial.

6. Conjugates

Definition. *Suppose that α is an algebraic number and let f_α be its minimal polynomial. We define the* **degree** *of α to be the degree of f_α. We define the* **conjugates** *of α to be the roots f_α.*

By the Fundamental Theorem of Algebra we may factorize f_α over $\mathbb{C}$ into a product of linear factors

$$f_\alpha(X) = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n).$$

Then $\alpha_1, \ldots, \alpha_n$ are the conjugates of α. Notice that α is one of them. Here n is the number of conjugates of α, and at the same time the degree f (which by definition is the degree of α). Thus an algebraic number with degree n has n conjugates. The reader probably expects us to say that an algebraic number with degree n has n conjugates up to repetition, since polynomials can have repeated roots. However there is no repetition involved here since minimal polynomials (being irreducible) do not have repeated roots, thanks to the following theorem.

Theorem 6. *Suppose $f \in \mathbb{Q}[x]$ is an irreducible polynomial. Then f does not have repeated roots in $\mathbb{C}$.*

In particular, this applies to minimal polynomials of algebraic numbers. Thus an algebraic number has distinct conjugates.

Proof. Suppose $f \in \mathbb{Q}[x]$ is irreducible, but has repeated root $\beta \in \mathbb{C}$. Consider the derivative f' of f. Clearly $f' \in \mathbb{Q}[x]$. Since f is irreducible and f' has degree less than f we know that f and f' are coprime. By Euclid there are some polynomials u, $v \in \mathbb{Q}[x]$ such that

$$u(x)f(x) + v(x)f'(x) = 1. \tag{3}$$

However, $\beta \in \mathbb{C}$ is a repeated root of f. Thus

$$f(x) = (x - \beta)^2 g(x)$$

where $g(x)$ is a polynomial with coefficients in $\mathbb{C}$. Differentiating we see that

$$f'(x) = (x-\beta)^2 g'(x) + 2(x-\beta)g(x).$$

It is clear that $f(\beta) = f'(\beta) = 0$. Substituting β for x in (3) gives $0 = 1$ which is a contradiction. □

Example 6.1. By Theorem 5, $f = X^2 - 3$ is the minimal polynomial of $\sqrt{3}$. Thus the conjugates of $\sqrt{3}$ are $\sqrt{3}$ and $-\sqrt{3}$.

7. Factorization of Polynomials

So far we have concerned ourselves with minimal polynomials of algebraic integers and have neglected algebraic integers. To recall, we say $\alpha \in \mathbb{C}$ is an algebraic integer if there exists some monic polynomial f with coefficients in $\mathbb{Z}$ such that $f(\alpha) = 0$. Of course, algebraic integers are algebraic numbers and so anything that applies to algebraic numbers must apply to algebraic integers. It is however natural to ask, if the minimal polynomial of an algebraic integer must have coefficients in $\mathbb{Z}$. Notice, that there is no reason a priori (on the basis of the above definition) to expect this. We do not know that the polynomial f is minimal. We know that α has some minimal polynomial f_α which is monic, has rational coefficients, is irreducible and satisfies $f_\alpha(\alpha) = 0$. As to the relationship between f_α and the polynomial f in the above definition, all we can conclude is that $f_\alpha \mid f$. Since f has integral coefficients, should we expect that f_α has rational coefficients. It turns out that the answer is yes. For this we need the following theorem of Gauss.

Theorem 7. *(Gauss) Suppose f is a polynomial with coefficients in $\mathbb{Z}$. Suppose that $f(x) = g(x)h(x)$ where g, h are polynomials with coefficients in $\mathbb{Q}$. Then there is some non-zero rational number λ such that $g^* = \lambda g$ and $h^* = \lambda^{-1}$ both have coefficients in $\mathbb{Z}$, and therefore we may factorize f over $\mathbb{Z}$ as $f = g^* h^*$.*

Before proving Gauss' Theorem we need the following Lemma.

Lemma 7.1. *Suppose R is an integral domain. Then $R[x]$ is also an integral domain.*

Proof. Suppose R is an integral domain. Suppose f, g are non-zero elements of $R[x]$. We would like to show that fg is also non-zero. For this write

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0, \qquad a_0, \ldots, a_m \in R,$$

and

$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0 \qquad b_0, \ldots, b_n \in R,$$

with $a_m \neq 0$, $b_n \neq 0$. Thus

$$f(x)g(x) = a_m b_n x^{m+n} + \text{lower terms}.$$

As R is an integral domain and a_m, b_n are non-zero we see that $a_m b_n \neq 0$. Thus fg is non-zero as required. □

We may now return to prove Gauss' Theorem.

Proof of Theorem 7. By clearing denominators we may write

$$nf(x) = g_1(x)h_1(x) \tag{4}$$

where n is a positive integer and g_1, h_1 are polynomials with coefficients in $\mathbb{Z}$ which are multiples of g, h. Write

$$g_1(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0, \qquad h_1(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0,$$

where the coefficients are in $\mathbb{Z}$.

We will eliminate the prime factors of n, one at a time, until we reach the desired factorization $f = g^* h^*$ where g^* and h^* have coefficients in $\mathbb{Z}$.

If $n = 1$ then of course there is nothing to prove. Suppose $n > 1$ and let p be any prime factor n. Reducing (4) modulo p we obtain

$$0 = \overline{g_1}(x)\overline{h_1}(x) \tag{5}$$

where

$$g_1(x) = \overline{a_m}x^m + \overline{a_{m-1}}x^{m-1} + \cdots + \overline{a_0}, \qquad h_1(x) = \overline{b_n}x^n + \overline{b_{n-1}}x^{n-1} + \cdots + \overline{b_0}.$$

The equality (5) takes place in $\mathbb{F}_p[x]$. But $\mathbb{F}_p$ is an integral domain (indeed it is a field), and so by the above Lemma $\mathbb{F}_p[x]$ is an integral domain. Hence either $\overline{g_1} = 0$ or $\overline{h_1} = 0$. Without loss of generality, let us say that $\overline{g_1} = 0$. This means that all the coefficients of g_1 are divisible by p. Let $g_2 = g_1/p$; this has integral coefficients. Let $h_2 = h_1$. Thus

$$n' f = g_2 h_2$$

where $n' = n/p$ and g_2, h_2 have coefficients in $\mathbb{Z}$. We repeat this until we have eliminated all prime factors of n. □

We now deduce our desired result.

Theorem 8. *Suppose α is an algebraic number. Then alpha is an algebraic integer if and only if its minimal polynomial f_α has coefficients in $\mathbb{Z}$.*

Proof. If f_α has integral coefficients, then α is an algebraic integer by the very definition of algebraic integers.

Conversely suppose that α is an algraic integer. By definition, $h(\alpha) = 0$ for some monic polynomial h with coefficients in $\mathbb{Z}$. By Lemma 5.1 we know that $f_\alpha \mid h$. Thus we may write

$$h(x) = f_\alpha(x) g(x)$$

where $g(x) \in \mathbb{Q}[x]$. By Gauss' Theorem above, there is some non-zero rational λ such that λf_α and $\lambda^{-1} g(x)$ both have integral coefficients. But both h and f_α are monic, and therefore g is monic. Examining the leading coefficients of λf_α and $\lambda^{-1} g(x)$ we see that both λ and λ^{-1} are integers. Thus $\lambda = \pm 1$. Hence $\pm f_\alpha(x)$ has integral coefficients which implies that $f_\alpha(x)$ has integral coefficients, as desired. □

8. Eisenstein's Criterion For Irreducibility

Theorem 9. *Let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

be a polynomials with coefficients in $\mathbb{Z}$, satisfying the following three conditions:

(i) $p \nmid a_n$;
(ii) $p \mid a_i$ *for* $1 \leq i \leq n-1$;
(iii) $p^2 \nmid a_0$.

Then f is irreducible over $\mathbb{Q}$.

Proof. We prove this by contradiction. Suppose that f is not irreducible over $\mathbb{Q}$. By Gauss' Theorem we know that $f(x) = g(x)h(x)$ where g, h are polynomials with coefficients in $\mathbb{Z}$ and degrees strictly less than that of f. Write

$$g(x) = b_r x^r + \cdots + b_0, \qquad h(x) = c_s x^s + \cdots + c_0.$$

Note that $n = r + s$ and $a_n = b_r c_s$. By assumption (i), a_n is not divisible by p and so neither b_r nor c_s are. Reducing the identity $f(x) = g(x)h(x)$ modulo p we obtain (using (ii))

$$\overline{g}(x)\overline{h}(x) = \overline{a_n}x^n;$$

here the equality takes place in $\mathbb{F}_p[x]$. The only possible way to factorize x^n as a product of two factors is $x^u x^v$ for some positive u, v satisfying $u+v = n$. However, $\overline{g}(x)$, $\overline{h}(x)$ are polynomials of degrees r, s with leading coefficients $\overline{b_r}$, $\overline{c_s}$ respectively. We deduce that

$$\overline{g}(x) = \overline{b_r}x^r, \qquad \overline{h}(x) = \overline{c_s}x^s.$$

Comparing the coefficients of g, h with those of $\overline{g}$, $\overline{h}$ we see that $p \mid b_0$ and $p \mid c_0$. However, $a_0 = b_0 c_0$. Thus $p^2 \mid a_0$ contradicting (iii). □

Example 8.1. Let $f(x) = x^7 - 9x + 3$. Letting $p = 3$ in Eisenstein's criterion, we immediately see that f is irreducible.

Many polynomials do not immediatly satisfy the conditions of Eisenstein's criterion, but do satisfy them after making an appropriate substitution. For example, take $g(X) = 8x^3 - 6x + 1$. Eisenstein's criterion does not apply to g regardless of the prime p chosen. Now let

$$h(x) = g(x+1) = 8(x+1)^3 - 6(x+1) + 1 = 8x^3 + 24x^2 + 18x + 3.$$

We see that Eisenstein's criterion applies to h with $p = 3$. Thus h is irreducible. But if g was reducible then h would also be reducible because of the relation $h(x) = g(x+1)$. Hence g is irreducible.

9. Symmetric Polynomials

This section is based on the corresponding section in Stewart and Tall.

Let $\mathbb{Z}[t_1, \ldots, t_n]$ be the ring of polynomials in indeterminants $t_1, \ldots, t_n$ with coefficients in $\mathbb{Z}$. Let S_n be the symmetric group of permutations on the set $\{1, 2, \ldots, n\}$. For any permutation $\pi \in S_n$ and any polynomial $f \in \mathbb{Z}[t_1, \ldots, t_n]$ we define the polynomial f^π by

$$f^\pi(t_1, \ldots, t_n) = f(t_{\pi(1)}, \ldots, t_{\pi(n)}).$$

For example, if $n = 5$, $f = t_1 + t_2 t_3 + t_4^2 - t_5$ and $\pi = (132)(45)$ then $f^\pi = t_3 + t_1 t_2 + t_5^2 - t_4$.

Definition. *We call a polynomial $f \in \mathbb{Z}[t_1, \ldots, t_n]$* **symmetric** *if $f^\pi = f$ for all $\pi \in S_n$.*

For example, if $n = 3$, then $t_1 + t_2 + t_3$ and $t_1 t_2 t_3$ are symmetric. Perhaps less obvious is the fact that $t_1 t_2 + t_2 t_3 + t_3 t_1$ is also symmetric. For general n, we define

$$s_1 = \sum_{i=1}^{n} t_i, \quad s_2 = \sum_{1 \le i < j \le n} t_i t_j, \quad s_3 = \sum_{1 \le i < j < k \le n} t_i t_j t_k, \quad \ldots, \quad s_n = t_1 t_2 \ldots t_n.$$

The polynomials $s_1, \ldots, s_n$ are called the *elementary symetric polynomials* in $t_1, \ldots, t_n$. Note the identity

$$(X - t_1)(X - t_2)\ldots(X - t_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n.$$

If we act on $t_1, \ldots, t_n$ by any permutation $\pi \in S_n$ then we will leave the left-hand side of this identity unchanged, and so the coefficients on the right-hand must be unchanged. This shows that the s_i are indeed symmetric functions.

It is easy to see that any polynomial in $s_1, \ldots, s_n$ with coefficients in $\mathbb{Z}$ is a symmetric function of $t_1, \ldots, t_n$. We would like to prove the converse.

Theorem 10. *(Newton) Every symmetric polynomial in $\mathbb{Z}[t_1, \ldots, t_n]$ is expressible as a polynomial in $s_1, \ldots, s_n$ with coefficients in $\mathbb{Z}$.*

Before proving the theorem, we will give an example to illustrate what we mean.

Example 9.1. Let $n = 2$. The polynomial

$$f = t_1^2 + t_2^2$$

is obviously symmetric. We can rewrite it as

$$f = t_1^2 + t_2^2 = (t_1 + t_2)^2 - 2t_1 t_2 = s_1^2 - 2s_2.$$

Hence f can be written as a polynomial in s_1, s_2 with coefficients in $\mathbb{Z}$.

Proof of Theorem 10. We give a constructive argument for writing a symmetric polynomial in terms of $s_1, \ldots, s_n$. First we define an ordering on the monomials $t_1^{a_1} \cdots t_n^{a_n}$. We will order the monomials 'lexicographically':

$$t_1^{a_1} \cdots t_n^{a_n} \succcurlyeq t_1^{b_1} \cdots t_n^{b_n} \qquad \text{iff} \qquad \begin{cases} a_1 > b_1, \\ \text{or } a_1 = b_1 \text{ and } a_2 > b_2, \\ \text{or } a_1 = b_1 \text{ and } a_2 = b_2 \text{ and } a_3 > b_3, \\ \text{etc.} \end{cases}$$

Suppose that f is a symmetric polynomial and let $ct_1^{a_1} \ldots t_n^{a_n}$ be the monomial appearing in f which is biggest according to the lexicographic ordering. We claim $a_1 \geq a_2$; suppose otherwise that $a_1 < a_2$. Since f is symmetric, f also has the monomial $ct_1^{a_2} t_2^{a_1} t_3^{a_3} \ldots t_n^{a_n}$ and this is bigger than $ct_1^{a_1} \ldots t_n^{a_n}$ giving a contradiction. Therefore $a_1 \geq a_2$ and similarly $a_2 \geq a_3$ and so on. In other words

$$a_1 \geq a_2 \geq a_3 \geq \cdots \geq a_n.$$

Now write

$$k_1 = a_1 - a_2, \quad k_2 = a_2 - a_3, \ldots, \quad k_{n-1} = a_{n-1} - a_n, \quad k_n = a_n.$$

These are all non-negative since $a_1 \geq a_2 \geq a_3 \geq \cdots a_n$. Consider

$$s_1^{k_1} s_2^{k_2} \ldots s_n^{k_n} = (t_1 + \cdots + t_n)^{k_1} (t_1 t_2 + \ldots)^{k_2} \ldots (t_1 \ldots t_n)^{k_n}.$$

The biggest monomial in this expression is

$$t_1^{k_1} (t_1 t_2)^{k_2} (t_1 t_2 t_3)^{k_3} \cdots = t_1^{k_1 + k_2 + \cdots + k_n} t_2^{k_2 + \cdots + k_n} \ldots t_n^{k_n} = t_1^{a_1} t_2^{a_2} \cdots t_n^{a_n}.$$

Therefore, the biggest monomials in f and in $cs_1^{k_1} s_2^{k_2} \ldots s_n^{k_n}$ are the same, and the polynomial

$$f_2 = f - cs_1^{k_1} s_2^{k_2} \ldots s_n^{k_n}$$

will contain only smaller monomials. Our objective was to show that f can be written as a polynomial in $s_1, \ldots s_n$ with coefficients in $\mathbb{Z}$. It is sufficient to do that

for f_2 which has a smaller leading monomial. We apply the argument recursively to obtain a sequence of polynomails $f_1 = f, f_2, f_3, \dots$ each with a smaller leading monomial; moreover the leading monomial will always be of the shape

$$t_1^{u_1} t_2^{u_2} \dots t_n^{u_n}, \qquad u_1 \geq u_2 \geq \dots \geq u_n \geq 0.$$

Clearly this process will stop eventually, leaving us with a a polynomial in $s_1, \dots s_n$ with integer coefficients. □

Example 9.2. Express $f = t_1^2 t_2^2 + t_2^2 t_3^2 + t_3^2 t_1^2$ in terms of elementary symmetric functions.

Answer: We follow the recipe in the above proof. The biggest monomial of f is $t_1^2 t_2^2$. Hence $a_1 = 2$, $a_2 = 2$, $a_3 = 0$. Thus $k_1 = 2 - 2 = 0$, $k_2 = 2 - 0 = 2$, $k_3 = 0$. The above recipe suggests that we subtract $s_1^0 s_2^2 s_3^0 = s_2^2$:

$$f - s_2^2 = t_1^2 t_2^2 + t_2^2 t_3^2 + t_3^2 t_1^2 - (t_1 t_2 + t_2 t_3 + t_3 t_1)^2 = -2t_1^2 t_2 t_3 - 2t_2^2 t_1 t_3 - 2t_3^2 t_1 t_2.$$

The biggest monomial now is $-2t_1^2 t_2 t_3$. Here $a_1 = 2$, $a_2 = 1$, $a_3 = 1$. Thus $k_1 = 2 - 1 = 1$, $k_2 = 1 - 1 = 0$ and $k_3 = 1$. We subtract $-2s_1^1 s_2^0 s_3^1$. In other words, we add $2s_1 s_3$:

$$f - s_2^2 + 2s_1 s_3 = 0.$$

It follows that $f = s_2^2 + 2s_1 s_3$.

10. Algebraic Integers form a Ring

We defined $\mathcal{O}$ to be the set of algebraic integers. In this section we show that $\mathcal{O}$ is a subring of $\mathbb{C}$. We recall first the elementary symmetric polynomials in indeterminants $t_1, \dots, t_n$:

$$s_1 = \sum_{i=1}^{n} t_i, \quad s_2 = \sum_{1 \leq i < j \leq n} t_i t_j, \quad s_3 = \sum_{1 \leq i < j < k \leq n} t_i t_j t_k, \quad \dots, \quad s_n = t_1 t_2 \dots t_n.$$

Theorem 11. *Suppose α is an algebraic integer of degree n and let $\alpha_1, \dots, \alpha_n$ be its conjugates. Let $h(t_1, \dots, t_n) \in \mathbb{Z}[t_1, \dots, t_n]$ be a symmetric polynomial. Then $h(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$.*

For the proof of the theorem we need the following lemma, which in fact is a special case of the theorem.

Lemma 10.1. *Suppose α is an algebraic integer of degree n and let $\alpha_1, \dots, \alpha_n$ be its conjugates. Let $s_1, \dots, s_n$ be the elementary symmetric polynomials in $t_1, \dots, t_n$ as above. Then*

$$s_1(\alpha_1, \dots, \alpha_n), \quad s_2(\alpha_1, \dots, \alpha_n), \dots, s_n(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}.$$

Proof. Recall the identity

$$(X - t_1)(X - t_2) \dots (X - t_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \dots + (-1)^n s_n.$$

Now substitute $\alpha_1, \dots, \alpha_n$ for $t_1, \dots, t_n$. We obtain

$$(X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_n) =$$
$$X^n - s_1(\alpha_1, \dots, \alpha_n) X^{n-1} + s_2(\alpha_1, \dots, \alpha_n) X^{n-2} - \dots + (-1)^n s_n(\alpha_1, \dots, \alpha_n).$$

Since $\alpha_1, \dots, \alpha_n$ are the conjugates of α, we recognize the polynomial on the left as the minimal polynomial of α. As α is an algebraic integer, its minimal polynomial has integral coefficients, and the lemma follows. □

Proof of Theorem 11. Suppose $h(t_1, \ldots, t_n) \in \mathbb{Z}[t_1, \ldots, t_n]$ is symmetric. By Newton's Theorem (Theorem 10), h can be expressed as a polynomial in $s_1, \ldots, s_n$ with coefficients in $\mathbb{Z}$. Lemma 10.1 tells us that

$$s_1(\alpha_1, \ldots, \alpha_n), \quad s_2(\alpha_1, \ldots, \alpha_n), \ldots, s_n(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}.$$

Hence $h(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$. □

We are now ready to prove our goal.

Theorem 12. *The set of algebraic integers $\mathcal{O}$ is a subring of $\mathbb{C}$.*

Proof. We know that $\mathbb{Z} \subset \mathcal{O}$, therefore $\mathcal{O} \neq \emptyset$. To show that $\mathcal{O}$ is a subring, it is enought to show that if α, $\beta \in \mathcal{O}$ then $\alpha + \beta$, $-\alpha$, $\alpha\beta \in \mathcal{O}$.

Suppose α, $\beta \in \mathcal{O}$ and let us prove that $\alpha + \beta \in \mathcal{O}$. To do this we construct a monic polynomial h with coefficients in $\mathbb{Z}$ such that $h(\alpha + \beta) = 0$. First let

$$f_\alpha(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

be the minimal polynomial of α. Suppose β has degree n and let $\beta_1, \ldots, \beta_n$ be its conjugates where we take $\beta_1 = \beta$. Consider the product

(6)
$$f_\alpha(x-t_1)f_\alpha(x-t_2)\ldots f_\alpha(x-t_n) = x^{mn}+u_{mn-1}(t_1, \ldots, t_n)x^{mn-1}+\cdots+u_0(t_1, \ldots, t_n).$$

As f_α has coefficients in $\mathbb{Z}$, it is clear that $u_i(t_1, \ldots, t_n) \in \mathbb{Z}[t_1, \ldots, t_n]$. Note that if we permute the t_j then we permute the factors of the left-hand side of (6), and so the product is unchanged. Hence the coefficients $u_i(t_1, \ldots, t_n)$ are unchanged on permuting the t_j; in other words they are symmetric polynomials. By Theorem 11 we deduce that

$$u_i(\beta_1, \ldots, \beta_n) \in \mathbb{Z}. \tag{7}$$

Now substitute $\beta_1, \ldots, \beta_n$ for $t_1, \ldots, t_n$ in (6), and let $h(x)$ be the resulting polynomial. We obtain

$$\begin{aligned} h(x) &= f_\alpha(x - \beta_1)f_\alpha(x - \beta_2)\ldots f_\alpha(x - \beta_n) \\ &= x^{mn} + u_{mn-1}(\beta_1, \ldots, \beta_n)x^{mn-1} + \cdots + u_0(\beta_1, \ldots, \beta_n). \end{aligned}$$

Now $h(x)$ is monic. Moreover, $h(x) \in \mathbb{Z}[x]$ by (7). Finally,

$$\begin{aligned} h(\alpha + \beta) &= f_\alpha(\alpha + \beta - \beta_1)f_\alpha(\alpha + \beta - \beta_2)\ldots f_\alpha(\alpha + \beta - \beta_n) \\ &= f_\alpha(\alpha)f_\alpha(\alpha + \beta - \beta_2)\ldots f_\alpha(\alpha + \beta - \beta_n) \quad \text{since } \beta_1 = \beta \\ &= 0 \cdot f_\alpha(\alpha + \beta - \beta_2)\ldots f_\alpha(\alpha + \beta - \beta_n) = 0. \end{aligned}$$

This shows indeed that $\alpha + \beta \in \mathcal{O}$.

The proofs that $-\alpha$ and $\alpha\beta \in \mathcal{O}$ are left as exercises. □

Example 10.1. Let α be a root of the polynomial x^3+4x+2. What is the minimal polynomial of $\alpha + \sqrt{2}$?

Answer: Note that the polynomial $f(x) = x^3+4x+2$ is irreducible by Eisenstein's criterion (take $p = 2$). Hence it is the minimal polynomial of α. We follow the steps in the above proof taking $\beta = \sqrt{2}$. The conjugates of β are $\beta_1 = \sqrt{2}$ and $\beta_2 = -\sqrt{2}$.

Then $\alpha+\beta$ is a root of

$$\begin{aligned} h(x) &= f(x-\beta_1)f(x-\beta_2) \\ &= f(x-\sqrt{2})f(x+\sqrt{2}) \\ &= \left((x^3+10x+2)-(3x^2+6)\sqrt{2}\right)\left((x^3+10x+2)+(3x^2+6)\sqrt{2}\right) \\ &= (x^3+10x+2)^2-2(3x^2+6)^2 \\ &= x^6+2x^4+4x^3+28x^2+40x-68. \end{aligned}$$

We haven't proved that h is the minimal polynomial for $\alpha+\sqrt{2}$. To do this we must show that h is irreducible, which we leave as an exercise for the reader.

11. Algebraic Numbers form a Field

Theorem 13. *The set of algebraic numbers $\overline{\mathbb{Q}}$ is in fact a subfield of $\mathbb{C}$.*

Proof. We know that $\mathbb{Q}\subset\overline{\mathbb{Q}}$. Hence $\overline{\mathbb{Q}}$ is non-empty. We need to show that if α, β are in $\overline{\mathbb{Q}}$, then so are $\alpha+\beta$, $-\alpha$, $\alpha\beta$ and α^{-1} (for non-zero α). The last we showed in Lemma 4.2. The first three are similar to the corresponding proofs for algebraic integers and so we leave them to the reader. □

12. Number Fields

Suppose L is a field and K a subfield. It is easy to see that L is a vector space over K (you can add and subtract elements of L, and you can multiply them by elements of K—check that the vector space axioms follow from the field axioms). We denote the dimension of L regarded as a vector space over K by $[L:K]$, and we say that L is a *field extension of K of degree $[L:K]$*. If the degree $[L:K]$ is finite, we say that L *is a finite extension of K*. Notice that this phrase does not mean that the field L is finite (like $\mathbb{F}_p$) but that L, as a vector space over K, has finite dimension.

We finally come to the main object of study of algebraic number theory.

Definition. *A* **number field** *K is a subfield of $\mathbb{C}$ that is a finite extension of $\mathbb{Q}$. The* **degree** *of K is $[K:\mathbb{Q}]$.*

A **quadratic number field** *is a number field of degree 2, a* **cubic number field** *is a number field of degree 3 and so on.*

Notice that any subfield K of $\mathbb{C}$ will contain contain the rationals. To see this note first that $1\in K$ because K is a subfield. Now repeated addition of 1 will show that the natural numbers are in K, and 'minusing' that the integers are in K. Taking ratios shows that the rationals are contained in K. However we do not call K a number field unless it is a finite extension of $\mathbb{Q}$.

Example 12.1. In previous courses you probably defined

$$\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\ :\ a,b\in\mathbb{Q}\},$$

and proved that this is a field. We see that 1, $\sqrt{2}$ is a basis for $\mathbb{Q}(\sqrt{2})$ as a $\mathbb{Q}$-vector space. Hence $\mathbb{Q}(\sqrt{2})$ is a number field of degree 2; in other words it is a quadratic number field.

Definition. *Suppose α is an algebraic number. Define*

$$\mathbb{Q}(\alpha) = \left\{ \frac{g(\alpha)}{h(\alpha)} \ : \ g, h \in \mathbb{Q}[x],\ h(\alpha) \neq 0 \right\}.$$

We call $\mathbb{Q}(\alpha)$ the field generated by α.

Exercise 12.2. Check that $\mathbb{Q}(\alpha)$ is indeed a field.

Theorem 14. *Suppose α is an algebraic number of degree n. Then $\mathbb{Q}(\alpha)$ is a number field of degree n. The set $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha)$.*

In other words, every element of $\mathbb{Q}(\alpha)$ can be expressed uniquely as a linear combination of $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. This shows that our old definition of $\mathbb{Q}(\sqrt{2})$ is consistent with the new one.

Proof of Theorem 14. It is sufficient to show that the set $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha)$. Suppose $\beta \in \mathbb{Q}(\alpha)$ we would like to show that β can be written as a $\mathbb{Q}$-linear combination of $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. By definition of $\mathbb{Q}(\alpha)$, we know that $\beta = g(\alpha)/h(\alpha)$ where g, $h \in \mathbb{Q}[x]$ and $h(\alpha) \neq 0$.

Our first step is to invert $h(\alpha)$. Let f_α be the minimal polynomial of α. Then $h(\alpha) \neq 0$ implies that $f_\alpha \nmid h$; since f_α is irreducible we deduce that f_α and h are coprime. By Euclid there exists polynomials u, $v \in \mathbb{Q}[x]$ such that

$$u(x)h(x) + v(x)f_\alpha(x) = 1.$$

Substituting α for x we obtain $u(\alpha) = 1/h(\alpha)$. Hence $\beta = g(\alpha)/h(\alpha) = g(\alpha)u(\alpha)$. Let $w(x) = g(x)u(x) \in \mathbb{Q}[x]$. Thus $\beta = w(\alpha)$. Thus we have written β as a polynomial in α. In other words, we have written β as a linear combination of $1, \alpha, \alpha^2, \ldots \alpha^m$ where m is the degree of w. Our problem is that m might be greater than $n-1$.

Recall that n is the degree of α. We know that this is also the degree of f_α. By Euclid again we know that there are two polynomials q, $r \in \mathbb{Q}[x]$ such that

$$w(x) = q(x)f_\alpha(x) + r(x), \qquad \deg(r) < \deg(f).$$

Since $\deg(r) < \deg(f) = n$ we can write

$$r(x) = a_0 + a_1 x + \cdots a_{n-1}x^{n-1}, \qquad a_i \in \mathbb{Q}.$$

Substitute α for x to obtain

$$\beta = w(\alpha) = r(\alpha) = a_0 + a_1\alpha + \cdots a_{n-1}\alpha^{n-1}.$$

Thus every element of $\mathbb{Q}(\alpha)$ can be written as a $\mathbb{Q}$-linear combination of $1, \alpha, \ldots, \alpha^{n-1}$.

To complete the proof that $1, \alpha, \ldots, \alpha^{n-1}$ is a basis, we must of course show that it is linearly independent. We leave this to the reader. □

To make sure you understood the proof of the above theorem, do the following exercise.

Exercise 12.3. Let $f(X) = X^3 + X^2 + 1$.

(i) Show that f is irreducible.

(ii) Let θ be a root of f and $K = \mathbb{Q}(\theta)$. Write the following elements as $\mathbb{Q}$-linear combinations of 1, θ, θ^2:

$$(\theta+1)^4, \qquad \frac{1}{\theta^2 - 1}, \qquad \frac{\theta+1}{\theta^2+1}.$$

Theorem 15. *(Primitive Element Theorem) Suppose K is an number field of degree n. Then $K = \mathbb{Q}(\alpha)$ for some algebraic number α of degree n.*

Proof. This will be proved in the Galois Theory course. □

13. Fields Generated by Conjugate Elements

Theorem 16. *Suppose that α is an algebraic number and $f_\alpha(x)$ is its minimal polynomial. Then we have an isomorphism of fields*

$$\mathbb{Q}[x]/(f_\alpha(x)) \cong \mathbb{Q}(\alpha),$$

explicitly given by

$$\phi:\ \mathbb{Q}[x]/(f_\alpha(x)) \to \mathbb{Q}(\alpha), \qquad \phi\left(x + (f_\alpha(x))\right) = \alpha.$$

Proof. Define the map

$$\psi:\ \mathbb{Q}[x] \to \mathbb{Q}(\alpha), \qquad \psi(g(x)) = g(\alpha).$$

The map ψ is an homomorphism of rings (check). By the First Isomorphism Theorem we have that

$$\mathbb{Q}[x]/\mathrm{Ker}(\psi) \cong \mathrm{Im}(\psi).$$

We need to calculate the kernel and the image.

Now $g(x) \in \mathrm{Ker}(\psi)$ if and only if $g(\alpha) = 0$. This is equivalent to $f_\alpha \mid g$ which in turn is equivalent to $g \in (f_\alpha)$. Hence

$$\mathrm{Ker}(\psi) = (f_\alpha(x)).$$

We claim that $\mathrm{Im}(\psi) = \mathbb{Q}(\alpha)$ (in other words the map ψ is surjective). To see this, suppose that $\beta \in \mathbb{Q}(\alpha)$. By Theorem 14 we can write

$$\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, \qquad a_i \in \mathbb{Q}.$$

Let $g(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$. Then

$$\psi(g(x)) = g(\alpha) = \beta.$$

In other words $\beta \in \mathrm{Im}(\psi)$, showing that ψ is surjective.

We now deduce that

$$\mathbb{Q}[x]/(f_\alpha(x)) \cong \mathbb{Q}(\alpha).$$

To complete the proof, we must determine the isomorphism explicitely. The explicit isomorphism we gave in the statement of the theorem comes from the proof of the First Isomorphism Theorem. □

Corollary 13.1. *Suppose that α, α' are conjugates (i.e. algebraic numbers having the same minimal polynomial). Then the fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\alpha')$ are isomorphic; indeed there is a unique isomorphism*

$$\mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha')$$

fixing $\mathbb{Q}$ and satisfying $\alpha \mapsto \alpha'$.

Proof. From Theorem 16 we have isomorphisms

$$\phi:\ \mathbb{Q}[x]/(f_\alpha(x)) \to \mathbb{Q}(\alpha), \qquad \phi\left(x + (f_\alpha(x))\right) = \alpha.$$

and

$$\phi':\ \mathbb{Q}[x]/(f_\alpha(x)) \to \mathbb{Q}(\alpha'), \qquad \phi'\left(x + (f_\alpha(x))\right) = \alpha'.$$

Then $\phi' \circ \phi^{-1}$ is the required isomorphism. □

Example 13.1. Let $K = \mathbb{Q}(\sqrt{2})$. Then $\sqrt{2}$ has minimal polynomial $x^2 - 2$. Hence the conjugates of $\sqrt{2}$ are $\sqrt{2}$ and $-\sqrt{2}$. Now $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$. We know from the above that the map

$$\sigma : \ K \to K, \qquad a + b\sqrt{2} \mapsto a - b\sqrt{2} \qquad \text{for all } a, b \in \mathbb{Q}$$

is an isomorphism of fields. The reader might want to check this directly. Notice also that $\sigma(a) = a$ for all $a \in \mathbb{Q}$. Hence σ fixes the rationals.

14. Embeddings

Lemma 14.1. *Let $f \in \mathbb{R}[x]$ and let $\gamma \in \mathbb{C}$ be a root of f. The $\overline{\gamma}$ (the complex conjugate of γ) is also a root of f.*

Proof. Write

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0, \qquad a_i \in \mathbb{R}.$$

But $f(\gamma) = 0$, so

$$\begin{aligned} 0 &= \overline{f(\gamma)} \\ &= \overline{a_n \gamma^n + \cdots + a_0} \\ &= \overline{a_n} \cdot \overline{\gamma}^n + \cdots \overline{a_0} \\ &= a_n \overline{\gamma}^n + \cdots + a_0 \qquad \text{since } a_i \in \mathbb{R} \\ &= f(\overline{\gamma}). \end{aligned}$$

Hence $\overline{\gamma}$ is a root of f. □

Suppose α is an algebraic number and let $\alpha_1, \ldots, \alpha_n$ be its conjugates. By definition, the α_i are the roots of $f_\alpha(x) \in \mathbb{Q}[x]$. By the above Lemma, $\overline{\alpha_i}$ is again of one $\alpha_1, \ldots, \alpha_n$. This means that either α_i is real, or if it is not real then its complex conjugate must be included in the list $\alpha_1, \ldots, \alpha_n$. It is traditional to reorder $\alpha_1, \ldots, \alpha_n$ as follows

$$\alpha_1, \ldots, \alpha_r, \quad \alpha_{r+1}, \ldots, \alpha_{r+s}, \quad \alpha_{r+s+1}, \ldots, \alpha_{r+2s},$$

where $\alpha_1, \ldots, \alpha_r$ are real, the others are non-real complexes, and

$$\overline{\alpha_{r+1}} = \alpha_{r+s+1}, \qquad \overline{\alpha_{r+2}} = \alpha_{r+s+2}, \qquad \overline{\alpha_{r+s}} = \alpha_{r+2s}.$$

Note that $n = r + 2s$ where r is the number of real conjugates of α and s is the number of *pairs* of complex conjugates of α.

Now Corollary 13.1 shows that $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\alpha_i)$ for $i = 1, \ldots, n$. However, for $i = 1, \ldots, r$ we have $\mathbb{Q}(\alpha_i) \subset \mathbb{R}$. Thus composing the isomorphism $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\alpha_i)$ with the inclusion $\mathbb{Q}(\alpha_i) \subset \mathbb{R}$ we obtain an embedding

$$\sigma_i : \ \mathbb{Q}(\alpha) \hookrightarrow \mathbb{R}, \qquad \sigma_i(\alpha) = \alpha_i.$$

An *embedding* (denoted by the hook arrow $\hookrightarrow$) is an injective homomorphism. We call $\sigma_1, \ldots, \sigma_r$ the real embeddings of $K = \mathbb{Q}(\alpha)$.

For $i = r + 1, \ldots, r + 2s$ we define the complex embeddings

$$\sigma_i : \ \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}, \qquad \sigma_i(\alpha) = \alpha_i.$$

Note that

$$\overline{\sigma_i(\beta)} = \sigma_{i+s}(\beta)$$

for all $i = r + 1, \ldots, r + s$ and all $\beta \in K$.

Example 14.1. Let $K = \mathbb{Q}(\sqrt{2})$. Since $\sqrt{2}$ has exactly two real conjugates, $\sqrt{2}$, $-\sqrt{2}$, we have $r = 2$, $s = 0$. The real embeddings are

$$\sigma_1 : K \hookrightarrow \mathbb{R}, \qquad \sigma_2 : K \hookrightarrow \mathbb{R}$$

where

$$\sigma_1(a + b\sqrt{2}) = a + b\sqrt{2}, \qquad \sigma_2(a + b\sqrt{2}) = a - b\sqrt{2}$$

for all $a, b \in \mathbb{Q}$.

Example 14.2. Let $K = \mathbb{Q}(\sqrt{-3})$. Since $\sqrt{-3}$ has exactly two complex, non-real, conjugates, $\sqrt{-3}$, $-\sqrt{-3}$, we have $r = 0$, $s = 1$. The complex embeddings are

$$\sigma_1 : K \hookrightarrow \mathbb{C}, \qquad \sigma_2 : K \hookrightarrow \mathbb{C}$$

where

$$\sigma_1(a + b\sqrt{-3}) = a + b\sqrt{-3}, \qquad \sigma_2(a + b\sqrt{-3}) = a - b\sqrt{-3}$$

for all $a, b \in \mathbb{Q}$.

Example 14.3. Let $K = \mathbb{Q}(\sqrt[3]{2})$. The minimal polynomial of $\sqrt[3]{2}$ is $f(x) = x^3 - 2$. Write $\omega = \exp(2\pi i/3)$. Then f has three roots

$$\alpha_1 = \sqrt[3]{2}, \qquad \alpha_2 = \omega\sqrt[3]{2}, \qquad \alpha_3 = \omega^2\sqrt[3]{2},$$

and so these are the conjugates of $\sqrt[3]{2}$. The first is real and the other two are complex conjugates. Hence $r = 1$, $s = 1$. We have embeddings

$$\sigma_1 : K \hookrightarrow \mathbb{R}, \qquad \sigma_2 : K \hookrightarrow \mathbb{C}, \qquad \sigma_3 : K \hookrightarrow \mathbb{C}$$

where

$$\begin{aligned}
\sigma_1\left(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2\right) &= a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2, \\
\sigma_2\left(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2\right) &= a + b\omega\sqrt[3]{2} + c\omega^2(\sqrt[3]{2})^2, \\
\sigma_3\left(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2\right) &= a + b\omega^2\sqrt[3]{2} + c\omega(\sqrt[3]{2})^2,
\end{aligned}$$

for all $a, b, c \in \mathbb{Q}$.

15. Field Polynomial

We continue with the notation of the previous section: $K = \mathbb{Q}(\alpha)$ is a number field of degree n and $\sigma_1, \ldots, \sigma_n$ are the embeddings of K.

Definition. *Let $\beta \in K$. We call $\sigma_1(\beta), \ldots, \sigma_n(\beta)$ the K-conjugates of β.*

We define the field polynomial $F_\beta(x)$ by

$$F_\beta(x) = \prod_{i=1}^{n} (x - \sigma_i(\beta)) .$$

We define the K-norm by

$$N_K(\beta) = \prod_{i=1}^{n} \sigma_i(\beta)$$

and the K-trace of β by

$$\mathrm{Tr}_K(\beta) = \sum_{i=1}^{n} \sigma_i(\beta)$$

Example 15.1. Suppose d is a square-free integer, $d \neq 0, 1$. Let $K = \mathbb{Q}(\sqrt{d})$. By Theorem 14 any element $\beta \in K$ can expressed uniquely in the form $\beta = a + b\sqrt{d}$ for some a, $b \in \mathbb{Q}$. The embeddings σ_1, σ_2 satisfy

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}, \qquad \sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}.$$

Note that σ_1, σ_2 are both real if $d > 0$ and both complex if $d < 0$. Thus the K-conjugates of $\beta = a + b\sqrt{d}$ are $a + b\sqrt{d}$ and $a - b\sqrt{d}$.

The field polynomial of $\beta = a + b\sqrt{d}$ is

$$\begin{aligned} F_\beta(x) &= (x - \sigma_1(\beta))\,(x - \sigma_2(\beta)) \\ &= x^2 - 2a\,x + (a^2 - db^2). \end{aligned}$$

Moreover

$$\mathrm{Tr}(\beta) = 2a, \qquad N_K(\beta) = a^2 - db^2.$$

We note in the above example that the for elements of quadratic fields, the K-norms, K-traces are rational, and that the field polynomials have rational coefficients. This isn't a coincidence.

Lemma 15.1. *Suppose $K = \mathbb{Q}(\alpha)$ is a number field and $\beta \in K$. Then*

(i) *$F_\beta(x) \in \mathbb{Q}[x]$;*
(ii) *$\mathrm{Tr}(\beta) \in \mathbb{Q}$ and $N_K(\beta) \in \mathbb{Q}$.*

Proof. Suppose $K = \mathbb{Q}(\alpha)$ is a number field of degree n with embeddings $\sigma_1, \ldots, \sigma_n$ corresponding to the conjugates $\alpha_1, \ldots, \alpha_n$ of α.

It is clear from the definitions that

$$F_\beta(x) = x^n - \mathrm{Tr}(\beta)\,x^{n-1} + \cdots + (-1)^n N_K(\beta).$$

Hence (ii) follows immediately from (i).

Let us prove (i). By Theorem 14 we can write $\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ with $a_i \in \mathbb{Q}$. Let $h(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathbb{Q}[x]$. Then $\beta = h(\alpha)$ and

$$\sigma_i(\beta) = h\left(\sigma_i(\alpha)\right) = h(\alpha_i).$$

By definition

$$F_\beta(x) = \prod_{i=1}^{n} (x - \sigma_i(\beta))$$

and hence

$$F_\beta(x) = \prod_{i=1}^{n} \left(x - h(\alpha_i)\right).$$

The polynomial on the right-hand side is unchanged by permutations of $\alpha_1, \ldots, \alpha_n$. Thus the coefficients of $F_\beta(x)$ are symmetric polynomials in $\alpha_1, \ldots, \alpha_n$ with coefficients in $\mathbb{Q}$. This shows indeed that the coefficients of $F_\beta(x)$ are in $\mathbb{Q}$. □

Theorem 17. *Suppose K is a number field of degree n. Suppose $\beta \in K$ has degree m. Then*

(i) *$m \mid n$;*
(ii) *Writing $l = n/m$, we have*

$$F_\beta(x) = f_\beta(x)^l;$$

(iii) *The K-conjugates of β are the conjugates of β repeated l times.*

Here as usual, F_β is the field polynomial of β and f_β is the minimal polynomial of β.

Before proving the theorem we make an important remark. When we defined the field polynomial $F_\beta(x)$, the definition depended not only on β and K but on a choice of a generator α for K. The above theorem shows that $F_\beta(x)$ depends only on β and the field K.

Proof of Theorem 17. As $f(\beta) = 0$ we see that

$$f(\sigma_i(\beta)) = \sigma_i(f(\beta)) = 0.$$

Thus $\sigma_i(\beta)$ is a root of f and so by definition a conjugate of β. Our first observation is: every K-conjugate of β (equivalently every root of F_β) is a conjugate of β.

Recall that the minimal polynomial f_β is irreducible. Thus we can write

$$F_\beta(x) = f_\beta(x)^l g(x) \tag{8}$$

for some non-negative integer l and some $g \in \mathbb{Q}[x]$ such that $f_\beta \nmid g$. We note that F_β and f_β are both monic, hence g is monic. We would like to show that $g = 1$. To do this it is enough to show that g has no roots. We argue by contradiction. Suppose γ is a root of g. From (8) we see that γ is a root of F_β. By our observation above, γ is a root of f_β. Thus γ is a common root of f_β and g. As f_β is irreducible and $f_\beta \nmid g$ we see that f_β and g are coprime. Hence there are polynomials $u(x), v(x) \in \mathbb{Q}[x]$ such that

$$u(x)f_\beta(x) + v(x)g(x) = 1.$$

Substituting γ for x we get $0 = 1$ which is a contradition. Hence $g = 1$ and this shows that $F_\beta(x) = f_\beta(x)^l$.

Now F_β has degree n (the same degree as K). However f_β has degree m (the same degree as β). Comparing degrees on both sides of $F_\beta(X) = f_\beta(x)^l$ we obtain $n = lm$. Thus $m \mid n$. This proves (i) and (ii) simultaneously.

(iii) follows immediately from the equality $F_\beta(x) = f_\beta(x)^l$. □

16. Ring of Integers

We recall that an algebraic integer β is a complex number satisfying $f(\beta) = 0$ for some monic polynomial with coefficients in $\mathbb{Z}$. We showed that an algebraic number β is an algebraic integer if and only if its minimal polynomial $f_\beta \in \mathbb{Z}[x]$. We denoted the set of algebraic integers by $\mathcal{O}$ and showed that it is a subring of $\mathbb{C}$.

Definition. *Let K be a number field. We define the ring of integers $\mathcal{O}_K$ of K to the set $\mathcal{O}_K = K \cap \mathcal{O}$.*

We note that $\mathcal{O}_K$ is the intersection of two subrings of $\mathbb{C}$ and hence must be a subring. Note also that $\mathbb{Z} \subseteq \mathcal{O}_K$.

Definition. *Let K be a number field of degree n. An integral basis for $\mathcal{O}_K$ is a set $\omega_1, \ldots, \omega_n$ of elements in $\mathcal{O}_K$ such that every $\beta \in \mathcal{O}_K$ can be written uniquely as*

$$\beta = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$$

with $a_1, \ldots, a_n \in \mathbb{Z}$.

Theorem 18. *Suppose K is a number field of degree n. Then $\mathcal{O}_K$ has an integral basis $\omega_1, \ldots, \omega_n$.*

We omit the proof of this theorem. This is essentially a theorem about torsion-free abelian groups.

Example 16.1. In Theorem 4 we showed that $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$. Thus the ring of integers of the number field $\mathbb{Q}$ is $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. An integral basis for this is $\{1\}$.

The following lemma is helpful in deciding if an algebraic number is an algebraic integer.

Lemma 16.1. *Suppose K is a number field and $\beta \in K$. Then $\beta \in \mathcal{O}_K$ if and only if $F_\beta \in \mathbb{Z}[x]$.*

Proof. We know from Theorem 17 that

$$F_\beta(x) = f_\beta(x)^l$$

for some positive integer l. If $\beta \in \mathcal{O}_K$, that is β is an algebraic integer, then $f_\beta \in \mathbb{Z}[x]$ and hence $F_\beta \in \mathbb{Z}[x]$.

Conversely, suppose that $F_\beta \in \mathbb{Z}[x]$. It follows from Theorem 7 that $f_\beta \in \mathbb{Z}[x]$. Thus β is an algebraic integers; i.e. $\beta \in \mathcal{O}_K$. □

Example 16.2. Let $K = \mathbb{Q}(i)$. We would like to compute $\mathcal{O}_K$ and an integral basis for it. We know that $\mathbb{Z} \subseteq \mathcal{O}_K$. Moreover i is the root of the monic $x^2 + 1 \in \mathbb{Z}[x]$ and so $i \in \mathcal{O}_K$.

Thus we see that $\mathbb{Z}[i] \subseteq \mathcal{O}_K$. Here

$$\mathbb{Z}[i] = \{a + bi \ : \quad a,\ b \in \mathbb{Z}\}.$$

We would like to determine whether or not $\mathcal{O}_K = \mathbb{Z}[i]$.

Suppose $\beta \in K$. Since 1, i is a $\mathbb{Q}$-basis for K we may write $\beta = u + vi$ for some u, $v \in \mathbb{Q}$. Write

$$u = u' + u'', \qquad v = v' + v''$$

where u', $v' \in \mathbb{Z}$ and

$$0 \leq u'' < 1, \qquad 0 \leq v'' < 1.$$

Let

$$\beta' = u' + v'i, \qquad \beta'' = u'' + v''i.$$

Now $\beta' \in \mathbb{Z}[i] \subseteq \mathcal{O}_K$. Hence

$$\begin{aligned}
\beta \in \mathcal{O}_K &\iff \beta - \beta' \in \mathcal{O}_K \\
&\iff \beta'' \in \mathcal{O}_K \\
&\iff F_{\beta''} \in \mathbb{Z}[x] \\
&\iff x^2 - 2u''x + u''^2 + v''^2 \in \mathbb{Z}[x] \\
&\iff 2u'' \in \mathbb{Z} \quad \text{and} \quad u''^2 + v''^2 \in \mathbb{Z}.
\end{aligned}$$

However $0 \leq u'' < 1$, and so $2u'' \in \mathbb{Z}$ gives us two possibilities $u'' = 0$ or $1/2$. If $u'' = 0$ then $v''^2 \in \mathbb{Z}$ and $0 \leq v'' < 1$ so $v'' = 0$. Thus we see that $\beta = \beta' \in \mathbb{Z}[i]$.

If however $u'' = 1/2$ then $1/4 + v''^2 \in \mathbb{Z}$. But $0 \leq v'' < 1$ so

$$\frac{1}{4} \leq \frac{1}{4} + v''^2 < \frac{5}{4}.$$

Hence $1/4 + v''^2 = 1$ and so $v''^2 = 3/4$ giving us a contradiction.

Thus $\mathcal{O}_K = \mathbb{Z}[i]$. The set 1, i is an integral basis for $\mathcal{O}_K$.

Example 16.3. Let $K = \mathbb{Q}(\sqrt{5})$. We follow the same steps as in the previous example to determine $\mathcal{O}_K$. Again $\mathbb{Z}[\sqrt{5}] \subseteq \mathcal{O}_K$, where

$$\mathbb{Z}[\sqrt{5}] = \left\{ a + b\sqrt{5} \ : \quad a,\ b \in \mathbb{Z} \right\}.$$

Suppose $\beta \in K$. Since 1, $\sqrt{5}$ is a $\mathbb{Q}$-basis for K we may write $\beta = u + v\sqrt{5}$ for some u, $v \in \mathbb{Q}$. Write

$$u = u' + u'', \qquad v = v' + v''$$

where u', $v' \in \mathbb{Z}$ and

$$0 \leq u'' < 1, \qquad 0 \leq v'' < 1.$$

Let

$$\beta' = u' + v'\sqrt{5}, \qquad \beta'' = u'' + v''\sqrt{5}.$$

Now $\beta' \in \mathbb{Z}[\sqrt{5}] \subseteq \mathcal{O}_K$. Hence

$$\begin{aligned} \beta \in \mathcal{O}_K &\iff \beta - \beta' \in \mathcal{O}_K \\ &\iff \beta'' \in \mathcal{O}_K \\ &\iff F_{\beta''} \in \mathbb{Z}[x] \\ &\iff x^2 - 2u''x + u''^2 - 5v''^2 \in \mathbb{Z}[x] \\ &\iff 2u'' \in \mathbb{Z} \quad \text{and} \quad u''^2 - 5v''^2 \in \mathbb{Z}. \end{aligned}$$

However $0 \leq u'' < 1$, and so $2u'' \in \mathbb{Z}$ gives us two possibilities $u'' = 0$ or $1/2$. If $u'' = 0$ then $v''^2 \in \mathbb{Z}$ and $0 \leq v'' < 1$ so $v'' = 0$. Thus we see that $\beta = \beta' \in \mathbb{Z}[\sqrt{5}]$.

If however $u'' = 1/2$ then $1/4 - 5v''^2 \in \mathbb{Z}$. But $0 \leq v'' < 1$ so

$$\frac{-19}{4} < \frac{1}{4} - 5v''^2 \leq 1/4.$$

Hence $1/4 - 5v''^2 = -4, -3, -2, -1, 0$. Examining all the possibilities we find that $v'' = 1/2$. Thus

$$\beta'' = 0, \qquad \text{or} \qquad \beta'' = \frac{1+\sqrt{5}}{2}$$

and both of these are in $\mathcal{O}_K$. It is now easy to see that

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] = \left\{ a + b\left(\frac{1+\sqrt{5}}{2}\right) \ : \quad a,\ b \in \mathbb{Z} \right\}.$$

It follows that the set 1, $(1+\sqrt{5})/2$ is an integral basis for $\mathcal{O}_K$.

We can generalize the above two examples to quadratic number fields.

Theorem 19. *Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer, and $d \neq 0, 1$*

(1) *If $d \not\equiv 1 \pmod 4$ then*

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{d}] = \left\{ a + b\sqrt{d} \ : \quad a,\ b \in \mathbb{Z} \right\}.$$

In particular, 1, $\sqrt{d}$ is an integral basis for $\mathcal{O}_K$.

(2) *If $d \equiv 1 \pmod 4$ then*

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{ a + b\left(\frac{1+\sqrt{d}}{2}\right) \ : \quad a,\ b \in \mathbb{Z} \right\}.$$

In particular 1, $(1+\sqrt{d})/2$ is an integral basis for $\mathcal{O}_K$.

We leave the proof of this theorem as an exercise.

17. Determinants and Discriminants

Let K be a number field of degree n with embeddings $\sigma_1, \ldots, \sigma_n$. Let $\omega_1, \ldots, \omega_n$ be a basis for K over $\mathbb{Q}$. Consider the matrix

$$\begin{pmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \ldots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \ldots & \sigma_2(\omega_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \ldots & \sigma_n(\omega_n) \end{pmatrix}$$

which we denote by $(\sigma_i(\omega_j))$ for short. We define the determinant of the basis $\omega_1, \ldots, \omega_n$ to be the determinant of this matrix and denote by $D(\omega_1, \ldots, \omega_n)$. Thus

$$D(\omega_1, \ldots, \omega_n) = \det(\sigma_i(\omega_j)).$$

We define the discriminant of the basis $\omega_1, \ldots, \omega_n$ to be the square of the determinant and denote by $\Delta(\omega_1, \ldots, \omega_n)$. Hence

$$\Delta(\omega_1, \ldots, \omega_n) = D(\omega_1, \ldots, \omega_n)^2 = \det(\sigma_i(\omega_j))^2.$$

Suppose now that $\beta_1, \ldots, \beta_n$ is another basis for K over $\mathbb{Q}$. Then

$$\beta_i = \sum_{j=1}^{n} c_{ij}\omega_j$$

for some $c_{ij} \in \mathbb{Q}$ satisfying

$$\det(c_{ij}) \neq 0.$$

It is an easy linear algebra exercise to show that

$$D(\beta_1, \ldots, \beta_n) = \det(c_{ij}) D(\omega_1, \ldots, \omega_n),$$

and hence

$$\Delta(\beta_1, \ldots, \beta_n) = \det(c_{ij})^2 \Delta(\omega_1, \ldots, \omega_n).$$

Theorem 20. *Suppose $K = \mathbb{Q}(\alpha)$ is a number field of degree n. Then*

(i) *The discriminant of the basis $1, \alpha, \ldots, \alpha^{n-1}$ is given by*

$$\Delta(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

where $\alpha_1, \ldots, \alpha_n$ are the conjugates of α.

(ii) *If $\beta_1, \ldots, \beta_n$ is any basis for K over $\mathbb{Q}$ then $\Delta(\beta_1, \ldots, \beta_n) \neq 0$ and $\Delta(\beta_1, \ldots, \beta_n) \in \mathbb{Q}$.*

(iii) *If $\beta_1, \ldots, \beta_n$ is an integral basis then $\Delta(\beta_1, \ldots, \beta_n) \neq 0$ and $\Delta(\beta_1, \ldots, \beta_n) \in \mathbb{Z}$.*

(iv) *If $\beta_1, \ldots, \beta_n$ and $\gamma_1, \ldots, \gamma_n$ are both integral bases for $\mathcal{O}_K$ then*

$$\Delta(\beta_1, \ldots, \beta_n) = \Delta(\gamma_1, \ldots, \gamma_n).$$

Proof. We know that $\sigma_i(\alpha) = \alpha_i$. Hence the determinant of the basis $1, \alpha, \ldots, \alpha^{n-1}$ is

$$D(1, \alpha, \ldots, \alpha^{n-1}) = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots & \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{vmatrix}. \tag{9}$$

You will instantaneously recognize this as a Vandermonde determinant, and recall that

$$D(1,\alpha,\dots,\alpha^{n-1}) = \prod_{1\le i<j\le n}(\alpha_i-\alpha_j).$$

This proves (i).

Before proving (ii) in complete generality, we prove it first for the basis $1,\alpha,\dots,\alpha^{n-1}$. We recall that the conjugates $\alpha_1,\dots,\alpha_n$ are distinct. This proves that $\Delta(1,\alpha,\dots,\alpha^{n-1})\neq 0$. Now permuting $\alpha_1,\dots,\alpha_n$ permutes the rows of the determinant in (9) and so affects only its sign. But $\Delta(1,\alpha,\dots,\alpha^{n-1})$ is the square of $D(1,\alpha,\dots,\alpha^{n-1})$ and so it is a polynomial in $\alpha_1,\dots,\alpha_n$ that is unaffected by permutations of $\alpha_1,\dots,\alpha_n$. We see that $\Delta(1,\alpha,\dots,\alpha^{n-1})\in\mathbb{Q}$. This proves (ii) for the basis $1,\alpha,\dots,\alpha^{n-1}$.

Now if $\beta_1,\dots,\beta_n$ is some other basis for K over $\mathbb{Q}$ then

$$\beta_i = \sum_{j=1}^{n} c_{ij}\alpha^{j-1}$$

for some $c_{ij}\in\mathbb{Q}$ satisfying

$$\det(c_{ij})\neq 0,$$

and (ii) follows immediately from the relationship

$$\Delta(\beta_1,\dots,\beta_n) = \det(c_{ij})^2\Delta(1,\alpha,\dots,\alpha^{n-1}).$$

Finally we turn to (iii). Suppose $\beta_1,\dots,\beta_n$ is an integral basis. From (ii) the discriminant of this basis is non-zero. We know that $\sigma_i(\beta_j)$ is a conjugate of β_j. As $\beta_j\in\mathcal{O}$, so $\sigma_i(\beta_j)$. Hence from the definition of Δ and the fact that $\mathcal{O}$ is a ring we see that $\Delta(\beta_1,\dots,\beta_n)\in\mathcal{O}$. But (ii) tells us that $\Delta(\beta_1,\dots,\beta_n)\in\mathbb{Q}$. From Theorem 4 we know that $\mathcal{O}\cap\mathbb{Q}=\mathbb{Z}$. Thus $\Delta(\beta_1,\dots,\beta_n)\in\mathbb{Z}$ as required.

We sketch a proof of (iv). Suppose that $\beta_1,\dots,\beta_n$ and $\gamma_1,\dots,\gamma_n$ are both integral basis for $\mathcal{O}_K$. It follows from the theory of abelian groups that $\beta_i = \sum_{j=1}^{n} c_{ij}\gamma_j$ where $c_{ij}\in\mathbb{Z}$ and $\det(c_{ij})=\pm 1$. So

$$\Delta(\beta_1,\dots,\beta_n) = \det(c_{ij})^2\Delta(\gamma_1,\dots,\gamma_n) = \Delta(\gamma_1,\dots,\gamma_n).$$

□

Definition. *Let K a number field. We define the discriminant of K, denoted by Δ_K, to be the discriminant of any integral basis $\beta_1,\dots,\beta_n$ for $\mathcal{O}_K$.*

We note, by Theorem 20 that Δ_K is independent of the choice of basis and moreover it is a non-zero rational integer.

Corollary 17.1. *Let $K=\mathbb{Q}(\sqrt{d})$ where d is a square-free integer, and $d\neq 0,1$*

$$\Delta_K = \begin{cases} 4d & \text{if } d\not\equiv 1 \pmod 4 \\ d & \text{if } d\equiv 1 \pmod 4. \end{cases}$$

Proof. In Theorem 19 we wrote down integral bases for $\mathcal{O}_K$. We merely have to write down their discriminants. We will do the case $d\equiv 1 \pmod 4$ and leave the other case as an exercise for the reader. Here we have 1, $(1+\sqrt{d})/2$ as an integral basis for $\mathcal{O}_K$. Now

$$D\left(1,(1+\sqrt{d})/2\right) = \begin{vmatrix} 1 & (1+\sqrt{d})/2 \\ 1 & (1-\sqrt{d})/2 \end{vmatrix} = -\sqrt{d}.$$

Hence

$$\Delta_K = \Delta\left(1, (1+\sqrt{d})/2\right) = D\left(1, (1+\sqrt{d})/2\right)^2 = d,$$

as required. □

Exercise 17.1. Let $K = \mathbb{Q}(\sqrt[3]{2})$. Compute Δ_K given that 1, $\sqrt[3]{2}$, $(\sqrt[3]{2})^2$ is an integral basis.

18. Ideals

We know that unique factorization fails for rings of integers of number fields. For example, in $\mathbb{Z}[\sqrt{-5}]$ we can factorize 6 as a product of irreducibles in two different ways:

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

It turns out that we can recover unique factorization for rings of integers of number fields if we look at ideals instead of elements. What this means is that we will show that every ideal can be written as a product of powers of prime ideals in a unique way.

We mostly use calligraphic letters for ideals of number fields: $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{P}$, $\mathcal{Q}$. Many books use gothic letters $\mathfrak{a}$, $\mathfrak{b}$, etc.

Let K be a number field and $\mathcal{O}_K$ be its ring of integers. A non-empty subset $\mathcal{A}$ of $\mathcal{O}_K$ is an *ideal* if it satisfies the following conditions:

- $\mathcal{A} \neq \emptyset$;
- $\alpha - \beta \in \mathcal{A}$ for every $\alpha, \beta \in \mathcal{A}$ (this really says that $\mathcal{A}$ is an additive subgroup of $\mathcal{O}_K$);
- if $\alpha \in \mathcal{A}$ and $\beta \in \mathcal{O}_K$ then $\beta\alpha \in \mathcal{A}$.

The *zero ideal* is just $\{0\}$. Of course $\mathcal{O}_K$ is an ideal of $\mathcal{O}_K$; ideals that are properly contained in $\mathcal{O}_K$ are called *proper* ideals.

If $0 \neq \alpha \in \mathcal{O}_K$ we define the *principal ideal* generated by α be

$$\alpha\mathcal{O}_K = \{\alpha r \ : \ r \in \mathcal{O}_K\}.$$

Another common notation for $\alpha\mathcal{O}_K$ is (α). Of course $(1) = \mathcal{O}_K$. When we think of $\mathcal{O}_K$ as an ideal it is usual to write it as (1).

In more generality, if $\alpha_1, \alpha_2, \ldots, \alpha_n$ are non-zero elements $\mathcal{O}_K$ we define the ideal generated by $\alpha_1, \ldots, \alpha_n$ to be

$$(\alpha_1, \ldots, \alpha_n) = \left\{ \sum_{i=1}^{n} \beta_i \alpha_i \ : \quad \beta_1, \ldots, \beta_n \in \mathcal{O}_K \right\}.$$

If $\mathcal{A}$, $\mathcal{B}$ are ideals the so is the set

$$(\mathcal{A}, \mathcal{B}) = \{\alpha + \beta \ : \ \alpha \in \mathcal{A}, \ \beta \in \mathcal{B}\}.$$

We sometimes write $\mathcal{A}+\mathcal{B}$ for $(\mathcal{A}, \mathcal{B})$. We say that $\mathcal{A}$, $\mathcal{B}$ are *coprime* if $\mathcal{A}+\mathcal{B} = (1)$.

We define the *ideal product*

$$\mathcal{A}\mathcal{B} = \left\{ \sum_{i=1}^{r} \alpha_i \beta_i \ : \ \alpha_i \in \mathcal{A}, \ \beta_i \in \mathcal{B} \right\}.$$

It is an easy exercise to show that $\mathcal{A}\mathcal{B}$ is again an ideal.

18.1. **Quotient Rings.** Let $\mathcal{A}$ be an ideal of the ring $\mathcal{O}_K$. A coset of $\mathcal{A}$ is of the form

$$x + \mathcal{A} = \{x + \alpha \ : \ \alpha \in \mathcal{A}\}.$$

Recall that two cosets are equal $x + \mathcal{A} = y + \mathcal{A}$ if and only if $x - y = \mathcal{A}$. We define the *quotient*

$$\mathcal{O}_K/\mathcal{A} = \{x + \mathcal{A} \ : \ x \in \mathcal{A}\}.$$

A priori $\mathcal{O}_K/\mathcal{A}$ is just the set of cosets of $\mathcal{A}$, but we can make it into a ring by defining addition and multiplication as follows:

$$(x + \mathcal{A}) + (y + \mathcal{A}) = (x + y) + \mathcal{A}, \qquad (x + \mathcal{A})(y + \mathcal{A}) = xy + \mathcal{A}.$$

It is an easy exercise to show that these operations are well-defined and that they do give a ring structure on $\mathcal{O}_K/\mathcal{A}$.

We would like to prove that if $\mathcal{A}$ is a non-zero ideal then $\mathcal{O}_K/\mathcal{A}$ is finite. Before we can do this we need the following lemma.

Lemma 18.1. *Suppose that $\mathcal{A}$ is a non-zero ideal of $\mathcal{O}_K$. Then $\mathcal{A} \cap \mathbb{Z} \neq \{0\}$.*

Proof. We want to show that $\mathcal{A}$ contains some non-zero element of $\mathbb{Z}$. As $\mathcal{A}$ is a non-zero ideal, we can choose some $\alpha \in \mathcal{A} \subseteq \mathcal{O}_K$ such that $\alpha \neq 0$. Since α is an algebraic integer, its minimal polynomial $f_\alpha(x)$ has integer coefficients; say

$$f_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0, \qquad a_i \in \mathbb{Z}.$$

Recall that f_α is irreducible. If $a_0 = 0$ then $x \mid f_\alpha(x)$ and since $f_\alpha(x)$ is irreducible we see that $f_\alpha(x) = x$. But this implies that $\alpha = 0$ contradicting our choice of α. Hence $a_0 \neq 0$. Now $f_\alpha(\alpha) = 0$, so

$$a_0 = -\alpha^n - a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha \in \mathcal{A},$$

showing that $a_0 \in \mathcal{A} \cap \mathbb{Z}$. □

Theorem 21. *Let $\mathcal{A}$ be a non-zero ideal of $\mathcal{O}_K$. Then the quotient ring $\mathcal{O}_K/\mathcal{A}$ is finite.*

Proof. We know that $\mathcal{O}_K$ has some $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_n$. From Lemma 18.1 there is some non-zero $m \in \mathcal{A} \cap \mathbb{Z}$. We would like to show that the quotient ring $\mathcal{O}_K/\mathcal{A}$ is finite. We do this by constructing a map

$$\phi \ : \ (\mathbb{Z}/m\mathbb{Z})^n \longrightarrow \mathcal{O}_K/\mathcal{A}.$$

Here $\mathbb{Z}/m\mathbb{Z}$ are the integers modulo m (which you denoted by $\mathbb{Z}_m$ in some other courses). We also show that our map ϕ is surjective. This will be enough to complete the proof: since the domain is finite, the co-domain of this surjective map must be finite.

Define

$$\phi(\overline{a_1}, \ldots, \overline{a_n}) = (a_1\omega_1 + \cdots + a_n\omega_n) + \mathcal{A}.$$

There is an issue here, which is to show that map is well-defined. This means that if $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are integers satisfying $\overline{a_1} = \overline{b_1}, \ldots, \overline{a_n} = \overline{b_n}$ then $(a_1\omega_1 + \cdots + a_n\omega_n) + \mathcal{A} = (b_1\omega_1 + \cdots + b_n\omega_n) + \mathcal{A}$. Let's do that. The condition $\overline{a_1} = \overline{b_1}, \ldots, \overline{a_n} = \overline{b_n}$ means that

$$a_1 - b_1 = mc_1, \quad \ldots, \quad a_n - b_n = mc_n, \qquad \text{for some } c_1, \ldots, c_n \in \mathbb{Z}.$$

But $m \in \mathcal{A}$. Hence $a_i - b_i \in \mathcal{A}$ for $i = 1, \ldots, n$ and so is $(a_i - b_i)\omega_i$. Thus

$$(a_1\omega_1 + \cdots + a_n\omega_n) - (b_1\omega_1 + \cdots + b_n\omega_n) = (a_1 - b_1)\omega_1 + \cdots + (a_n - b_n)\omega_n \in \mathcal{A},$$

proving that $(a_1\omega_1 + \cdots + a_n\omega_n) + \mathcal{A} = (b_1\omega_1 + \cdots + b_n\omega_n) + \mathcal{A}$. This shows that ϕ is well-defined.

Since any $x \in \mathcal{O}_K$ can be written as $x = a_1\omega_1 + \cdots + a_n\omega_n$ for some $a_i \in \mathbb{Z}$, we see that $x + \mathcal{A} = \phi(\overline{a_1}, \ldots, \overline{a_n})$. Hence ϕ is surjective. □

Definition. *Suppose that $\mathcal{A}$ is a non-zero ideal of $\mathcal{O}_K$. We define the* **norm** *of the ideal $\mathcal{A}$, denoted by $N(\mathcal{A})$ to be the number of elements of the quotient ring $\mathcal{O}_K/\mathcal{A}$.*

Theorem 22. *Let K be a number field of degree n and $\mathcal{A}$ a non-zero ideal of $\mathcal{O}_K$. Then $\mathcal{A}$ has a $\mathbb{Z}$-basis consisting of n elements. Moreover, if $\delta_1, \ldots, \delta_n$ is a $\mathbb{Z}$-basis for $\mathcal{A}$ and $\omega_1, \ldots, \omega_n$ is an integral basis for $\mathcal{O}_K$ then*

$$N(\mathcal{A}) = \left| \frac{D(\delta_1, \ldots, \delta_n)}{D(\omega_1, \ldots, \omega_n)} \right|.$$

By a $\mathbb{Z}$-basis consisting of n elements we mean some $\delta_1, \ldots, \delta_n \in \mathcal{A}$ such that any element of $\alpha \in \mathcal{A}$ can be written uniquely as a linear combination

$$\alpha = a_1\delta_1 + a_2\delta_2 + \cdots + a_n\delta_n.$$

The proof of the theorem is essentially abelian group theory and we omit it.

It is natural to ask what is the relationship between the norms of ideals and the norms of elements of the field. Recall that if $\beta \in K$ we defined the K-norm of β by

$$N_K(\beta) = \prod_{i=1}^{n} \sigma_i(\beta)$$

where σ_i are the embeddings of K.

Proposition 18.2. *If $\beta \in \mathcal{O}_K$ is non-zero and $\mathcal{B} = (\beta)$ is the principal ideal generated by β then*

$$N(\mathcal{B}) = |N_K(\beta)|.$$

Proof. Suppose that $\omega_1, \ldots, \omega_n$ is an integral basis for $\mathcal{O}_K$. It is clear that $\beta\omega_1, \ldots, \beta\omega_n$ is a $\mathbb{Z}$-basis for $\mathcal{B} = (\beta) = \beta\mathcal{O}_K$. Hence by Theorem 22 we have

$$N(\mathcal{B}) = \left| \frac{D(\beta\omega_1, \ldots, \beta\omega_n)}{D(\omega_1, \ldots, \omega_n)} \right|.$$

But

$$\begin{aligned}
D(\beta\omega_1, \ldots, \beta\omega_n) &= \begin{vmatrix} \sigma_1(\beta\omega_1) & \sigma_1(\beta\omega_2) & \ldots & \sigma_1(\beta\omega_n) \\ \sigma_2(\beta\omega_1) & \sigma_2(\beta\omega_2) & \ldots & \sigma_2(\beta\omega_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\beta\omega_1) & \sigma_n(\beta\omega_2) & \ldots & \sigma_n(\beta\omega_n) \end{vmatrix} \\
&= \begin{vmatrix} \sigma_1(\beta)\sigma_1(\omega_1) & \sigma_1(\beta)\sigma_1(\omega_2) & \ldots & \sigma_1(\beta)\sigma_1(\omega_n) \\ \sigma_2(\beta)\sigma_2(\omega_1) & \sigma_2(\beta)\sigma_2(\omega_2) & \ldots & \sigma_2(\beta)\sigma_2(\omega_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\beta)\sigma_n(\omega_1) & \sigma_n(\beta)\sigma_n(\omega_2) & \ldots & \sigma_n(\beta)\sigma_n(\omega_n) \end{vmatrix} \\
&= \sigma_1(\beta)\cdots\sigma_n(\beta) \begin{vmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \ldots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \ldots & \sigma_2(\omega_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \ldots & \sigma_n(\omega_n) \end{vmatrix} \\
&= N_K(\beta) D(\omega_1, \ldots, \omega_n)
\end{aligned}$$

proving that $N(\mathcal{B}) = |N_K(\beta)|$. □

Eventually we will show that norms are multiplicative. Meaning $N(\mathcal{AB}) = N(\mathcal{A})N(\mathcal{B})$. For now we have be content with a special case.

Theorem 23. *Suppose that $\mathcal{A}$, $\mathcal{B}$ are* **coprime** *non-zero ideals. Then*

(i) $\mathcal{A} \cap \mathcal{B} = \mathcal{AB}$;
(ii) *(Chinese Remainder Theorem) we have an isomorphism*

$$\mathcal{O}_K/\mathcal{AB} \cong \mathcal{O}_K/\mathcal{A} \times \mathcal{O}_K/\mathcal{B};$$

(iii) $N(\mathcal{AB}) = N(\mathcal{A})N(\mathcal{B})$.

Proof. We are supposing that $\mathcal{A}$, $\mathcal{B}$ are coprime. This means that $\mathcal{A} + \mathcal{B} = (1)$ or equivalently $a + b = 1$ for some $a \in \mathcal{A}$ and $b \in \mathcal{B}$. We know that $\mathcal{AB} \subseteq \mathcal{A} \cap \mathcal{B}$. To prove (i) we must show that $\mathcal{A} \cap \mathcal{B} \subseteq \mathcal{AB}$. Equivalently, we must show that any $c \in \mathcal{A} \cap \mathcal{B}$ satisfies $c \in \mathcal{AB}$. Thus suppose that $c \in \mathcal{A} \cap \mathcal{B}$. Remember that there are elements $a \in \mathcal{A}$ and $b \in \mathcal{B}$ such that $a + b = 1$. Thus $c = ac + bc$. Now $a \in \mathcal{A}$ and $c \in \mathcal{A} \cap \mathcal{B} \subseteq \mathcal{B}$, so $ac \in \mathcal{AB}$. Similarly $bc \in \mathcal{AB}$. Hence $c = ac + bc \in \mathcal{AB}$. This proves (i).

To prove (ii) consider the map

$$\phi : \mathcal{O}_K \longrightarrow \mathcal{O}_K/\mathcal{A} \times \mathcal{O}_K/\mathcal{B}, \qquad \phi(c) = (c + \mathcal{A}, c + \mathcal{B}).$$

It is easy to show that ϕ is a homomorphism of rings. Thus by the First Isomorphism Theorem

$$\mathcal{O}_K/\mathrm{Ker}(\phi) = \mathrm{Im}(\phi).$$

Let us calculate the kernel and image. Now

$$\begin{aligned} c \in \mathrm{Ker}(\phi) &\iff \phi(c) = (0 + \mathcal{A}, 0 + \mathcal{B}) \\ &\iff (c + \mathcal{A}, c + \mathcal{B}) = (0 + \mathcal{A}, 0 + \mathcal{B}) \\ &\iff c \in \mathcal{A} \text{ and } c \in \mathcal{B} \\ &\iff c \in \mathcal{A} \cap \mathcal{B}. \end{aligned}$$

Thus $\mathrm{Ker}(\phi) = \mathcal{A} \cap \mathcal{B}$. By (i) $\mathcal{A} \cap \mathcal{B} = \mathcal{AB}$ so we have $\mathrm{Ker}(\phi) = \mathcal{AB}$. We would like to show that ϕ is surjective. Suppose that $(c_1 + \mathcal{A}, c_2 + \mathcal{B}) \in \mathcal{O}_K/\mathcal{A} \times \mathcal{O}_K/\mathcal{B}$. Let $c = c_1 b + c_2 a$ where as above $a + b = 1$ and $a \in \mathcal{A}$, $b \in \mathcal{B}$. We claim that $\phi(c) = (c_1 + \mathcal{A}, c_2 + \mathcal{B})$. Note that

$$c - c_1 = c_1(b - 1) + c_2 a = c_1(-a) + c_2 a = a(c_2 - c_1) \in \mathcal{A},$$

and similarly $c - c_2 \in \mathcal{B}$. Hence

$$\phi(c) = (c + \mathcal{A}, c + \mathcal{B}) = (c_1 + \mathcal{A}, c_2 + \mathcal{B}).$$

This shows that ϕ is surjective and so $\mathrm{Im}(\phi) = \mathcal{O}_K/\mathcal{A} \times \mathcal{O}_K/\mathcal{B}$. Putting all this together proves (ii).

Now (iii) follows immediately from (ii) and the definition of norms of ideals. □

19. Prime and Maximal Ideals

Definition. *We call a proper ideal $\mathcal{P}$* **prime**, *if for all α, $\beta \in \mathcal{O}_K$ we have*

$$\alpha\beta \in \mathcal{P} \implies \alpha \in \mathcal{P} \quad or \quad \beta \in \mathcal{P}.$$

We call a proper ideal $\mathcal{M}$ **maximal** *if there isn't any ideal $\mathcal{A}$ satisfying*

$$\mathcal{M} \subsetneq \mathcal{A} \subsetneq \mathcal{O}_K.$$

In words, a proper ideal is maximal if and only if it is not properly contained in some other proper ideal.

Theorem 24. *Every maximal ideal is prime. An ideal $\mathcal{P}$ is prime if and only if $\mathcal{O}_K/\mathcal{P}$ is an integral domain. An ideal $\mathcal{M}$ is maximal if and only if $\mathcal{O}_K/\mathcal{M}$ is a field. Every maximal ideal is prime.*

Proof. The statements about $\mathcal{O}_K/\mathcal{P}$ are reformulations of the definitions of prime and maximal ideals. For the last statement, suppose that $\mathcal{M}$ is maximal. Then $\mathcal{O}_K/\mathcal{M}$ is a field. But fields are integral domains, so $\mathcal{M}$ is prime. □

The above theorem tells us that maximal ideals are prime. The converse is not true in general, but it is true for non-zero prime ideals of **the ring of integers of a number field**.

Theorem 25. *Let K be a number field and $\mathcal{O}_K$ be its ring of integers. A non-zero ideal of $\mathcal{O}_K$ is prime if and only if it is maximal.*

Proof. By Theorem 24 we know that every maximal ideal is prime. Let us prove the converse. Suppose that $\mathcal{P}$ is a prime ideal of $\mathcal{O}_K$. Theorem 24 tells us that $\mathcal{O}_K/\mathcal{P}$ is an integral domain. However, we know by Theorem 21 that $\mathcal{O}_K/\mathcal{P}$ is finite. In other words $\mathcal{O}_K/\mathcal{P}$ is a finite integral domain. But we recall that every finite integral domain is a field (if you've forgotten how this is proved, see Part I of these notes, or do the exercise below). Hence $\mathcal{O}_K/\mathcal{P}$ is a field. We apply Theorem 24 again to deduce that $\mathcal{P}$ is maximal. □

Exercise 19.1. Let R be a finite integral domain. Prove that R is a field as follows: let $x \in R\backslash\{0\}$. Consider that list x, x^2, x^3, ... Why must there be repetition in this list? Use this to show that x must have an inverse. [This proof is in the style of elementary number theory. The other proof you saw before is in the style of combinatorics.]

Exercise 19.2. Here is an alternative way of showing the maximal ideals are prime. Suppose that $\mathcal{M}$ is maximal and suppose that $\alpha\beta \in \mathcal{M}$ but $\alpha \notin \mathcal{M}$. Let $\mathcal{M}' = (\alpha) + \mathcal{M}$. Show that $\mathcal{M}' = (1)$. Deduce that $\beta \in \mathcal{M}$. Hence $\mathcal{M}$ is prime.

Before proceeding we need one more property of prime ideals.

Lemma 19.1. *Suppose that $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{P}$ are ideals such that $\mathcal{P}$ is prime and $\mathcal{P} \supseteq \mathcal{AB}$. Then either $\mathcal{P} \supseteq \mathcal{A}$ or $\mathcal{P} \supseteq \mathcal{B}$.*

Perhaps you would like to prove this for yourself before looking at the proof.

Proof of Lemma 19.1. Suppose that $\mathcal{AB} \subseteq \mathcal{P}$ but $\mathcal{A} \not\subseteq \mathcal{P}$. Then there is some $\alpha \in \mathcal{A}$ such that $\alpha \notin \mathcal{P}$. We want to show that $\mathcal{B} \subseteq \mathcal{P}$. Consider $\beta \in \mathcal{B}$. Then $\alpha\beta \in \mathcal{AB} \subseteq \mathcal{P}$. By the definition of a prime ideal, $\alpha \in \mathcal{P}$ or $\beta \in \mathcal{P}$. But we know already that $\alpha \notin \mathcal{P}$ and so $\beta \in \mathcal{P}$. Since this is true for all $\beta \in \mathcal{P}$ we deduce that $\mathcal{B} \subseteq \mathcal{P}$ as required. □

20. Towards Unique Factorization for Ideals I

Our objective is to prove the following theorem.

Theorem 26. *(Unique Factorization Theorem for Ideals) Let K be a number field and $\mathcal{O}_K$ be its ring of integers. Then every non-zero ideal $\mathcal{A}$ can be written as a product of of finitely prime ideals*

$$\mathcal{A} = \prod_{i=1}^{n} \mathcal{P}_i.$$

Moreover this factorization is unique up to re-ordering.

We note an important convention, which is that the ideal (1) is regarded as the product of zero many prime ideals:

$$(1) = \prod_{i=1}^{0} \mathcal{P}_i.$$

The proof of the Unique Factorization Theorem for Ideals will require many steps. One of these is the Cancellation Lemma which we prove later.

Lemma 20.1. *(Cancellation Lemma) Let K be is a number field and $\mathcal{O}_K$ be its ring of integers. Suppose that $\mathcal{BA} = \mathcal{CA}$ for some non-zero ideals $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$. Then $\mathcal{B} = \mathcal{C}$.*

The proof the Cancellation Lemma is highly non-trivial. You can't just say "divide", because we are talking about ideals (which are sets) and we haven't defined what division of ideals means.

However the Cancellation Lemma is enough to imply the uniqueness part of the Unique Factorization Theorem.

Lemma 20.2. *(Uniqueness Part of the Unique Factorization Theorem) Let K be a number field and* **suppose the Cancellation Lemma holds** *for $\mathcal{O}_K$. Suppose that $\mathcal{P}_1, \ldots, \mathcal{P}_m$ and $\mathcal{Q}_1, \ldots, \mathcal{Q}_n$ are prime ideals of $\mathcal{O}_K$. If*

$$\prod_{i=1}^{m} \mathcal{P}_i = \prod_{j=1}^{n} \mathcal{Q}_j$$

then $n = m$ and the $\mathcal{P}_1, \ldots, \mathcal{P}_m$ and $\mathcal{Q}_1, \ldots, \mathcal{Q}_n$ are the same up to re-ordering.

Proof. We prove the lemma by induction on $\min(m, n)$. Suppose first that $\min(m, n) = 0$. Without loss of generality suppose that $m = 0$. If $n = 0$ then there is nothing to prove. So suppose that $n > 0$. Hence we have

$$(1) = \mathcal{Q}_1 \mathcal{Q}_2 \ldots \mathcal{Q}_n.$$

But $\mathcal{Q}_1 \mathcal{Q}_2 \ldots \mathcal{Q}_n \subseteq \mathcal{Q}_i$ for $i = 1, \ldots, n$, so $\mathcal{Q}_i = (1)$. As prime ideals are proper by definition, we have a contradiction. Hence if $\min(m, n) = 0$ then $m = n = 0$ and the lemma is true.

We now come to the inductive step. Suppose $\min(m, n) \geq 1$. Note that

$$\mathcal{P}_m \supseteq \prod_{i=1}^{m} \mathcal{P}_i = \prod_{j=1}^{n} \mathcal{Q}_j.$$

By Lemma 19.1 we see that $\mathcal{P}_m \supseteq \mathcal{Q}_j$ for some j. After re-labeling we can suppose that $\mathcal{P}_m \supseteq \mathcal{Q}_n$. Now we recall that prime ideals are maximal (in our present

context, not in general). Hence $\mathcal{P}_m = \mathcal{Q}_n$. Now we apply the Cancellation Lemma to cancel $\mathcal{P}_m = \mathcal{Q}_n$ from

$$\mathcal{P}_1\mathcal{P}_2 \dots \mathcal{P}_m = \mathcal{Q}_1\mathcal{Q}_2 \dots \mathcal{Q}_n$$

to obtain

$$\mathcal{P}_1\mathcal{P}_2 \dots \mathcal{P}_{m-1} = \mathcal{Q}_1\mathcal{Q}_2 \dots \mathcal{Q}_{n-1}.$$

Now we can apply the inductive hypothesis to complete the proof. □

21. Towards Unique Factorization for Ideals II

In the previous section we showed that if we can factorize an ideal as a product of primes then such a factorization is unique up to re-ordering (of course we assumed the Cancellation Lemma). To prove the Unique Factorization Theorem we must also prove *existence*: that any non-zero ideal can be written as a product of prime ideals. This is again a long-term goal. For now we introduce the notion of an irreducible ideal and prove the existence of prime factorization under the assumption that irreducible ideals are prime.

Definition. *We say a proper ideal is* **irreducible** *if it is* **not** *the product of two strictly larger ideals.*

Lemma 21.1. *(Irreducibles are Primes) A non-zero ideal is prime if and only if it is irreducible.*

Showing that a prime ideal is irreducible is easy. Suppose $\mathcal{P}$ is prime and suppose $\mathcal{P} = \mathcal{A}\mathcal{B}$. By Lemma 19.1 we see that $\mathcal{P} \supseteq \mathcal{A}$ or $\mathcal{P} \supseteq \mathcal{B}$. Let's say $\mathcal{P} \supseteq \mathcal{A}$. Then $\mathcal{P} \supseteq \mathcal{A} \supseteq \mathcal{A}\mathcal{B} = \mathcal{P}$. Hence $\mathcal{P} = \mathcal{A}$. Thus we see that $\mathcal{A}$ is not strictly bigger than $\mathcal{P}$. So we have shown that every prime ideal is irreducible. Showing the converse will require much effort.

Lemma 21.2. *(Existence of Factorization into Prime Ideals) Let K be a number field and $\mathcal{O}_K$ be its ring of integers.* **Assume that irreducible ideals of $\mathcal{O}_K$ are prime.** *Then every non-zero ideal can be written as a product of prime ideals.*

Proof. Since we are assuming that irreducible ideals are prime, we need only show that every non-zero ideal $\mathcal{A}$ can be written as a product of irreducible ideals. We do this by induction on the norm $N(\mathcal{A})$.

Note first that $N(\mathcal{A}) = 1$ if and only if $\mathcal{O}_K/\mathcal{A} = 0$ which is equivalent to $\mathcal{A} = \mathcal{O}_K$. But $\mathcal{O}_K = (1)$ is the product of zero many irreducible ideals.

Now suppose that $N(\mathcal{A}) > 1$ and we want to show that $\mathcal{A}$ can be written as a product of irreducible ideals. If $\mathcal{A}$ is irreducible then there is nothing to prove. Thus we may suppose that $\mathcal{A}$ is reducible, which means that $\mathcal{A} = \mathcal{B}\mathcal{C}$ where $\mathcal{B}$ and $\mathcal{C}$ are strictly larger ideals (strictly larger means $\mathcal{A} \subsetneq \mathcal{B}$ and $\mathcal{A} \subsetneq \mathcal{C}$). We will show that $N(\mathcal{B}) < N(\mathcal{A})$ and $N(\mathcal{C}) < N(\mathcal{A})$. After this we simply apply the inductive hypothesis to deduce that $\mathcal{B}$ and $\mathcal{C}$ can written as products of irreducibles and hence so can $\mathcal{A} = \mathcal{B}\mathcal{C}$.

It remains to show that $N(\mathcal{B}) < N(\mathcal{A})$ and $N(\mathcal{C}) < N(\mathcal{A})$. To do this define the map

$$\phi \ : \ \mathcal{O}_K/\mathcal{A} \to \mathcal{O}_K/\mathcal{B}, \qquad \alpha + \mathcal{A} \mapsto \alpha + \mathcal{B}$$

and show that this is well-defined and surjective using $\mathcal{B} \supset \mathcal{A}$ (exercise). Moreover show that the map is not injective using $\mathcal{B} \supsetneq \mathcal{A}$ (exercise). Hence the cardinality

(i.e. number of elements) of $\mathcal{O}_K/\mathcal{A}$ is strictly larger than that of $\mathcal{O}_K/\mathcal{B}$. Recalling the definition of norm we see that $N(\mathcal{A}) > N(\mathcal{B})$ and similarly $N(\mathcal{A}) > N(\mathcal{C})$. □

22. Unique Factorization Proof—A Summary so Far

Our objective was (and is) to prove the Unique Factorization Theorem for Ideals (Theorem 26). We made two assumptions:

- The **Cancellation Lemma**;
- **Irreducible ideals are prime**.

From these two assumptions we deduced the existence (Lemma 21.2) and uniquess (Lemma 20.2) parts of the Unique Factorization Theorem. In other words to complete the proof of the Unique Factorization Theorem 'all' we have to do is to prove our two assumptions. To do this we need to introduce ideal classes and show that there are finitely many ideal classes.

23. A Special Case of the Cancellation Lemma

The Cancellation Lemma 20.1 is one of our two ingredients needed to prove the Unique Factorization Theorem for ideals. In this section we content ourselves with proving a special case of the Cancellation Lemma. In turns out that this special case is needed in the proof of the full Cancellation Lemma.

Later on we prove the following statement for ideals of $\mathcal{O}_K$: **to contain is to divide**. What this means is the following: if $\mathcal{A}$, $\mathcal{B}$ are non-zero ideals and $\mathcal{B} \supseteq \mathcal{A}$ (i.e. $\mathcal{B}$ contains $\mathcal{A}$) then $\mathcal{BD} = \mathcal{A}$ for some non-zero ideal $\mathcal{D}$ (i.e. $\mathcal{B}$ divides $\mathcal{A}$). We cannot prove this yet, but we can prove a useful special case of this statement.

Lemma 23.1. *Let $\mathcal{C}$ be a non-zero ideal and β be a non-zero element of $\mathcal{O}_K$. If $\mathcal{C} \subseteq (\beta)$ then there is a non-zero ideal $\mathcal{D}$ such that $\mathcal{C} = (\beta)\mathcal{D}$.*

Proof. Suppose $\mathcal{C} \subseteq (\beta)$. Define

$$\mathcal{D} = \{\delta \in \mathcal{O}_K \ : \quad \delta\beta \in \mathcal{C}\}.$$

We want to show that $\mathcal{D}$ is an ideal that does the required job, namely $\mathcal{C} = (\beta)\mathcal{D}$.

First we show that $\mathcal{D}$ is an ideal. Note that $0\beta \in \mathcal{C}$ and so $0 \in \mathcal{D}$. Suppose δ_1, $\delta_2 \in \mathcal{D}$. Then $\delta_1\beta$, $\delta_2\beta \in \mathcal{C}$. Hence

$$(\delta_1 + \delta_2)\beta \in \mathcal{C},$$

showing that $\delta_1 + \delta_2 \in \mathcal{D}$.

Moreover, if $\delta \in \mathcal{D}$ and $\alpha \in \mathcal{O}_K$ then $\delta\beta \in \mathcal{C}$ and hence

$$(\alpha\delta)\beta = \alpha(\delta\beta) \in \mathcal{C}.$$

Thus $\alpha\delta \in \mathcal{D}$. This shows that $\mathcal{D}$ is an ideal.

From the definition of $\mathcal{D}$ it is clear that $(\beta)\mathcal{D} \subseteq \mathcal{C}$. Suppose $\gamma \in \mathcal{C}$. Since $\mathcal{C} \subseteq (\beta)$ we can write $\gamma = \beta\delta$ for some $\delta \in \mathcal{O}_K$. Again, from the definition of $\mathcal{D}$ we see that $\delta \in \mathcal{D}$. Hence $\gamma \in (\beta)\mathcal{D}$. This shows that $\mathcal{C} = (\beta)\mathcal{D}$. □

Exercise 23.1. This is an exercise on the theme "to contain is to divide". Recall that any ideal of $\mathbb{Z}$ is principal. Suppose that $m,\ n \in \mathbb{Z}\backslash\{0\}$. Show that $(m) \supseteq (n)$ if and only if $m \mid n$.

Now for our special case of the Cancellation Lemma.

Lemma 23.2. *Suppose that $\beta \in \mathcal{O}_K$ is non-zero and $\mathcal{A}$, $\mathcal{C}$ are non-zero ideals of $\mathcal{O}_K$. If $(\beta)\mathcal{A} = \mathcal{C}\mathcal{A}$ then $(\beta) = \mathcal{C}$.*

Proof. Let $\omega_1, \ldots, \omega_n$ be a $\mathbb{Z}$-basis for the ideal $\mathcal{A}$. Then $\beta\omega_1, \ldots, \beta\omega_n$ is a $\mathbb{Z}$-basis for $\beta\mathcal{A} = (\beta)\mathcal{A}$. Suppose that $\gamma \in \mathcal{C}$. Then $\gamma\omega_i \in \mathcal{C}\mathcal{A} = (\beta)\mathcal{A}$. Hence there are $a_{ij} \in \mathbb{Z}$ such that

$$\gamma\omega_i = \sum_{j=1}^{n} a_{ij}\beta\omega_j.$$

This system of equalties for $i = 1, \ldots, n$ can be rewritten in matrix notation as

$$\beta^{-1}\gamma\mathbf{w} = A\mathbf{w}$$

where $A = (a_{ij})$ and $\mathbf{w}$ is the column vector with entries ω_i. Hence $\beta^{-1}\gamma$ is an eigenvalue of the matrix A. In other words, $\beta^{-1}\gamma$ is a root of $\chi_A(x) = \det(xI_n - A)$. But A has entries in $\mathbb{Z}$ and so χ_A is monic with coefficients in $\mathbb{Z}$. Thus $\beta^{-1}\gamma$ is an algebraic integer, and so $\beta^{-1}\gamma \in \mathcal{O}_K$.

We deduce that $\gamma \in \beta\mathcal{O}_K = (\beta)$. This is true for all $\gamma \in \mathcal{C}$. Thus $\mathcal{C} \subseteq (\beta)$. Lemma 23.1 tells us that $\mathcal{C} = (\beta)\mathcal{D}$ for some ideal $\mathcal{D}$.

We return to our original equality: $(\beta)\mathcal{A} = \mathcal{C}\mathcal{A}$ and substitute $\mathcal{C} = (\beta)\mathcal{D}$ to obtain $(\beta)\mathcal{A} = (\beta)\mathcal{D}\mathcal{A}$ or equivalently $\beta\mathcal{A} = \beta\mathcal{D}\mathcal{A}$. Dividing by β we obtain $\mathcal{A} = \mathcal{D}\mathcal{A}$. Recall that ω_i was a $\mathbb{Z}$-basis for $\mathcal{A}$. It is easy to see that (Exercise)

$$\omega_i = \sum \delta_{ij}\omega_j,$$

where $\delta_{ij} \in \mathcal{D}$. Thus 1 is an eigenvalue of the matrix (δ_{ij}) and so is a root of the polynomial

$$\det(xI_n - (\delta_{ij})) = x^n + d_{n-1}x^{n-1} + \cdots + d_0,$$

where $d_i \in \mathcal{D}$. From this we obtain

$$1 = -d_{n-1} - d_{n-2} - \cdots - d_0 \in \mathcal{D},$$

so $\mathcal{D} = (1)$. Substituting $\mathcal{D} = (1)$ in $\mathcal{C} = (\beta)\mathcal{D}$ we obtain $\mathcal{C} = (\beta)$ as desired. □

24. Ideal Classes

Definition. *Let K be a number field and $\mathcal{O}_K$ be its ring of integers. We define the following relation on the non-zero ideals of $\mathcal{O}_K$: $\mathcal{A} \sim \mathcal{B}$ if and only if $(\beta)\mathcal{A} = (\alpha)\mathcal{B}$ for some non-zero elements α, $\beta \in \mathcal{O}_K$. It is easy to show that this is an equivalence relation and so when $\mathcal{A} \sim \mathcal{B}$ we say that $\mathcal{A}$ and $\mathcal{B}$ are in the* **same ideal class**. *We write $[\mathcal{A}]$ for the class represented by $\mathcal{A}$. The* **principal class** *is the class of (1).*

Exercise 24.1. Verify that $\sim$ really gives an equivalence relation on the non-zero ideals. Show that the principal class consists precisely of principal ideals.

Define multiplication on the set of ideal classes by $[\mathcal{A}][\mathcal{B}] = [\mathcal{A}\mathcal{B}]$. Show that this operation is well-defined. Eventually we will show that this operation turns the ideal classes into an abelian group. For now, which of the group axioms can you prove straightforwardly from the definitions? What is the identity element?

Theorem 27. *(Finiteness of Ideal Classes) Let K be a number field and $\mathcal{O}_K$ be its ring of integers. There are only finitely many classes of ideals of $\mathcal{O}_K$.*

We delay proving this theorem till later. For now we show that it implies the Cancellation Lemma and that irreducible ideals are prime. In other words, we show that this theorem implies the Unique Factorization Theorem for Ideals.

Lemma 24.1. Assume that $\mathcal{O}_K$ has only finitely many ideal classes. *Given any non-zero ideal $\mathcal{A}$, there is some exponent $h > 0$ such that $\mathcal{A}^h$ is principal.*

Proof. First consider that sequence of ideals $\mathcal{A}, \mathcal{A}^2, \mathcal{A}^3, \ldots$. Since there are only finitely many ideal classes, there must be some exponents $r > s > 0$ such that $\mathcal{A}^r \sim \mathcal{A}^s$. Hence there are non-zero integers α, β such that

$$(\alpha)\mathcal{A}^r = (\beta)\mathcal{A}^s.$$

Write $\mathcal{C}$ for the ideal $\alpha\mathcal{A}^{r-s}$. Then

$$\mathcal{C}\mathcal{A}^s = (\beta)\mathcal{A}^s.$$

By our special case of the Cancellation Lemma 23.2 we have that $\mathcal{C} = (\beta)$. Hence $(\alpha)\mathcal{A}^{r-s} = (\beta)$. Hence $\mathcal{A}^{r-s}$ is principal as required. □

We can now prove the Cancellation Lemma itself, assuming finiteness of ideal classes.

Lemma 24.2. *(Cancellation Lemma) Let K be is a number field and $\mathcal{O}_K$ be its ring of integers.* **Assume that $\mathcal{O}_K$ has only finitely many ideal classes.** *Suppose that $\mathcal{B}\mathcal{A} = \mathcal{C}\mathcal{A}$ for some non-zero ideals $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$. Then $\mathcal{B} = \mathcal{C}$.*

Proof. As we are assuming that there are only finitely many ideal classes, we know from Lemma 24.1 that $\mathcal{A}^h = (\alpha)$ for some non-zero $\alpha \in \mathcal{O}_K$ and exponent $h > 0$. Multiplying both sides of $\mathcal{B}\mathcal{A} = \mathcal{C}\mathcal{A}$ by $\mathcal{A}^{h-1}$ we obtain $\mathcal{B}(\alpha) = \mathcal{C}(\alpha)$, which we can rewrite as $\alpha\mathcal{B} = \alpha\mathcal{C}$. Dividing by α we obtain $\mathcal{B} = \mathcal{C}$. □

Lemma 24.3. *(To Contain is to Divide) Let K be is a number field and $\mathcal{O}_K$ be its ring of integers.* **Assume that $\mathcal{O}_K$ has only finitely many ideal classes.** *If $\mathcal{A} \subseteq \mathcal{B}$ are non-zero ideals, then there is a non-zero ideal $\mathcal{D}$ such that $\mathcal{A} = \mathcal{B}\mathcal{D}$.*

Proof. As we are assuming that there are only finitely many ideal classes, we know from Lemma 24.1 that $\mathcal{B}^h = (\beta)$ for some non-zero $\beta \in \mathcal{O}_K$ and exponent $h > 0$. From $\mathcal{A} \subseteq \mathcal{B}$ we obtain $\mathcal{A}\mathcal{B}^{h-1} \subseteq \mathcal{B}^h$ and so $\mathcal{A}\mathcal{B}^{h-1} \subseteq (\beta)$. By Lemma 23.1 there is some non-zero ideal $\mathcal{D}$ such that

$$\mathcal{A}\mathcal{B}^{h-1} = (\beta)\mathcal{D}.$$

Substituting back $(\beta) = \mathcal{B}^h$ we get

$$\mathcal{A}\mathcal{B}^{h-1} = \mathcal{D}\mathcal{B}^h.$$

By the Cancellation Lemma 24.2 we can cancel $\mathcal{B}^{h-1}$ to obtain $\mathcal{A} = \mathcal{D}\mathcal{B}$ as required. □

Lemma 24.4. *(Irreducibles are Primes) Let K be is a number field and $\mathcal{O}_K$ be its ring of integers.* **Assume that $\mathcal{O}_K$ has only finitely many ideal classes.** *A non-zero ideal is prime if and only if it is irreducible.*

Proof. We proved before that prime ideals are irreducible. Suppose that $\mathcal{P}$ is a non-zero irreducible ideal, we would like to show that it is prime. It is enough

to show that $\mathcal{P}$ is maximal (since maximal ideals are prime). Suppose $\mathcal{P}$ is not maximal. Then there is some ideal $\mathcal{A}$ such that

$$\mathcal{P} \subsetneq \mathcal{A} \subsetneq \mathcal{O}_K.$$

By Lemma 24.3 we see that $\mathcal{P} = \mathcal{A}\mathcal{D}$ for some non-zero ideal $\mathcal{D}$. We know that $\mathcal{P} \subsetneq \mathcal{A}$ and also $\mathcal{P} = \mathcal{A}\mathcal{D} \subseteq \mathcal{D}$.

Now $\mathcal{P} = \mathcal{A}\mathcal{D}$ is irreducible. By definition of irreducible, $\mathcal{P}$ is not properly contained in $\mathcal{A}$ or not properly contained in $\mathcal{D}$. However $\mathcal{P} \subsetneq \mathcal{A}$. Hence $\mathcal{P}$ is not properly contained in $\mathcal{D}$. Thus $\mathcal{P} = \mathcal{D}$. Cancelling from $\mathcal{P} = \mathcal{A}\mathcal{D}$ we get $\mathcal{A} = (1) = \mathcal{O}_K$ contradicting $\mathcal{A} \subsetneq \mathcal{O}_K$. □

25. Unique Factorization Proof—Summary So Far (again)

Recall the conclusion of our previous summary in Section 22: to complete the proof of the Unique Factorization Theorem for Ideals (Theorem 26) we needed to prove two results:

- The **Cancellation Lemma**;
- **Irreducible ideals are prime**.

In the previous section we proved both of these results under the assumption that there ring of integers of a number field has only finitely many ideal classes. **Thus to complete the proof of the Unique Factorization Theorem for Ideals all we have to do is to prove the finiteness of ideal classes.**

26. What are the prime ideals of K?

In this section we take a well-earned rest from the proof of the proof of the Unique Factorization Theorem to ask ourselves, "What do the prime ideals of rings of integers of number fields look-like?". **We assume the Unique Factorization Theorem, Cancellation Lemma, to Contain is to Divide, Irreducible Ideals are Prime** throughout this section. Later on we return to complete the proof of all of these once we had our rest.

Lemma 26.1. *Suppose $\mathcal{P}$ is a non-zero prime ideal of $\mathcal{O}_K$. Then $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime number p. Moreover, $\mathcal{P}$ divides $p\mathcal{O}_K$ (the principal ideal of $\mathcal{O}_K$ generated by p).*

Proof. It is easy to see that $\mathcal{P} \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$. Moreover, we proved previously that for any non-zero ideal $\mathcal{A}$ we have $\mathcal{A} \cap \mathbb{Z} \neq 0$. Hence $\mathcal{P} \cap \mathbb{Z}$ is a non-zero ideal of $\mathbb{Z}$. We recall that $\mathbb{Z}$ is a principal ideal domain. So $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$ for some non-zero integer p, which we may take to be positive. We want to show that p is prime. Suppose $p \mid ab$ where a, b are positive integers. Then $ab \in p\mathbb{Z} \subseteq \mathcal{P} \cap \mathbb{Z} \subseteq \mathcal{P}$. As $\mathcal{P}$ is prime, we see that $a \in \mathcal{P}$ or $b \in \mathcal{P}$. But a, $b \in \mathbb{Z}$. Hence, $a \in \mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$ or $b \in \mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$. In otherwords $p \mid a$ or $p \mid b$. This shows that p is prime.

Thus we have shown $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime p. Now $p \in \mathcal{P}$. Hence $p\mathcal{O}_K \subseteq \mathcal{P}$. By "to contain is to divide" we see that $\mathcal{P} \mid p\mathcal{O}_K$. □

We see from the above lemma that any non-zero prime ideal of $\mathcal{O}_K$ divides $p\mathcal{O}_K$ for some prime number p. To get the prime ideals of $\mathcal{O}_K$ all we have to do is factorize $p\mathcal{O}_K$ as a product of prime ideals. The following theorem tells us how, provided $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$.

Theorem 28. *Suppose that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where α has minimal polynomial $f_\alpha(X) \in \mathbb{Z}[X]$ of degree n. Suppose that*

$$f_\alpha(X) \equiv \prod g_i(X)^{e_i} \pmod{p} \tag{10}$$

where each g_i is a monic polynomial in $\mathbb{Z}[X]$ which is irreducible modulo p. Write $\mathcal{P}_i = (p, g_i(\alpha))$. Then each ideal $\mathcal{P}_i$ is prime and

$$p\mathcal{O}_K = \prod \mathcal{P}_i^{e_i}.$$

Example 26.1. Let us take $K = \mathbb{Q}(i)$ and see the factorizations of some small primes in $\mathcal{O}_K$ (the Gaussian integers). We know $\mathcal{O}_K = \mathbb{Z}[i]$, and i has minimal polynomial $f(X) = X^2 + 1$. Let us factorize the ideals $2\mathcal{O}_K$, $3\mathcal{O}_K$, $5\mathcal{O}_K$ in $\mathcal{O}_K$. We note

$$X^2 + 1 \equiv (X + 1)^2 \pmod{2}.$$

Hence $2\mathcal{O}_K = \mathcal{P}^2$ where $\mathcal{P} = (2, 1 + i)$ is prime. But we remember that $\mathbb{Z}[i]$ is a principal ideal domain. So we should be able to write $\mathcal{P}$ as a principal ideal. Now notice that $2 = (1 + i)(1 - i)$. Hence $2 \in (1 + i)\mathcal{O}_K$. Thus

$$(1 + i)\mathcal{O}_K \subseteq (2, 1 + i) \subseteq (1 + i)\mathcal{O}_K.$$

Hence $\mathcal{P} = (1 + i)\mathcal{O}_K$ and $2\mathcal{O}_K = \mathcal{P}^2$.

To factorize 3, we note that $X^2 + 1$ is irreducible modulo 3. Hence $3\mathcal{O}_K = (3, i^2 + 1) = (3)$ is a prime ideal.

To factorize 5, note that

$$X^2 + 1 \equiv X^2 - 4 \equiv (X + 2)(X - 2) \pmod{5}.$$

Hence $5\mathcal{O}_K = \mathcal{P}\mathcal{Q}$ where $\mathcal{P} = (5, 2+i)$ and $\mathcal{Q} = (5, 2-i)$. However $5 = (2+i)(2-i)$ so $\mathcal{P} = (2 + i)\mathcal{O}_K$ and $\mathcal{Q} = (2 - i)\mathcal{O}_K$.

Samir Siksek, Department of Mathematics, University of Warwick, Coventry, CV4 7AL, United Kingdom

E-mail address: siksek@maths.warwick.ac.uk