Math 1560: Number Theory *Lecture Notes*

N. Looper

Spring 2022

These are lecture notes for Math 1560: Number Theory taught at Brown University by Nicole Looper in the Spring of 2022.

Notes last updated April 22, 2022.

Contents

References

[IR90] K. Ireland and M.I. Rosen. *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics. Springer, 1990.

[ST15] I. Stewart and D. Tall. *Algebraic Number Theory and Fermat's Last Theorem*. CRC Press, 2015.

§0 January 27, 2022

§0.1 Course Logistics

- Mostly refer to syllabus for any information that you might need.
- Midterm is planned for March 17.
- Final exam schedule can be found on CAB.

§0.2 Introduction to Number Theory

Number theory can be split into two branches: analytic number theory and algebraic number theory.

What is number theory? Number theory is the study of integers and their analogues in algebraic number fields.

Prime numbers are a key focus of number theory, and the study of different properties of primes constitutes different fields of number theory:

i. The study of their distributional properties, which is analytic number theory.

ii. As building blocks for algebraic numbers, which is algebraic number theory.

§0.2.1 Examples of Analytic Number Theory

Here are some examples of analytic number theory and their statements:

- Prime Number Theorem
- Twin Prime Conjecture
- Goldbach's conjecture

Theorem 0.1 (Prime Number Theorem)
Let $\pi(x)$ be the number of primes between 1 and x, then

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

Conjecture 0.2 (Twin Prime Conjecture)
Twin primes are pairs of primes p, q of the form $q = p + 2$. Examples include $(3, 5), (11, 13), \ldots$. The conjecture postulates that there are infinitely many twin primes.

Conjecture 0.3 (Goldbach's conjecture)
Any positive even integer greater than 2 can be written as the sum of 2 primes.

§0.2.2 Examples of Algebraic Number Theory

Analyzing the factorization (rings of integers) of number fields is one topic of algebraic number theory.

Example 0.4
2 is prime (irreducible) in $\mathbb{Z}$.

Yet 2 is not prime in $\mathbb{Z}[i]$ (the Gaussian integers). This is because

$$2 = \underbrace{(1+i)(1-i)}_{\text{associates}}$$

we have that $(1+i) = i(1-i)$. We also note the property that the principal ideals $(2) = (1+i)^2$ are equal.

In this example, we say that 2 "ramifies" in the ring of integers.

Fermat's Last Theorem is another such example.

Recall: that a *Pythagorean triple* is a triple of the form $a, b, c \in \mathbb{Z}_+$ such that

$$a^2 + b^2 = c^2$$

Are there examples of such numbers with different exponents (say, k^{th} powers for $k \geq 3$)?

Theorem 0.5 (Fermat's Last)
There are no positive integers $a, b, c \in \mathbb{Z}_+$ satisfying

$$a^k + b^k = c^k$$

for $k \geq 3$.

The answer is no! (Proved by Andrew Wiles)

Conjecture 0.6 (*abc* Conjecture, informally)

We say *powerful numbers* are positive integers whose prime factorization contains relatively few distinct primes (appropriately weighted) with an exponent of 1.

Example

$2^{10}3^7$ is powerful, $2^{10}3^75$ is powerful, 1 is powerful.

If a, b are *very powerful* coprime numbers, then $a+b$ is predicted to be *not powerful*.

Example 0.7

Consider 2^{10} and 3^{15}. We have

$$2^{10} + 3^{15} = 14,349,931 = \underbrace{31 \cdot 462 \cdot 901}_{\text{not powerful}}$$

What about another example, like $3^{15}+5$? The *abc* conjecture also predicts that this number is not so powerful...[1]

§1 February 1, 2022

Happy Lunar New Year!

(Thanks Qinan and Andrew for allowing me to shamelessly copy their notes.)

§1.1 Divisibility and Factorization

We start with some commonly used notation:

Definition 1.1 (Divisibility)

We use $a \mid b$ to mean "a divides b" and $a \nmid b$ to mean "a does not divide b".

Now for a series of definitions:

Definition 1.2 (Primality)

A positive integer $p \geq 2$ is said to be prime if its only positive divisors are 1 and p.

[1] After lecture Jiahua: It's a prime!?

Definition 1.3 (Positive Integers)

$\mathbb{Z}_+$ will denote the positive integers.

Definition 1.4 (Order)

For a nonzero $n \in \mathbb{Z}$ and a prime p, there is a nonnegative integer a such that $p^a \mid n$ but $p^{a+1} \nmid n$. This number a is called the order of n at p, denoted by $\operatorname{ord}_p n$.

For $n = 0$, we set $\operatorname{ord}_p 0 = \infty$. We also have $\operatorname{ord}_p n = 0 \Leftrightarrow p \nmid n$.

We prove a lemma as warm-up:

Lemma 1.5 (Existence of Factorization)

Every nonzero integer can be written as a product of primes.

We make an exception for -1. *The empty product is* 1 *so* 1 *is fine.*

Proof. Suppose for the sake of contradiction otherwise, that some nonzero integer can be written as a product of primes. Let N be the smallest integer greater than 2 that cannot be written as a product of primes.

N had better not be a prime number itself (since then it would be a product of itself). Then we can write $N = a \cdot b$ where $1 < a, b < N$.

Since we took N as the least such number that cannot be written as a product of primes, a and b which are less than N can be written as a product of primes. Then N is a product of primes since a and b individually are. This is a contradiction! Thus it had better be the case that *every* nonzero integer can be written as a product of primes. □

This is the theorem we will eventually work toward proving:

Theorem 1.6 (Unique Factorization)

Every nonzero integer n yields a *unique* prime factorization

$$n = (-1)^{\varepsilon} \cdot \prod_p p^{a(p)}, a(p) \geq 0$$

where $\varepsilon = 0$ or 1, and $\varepsilon, a(p)$ are uniquely determined by n. Moreover, we note that $a(p) = \operatorname{ord}_p n$.

§1.2 Euclidean and Principal Ideal Domains

Before this proof, we first recall a conclusion from Math 1530:

Lemma 1.7 (Division Lemma)
If $a, b \in \mathbb{Z}$ and $b > 0$, then there exists $q, r \in \mathbb{Z}$ such that

$$a = bq + r$$

with $0 \leq r < b$.

Proof. Consider the set

$$S = \{a - xb \mid x \in \mathbb{Z}\}$$

We note that S contains *some* positive elements. Let $r = a - qb$ be the least nonnegative element of S.

We claim that $0 \leq r < b$. Suppose for the sake of contradiction otherwise, then $r = a - qb \geq b$ gives $a - qb - b \leq 0$ and $a - (q+1)b \leq 0$. Which is a contradiction since we took r to be a the least nonnegative element in S and we've found such smaller element $a - (q+1)b$.

Then it had better be that $0 \leq r < b$ for some $r, q \in \mathbb{Z}$. □

Corollary 1.8
$\mathbb{Z}$ is a Euclidean domain, with a Euclidean function given by lemma 1.7.

Definition 1.9 (Euclidean Domain)
Let R be an integral domain. R is a Euclidean domain if there exists a function $\lambda : R \setminus \{0\} \to \mathbb{N}$ such that if $a, b \in R$ with $b \neq 0$, then there exists some $c, d \in R$ with the property that $a = cb + d$ with $d = 0$ or $\lambda(d) < \lambda(b)$.

Example 1.10
$\mathbb{Z}$ is a Euclidean domain with λ function given in lemma 1.7.

$R[x]$ for field R is also a Euclidean domain, with $\lambda = \deg$.

Proposition 1.11
If R is a Euclidean domain, then R is a principal ideal domain. That is, if $I \subseteq R$ is an ideal, then $\exists a \in R$ such that $I = Ra = \{ra \mid r \in R\}$.

Proof. Assume WLOG that I is not the trivial ideal $I \neq (0)$. Let $0 \neq a \in I$ such that $\lambda(a) \leq \lambda(b) \forall b \in I, b \neq 0$.

We claim that $I = (a) = Ra$.

We know that $Ra \subseteq I$ since I is an ideal. Let $b \in I$. Then $\exists c, d \in R$ such that $b = ca + d$ where $d = 0$ or $\lambda(d) < \lambda(a)$. Now we have $d = b - ca \in I$, so we can't have $\lambda(d) < \lambda(a)$. Thus $d = 0$, so $b = ca \in Ra$.

Hence we have $I \subseteq Ra$. Together, we conclude that $I = Ra$. □

Definition 1.12 (Principal Ideals, PIDs)
If $I = (a)$ for some $a \in I$, then I is said to be a principal ideal.

R is a principal ideal domain (PID) if every ideal of R is principal.

Here are some important properties of PIDs:

1. Nonunit irreducible elements are exactly the prime elements in R.

   Recall: $p \in R$ is irreducible if $a \mid p \Rightarrow a$ is either a unit or an associate of p.

   $p \in R$ is prime if $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ and p is a nonzero, nonunit of R.

2. GCDs always exist in PIDs.

§1.3 Unique Prime Factorization

We're nearly ready to prove unique factorization, after a lemma:

Lemma 1.13
Suppose p is a prime, and $a, b \in Z$. Then $\text{ord}_p(ab) = \text{ord}_p a + \text{ord}_p b$.

Proof. WLOG, assume $a, b \neq 0$. We let

$$\alpha = \text{ord}_p a$$
$$\beta = \text{ord}_p b$$

Then we have

$$a = p^\alpha \cdot c \text{ where } p \nmid c$$
$$b = p^\beta \cdot d \text{ where } p \nmid d$$

Thus, $ab = p^{\alpha+\beta} \cdot cd$. We have that $p \nmid cd$ since $p \nmid c$ and $p \nmid d$ (we rely on the fact that if p is irreducible, p is prime). Thus we have that $\text{ord}_p(ab) = \alpha + \beta$. □

Proof. (of theorem 1.6, that $\mathbb{Z}$ is a UFD). Recall that for a nonzero $n \in \mathbb{Z}$, we write

$$n = (-1)^{\varepsilon} \prod_p p^{a(p)}, \text{where } \varepsilon = 0 \text{ or } 1 \text{ and } a(p) \geq 0$$

Given a positive prime q, we take ord_q of both sides. By lemma 1.13, this yields

$$\text{ord}_q n = \varepsilon \cdot \text{ord}_q(-1) + \sigma_p a(p) \, \text{ord}_q(p)$$

Since we have that $\text{ord}_q(-1) = 0$ and $\text{ord}_q(p) = 0, \forall p \neq q$, we've uniquely determined $a(q)$ since $\text{ord}_q(n) = a(q)$. That is, $a(q)$ is *uniquely determined* for all primes q. So n has a *unique* prime factorization. □

§1.4 Greatest Common Divisors

Definition 1.14

Let R be an integral domain. Then $d \in R$ is said to be a gcd of two elements a, b if

i) $d \mid a$ and $d \mid b$,

ii) if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

Remark. An aside for ring theory enthusiasts: gcd domains are a class of rings mroe general than PIDs or UFDs.

We will denote (a, b) as the gcd of a and b.

Caution, however! gcd's are only unique up to units.

Example

-5 and 5 are both gcds of -5 and 10 since -1 is a unit.

We will make the convention that the gcd of 2 integers is the positive gcd, that is, $(-5, 10) = 5$.

An edge case is that $\gcd(0, 0) = 0$.

§2 February 3, 2022

§2.1 Arithmetic Functions

We look at arithmetic functions and how they act on prime numbers:

Definition 2.1 (Arithmetic Function)
An arithmetic function is a function $f : \mathbb{Z}_+ \to \mathbb{C}$.

(Typically, these are integer valued.)

Example 2.2
We have some examples of arithmetic functions:

- Euler ϕ function.
- $\tau(n)$, the counting function. It takes a positive integer and counts the number of positive divisors of n.
$$\tau(n) = \sum_{d|n} 1$$
- $\sigma(n)$, the sum of divisors function. It is the sum over all the positive divisors of n.
$$\sigma(n) = \sum_{d|n} d$$

We have some properties of these functions, like *multiplicative*, *completely multiplicative*, *additive*, *completely additive*.

Definition 2.3 (Multiplicativity)
An arithmetic function f is multiplicative if
$$f(mn) = f(m)f(n) \quad \text{whenever } (m,n) = 1$$
f is said to be totally or completely multiplicative if
$$f(mn) = f(m)f(n) \quad \forall m, n \in \mathbb{Z}_+$$
regardless of coprimality.

If f is multiplicative and $n_1, \ldots, n_k$ are positive pairwise coprime integers, then

$$f(n_1 \ldots n_k) = f(n_1)f(n_2)\ldots f(n_k).$$

A particular case that is useful is when we write

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

so that assuming multiplicativity, we have that

$$f(n) = f(p_1^{e_1})f(p_2^{e_2}) \cdots f(p_k^{e_k})$$

A common type of arithmetic function is a summatory function, namely a function f of the form

$$f(n) = \sum_{d|n} g(d), \quad \text{where } g \text{ is some arithmetic function.}$$

Food for thought: how special are summatory functions within the set of all arithmetic functions?

A special property of summatory functions is that they "inherit multiplicativity".

Lemma 2.4

If g is a multiplicative function, and

$$f(n) = \sum_{d|n} g(d) \quad \forall n,$$

then f itself is multiplicative.

Proof. Suppose $m, n \in \mathbb{Z}_+$ are coprime positive integers.

The divisors d of mn are the products $a \cdot b$ where $a \mid m$ and $b \mid n$. Each such pair a, b yields a uniquely determined produce $d = a \cdot b$. Conversely, since $(m, n) = 1$, each divisor d of mn determines a unique divisor $a = \gcd(d, m)$ and $b = \gcd(d, n)$ so that $d = a \cdot b$.

Thus there is a *bijection* between divisors of mn and m, n separately

$$d \mid mn \longleftrightarrow (a \mid m, b \mid n)$$

Thus we have

$$\begin{aligned} f(m \cdot n) &= \sum_{d|mn} g(d) \\ &= \sum_{a|m} \sum_{b|n} g(ab) \\ &= \sum_{a|m} \sum_{b|n} g(a)g(b) \\ &= \left(\sum_{a|m} g(a) \right) \left(\sum_{b|n} g(b) \right) = f(m) \cdot f(n) \end{aligned}$$

Thus completes the proof that f is multiplicative. □

Recall: The functions introduced earlier

$$\tau(n) = \sum_{d|n} 1 \qquad \sigma(n) = \sum_{d|n} d$$

So τ is the summatory function of the constant 1 functions, and σ is the summatory function of the identity function. We know that the constant 1 function and the identity function are both completely multiplicative, so σ and τ are multiplicative functions.

The implication of which is that it suffices to apply τ and σ on prime powers and multiply.

Let p be a prime. Then

$$\tau(p^e) = e + 1 \quad (\text{from } p^0 \text{ to } p^e).$$

We also have

$$\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1}$$

Therefore, if $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then

$$\tau(n) = \prod_{i=1}^{k} (e_i + 1)$$
$$\sigma(n) = \prod_{i=1}^{k} \left(\frac{p_i^{e_i+1} - 1}{p_i - 1} \right).$$

Remark 2.5. There are higher order divisor functions

$$\sigma_k(n) = \sum_{d|n} d^k$$

so $\sigma_0 = \tau, \sigma_1 = \sigma, \ldots$

§2.2 Review of $\mathbb{Z}/n\mathbb{Z}$ and its units

Definition 2.6 (Modular Congruence)
If $a, b, m \in \mathbb{Z}$, $m \neq 0$, we say that a is congruent to b modulo m if $m \mid b - a$. We write

$$a \equiv b \mod m, \text{ or more simply } a \equiv b \ (m)$$

Congruence mod m is an equivalence relation on $\mathbb{Z}$. If $a \in \mathbb{Z}$, $\overline{a}$ denotes the set of integers congruent to $a \mod m$, i.e. $\overline{a} = \{a + km \mid k \in \mathbb{Z}\}$.

Definition 2.7 ($\mathbb{Z}/m\mathbb{Z}$, Residues mod m)

The set of congruence classes mod m is denoted $\mathbb{Z}/m\mathbb{Z}$. This is a quotient ring of the ring of integers $\mathbb{Z}$.

If $\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_m$ form a complete set of congruence classes mod m, then the set of integers $\{a_1, a_2, \ldots, a_m\}$ is called a complete set of residues mod m.

$\mathbb{Z}/m\mathbb{Z}$ can be endowed with the structure of a commutative ring by setting

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$\text{and } \overline{a} \cdot \overline{b} = \overline{ab},$$

and proving that this is well-defined as ring operations.

Proposition 2.8

The set of units in $\mathbb{Z}/m\mathbb{Z}$ is exactly

$$\{\overline{a} \mid (a, m) = 1\}$$

Proof. Let $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$, then

$$\exists \overline{b} \in \mathbb{Z}/m\mathbb{Z} \text{ s.t. } \overline{b} \cdot \overline{a} \equiv 1 \mod m$$
$$\iff \exists b, n \in \mathbb{Z} \text{ s.t. } ba - mn = 1$$

Then by Bézout's identity...

$$\iff (a, m) = 1$$

□

§2.3 The Euler ϕ Function

For $n \in \mathbb{Z}_+$, $\phi(n)$ is defined to be the number of integers $1 \leq m \leq n$ coprime to n.

Example 2.9

We have some examples of the Euler ϕ functions:

$$\phi(1) = 1$$
$$\phi(p) = p - 1 \text{ for any prime } p$$

Let $e \geq 1$,

$$\phi(p^e) = p^e - p^{e-1} \text{ for prime powers, we exclude multiples of } p$$

Wouldn't be great if ϕ were multiplicative? It is!

Theorem 2.10
If $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Proof. By the Chinese Remainder Theorem[2], $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ if $(m, n) = 1$.

Taking the unit groups on both sides, we have

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

and the Euler ϕ function is simply measuring the order of said unit groups ($\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$). □

Here is an important fact about the Euler ϕ function:

Proposition 2.11
We have

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

Proof. (1: a cute, snazzy proof) Consider the n rational numbers

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n} = 1$$

and reduce all to lowest terms so that the numerator and denominator are coprime.

Q: Given a positive divisor d of n, how many fractions have d as the denominator?

A: We have exactly $\phi(d)$ of them.

Conversely, every denominator d is certainly a divisor of n. So we conclude that $n = \sum_{d|n} \phi(d)$. □

Proof. (2: using what we've learnt) We use the fact that ϕ is multiplicative, and that this function is a summatory function of ϕ, so this function itself is multiplicative. We can decompose this into prime powers. So it suffices to show this for prime powers.

[2]This is an easy way to prove this assuming Math 1530 (Abstract Algebra). There is another way to prove this with one hand tied behind the back, it just takes more mental muscle to do.

Let $n = p^k$. Let

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

Then we have

$$f(p^k) = \sum_{d|p^k} \phi(d) = 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1})$$

which is a telescoping sum which leaves

$$= p^k$$

which is as intended. □

§3 February 8, 2022

§3.1 Dirichlet Convolutions

Definition 3.1 (Dirichlet Convolution)

Let f, g be arithmetic functions. Then the Dirichlet convolution/product of g and g it

$$\begin{aligned}(f * g)(n) :&= \sum_{d_1 d_2 = n} f(d_1) g(d_2) \\ &= \sum_{d|n} f(d) g(n/d)\end{aligned}$$

We do check that this has properties that we want it to have, like associativity:

$$\begin{aligned}((f * g) * h)(n) &= (f * (g * h))(n) \\ &= \sum_{d_1 d_2 d_3 = n} f(d_1) g(d_2) h(d_3)\end{aligned}$$

It is also clearly commutative.

We also have that this product has a multiplicative identity.

Definition 3.2

Let $I : \mathbb{Z}_+ \to \{0, 1\}$ be given by

$$I(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Then I is an identity for $*$, in the sense that $f * I = I * f = f$.

Lemma 3.3

If f is an arithmetic function such that $f(1) \neq 0$, then there exists an arithmetic function g such that $f * g = I$.

It is given recursively by

$$g(1) = \frac{1}{f(1)}$$
$$g(n) = -\frac{1}{f(1)} \cdot \sum_{d|n, d<n} g(d) f(n/d)$$

Proof. We want to show that given g and g defined as above, we have that $f * g = I$.

$n = 1$:

$$g(1) \cdot f(1) = \frac{1}{f(1)} f(1) = 1$$

$n > 1$:

$$\begin{aligned} \sum_{d|n} g(d) f(n/d) &= g(n) \cdot f(1) + \sum_{d|n, n<n} g(d) f(n/d) \\ &= -\frac{1}{f(1)} \cdot \sum_{d|n, d<n} g(d) f(n/d) \cdot f(1) + \sum_{d|n, n<n} g(d) f(n/d) \\ &= 0 \end{aligned}$$

So g is indeed an inverse of f since they produce the identity function I. □

§3.2 Möbius Inversion

The motivation of this is: given a summatory function of multiplicative functions, can we recover the multiplicative function?

Definition 3.4 (Möbius μ Function)

We define $\mu : \mathbb{Z}_+ \to \{-1, 0, 1\}$ given by

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n = p_1 p_2 \dots p_k \text{ if } p_i \text{ are pairwise distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

(We note that $\mu(1) = 1$.)

Lemma 3.5

μ is a multiplicative function.

Proof. Let $m, n \in \mathbb{Z}_+$ such that $(m, n) = 1$. We write

$$m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$
$$n = q_1^{f_1} q_2^{f_2} \cdots q_l^{f_l}$$

Case 1 Some exponent e_i or $f_i \geq 2$. Then we have that

$$\mu(mn) = \mu(m)\mu(n) = 0$$

Case 2 We have that

$$m = p_1 p_2 \cdots p_k$$
$$n = q_1 q_2 \cdots q_l$$

where p_i and q_i are all pairwise distinct. Then $\mu(m) = (-1)^k$ and $\mu(n) = (-1)^l$, so $\mu(m) = \mu(n) = (-1)^{k+l}$.

Since these are coprime $(m, n) = 1$, then we have that $\mu(mn) = (-1)^{k+l}$.

Which is as intended, giving that μ is a multiplicative function. □

Lemma 3.6

We have the property:

$$\sum_{d|n} \mu(d) = 0 \qquad \forall n \geq 2.$$

Which tells us that the summatory function of μ is I.

Proof. We define

$$f(n) := \sum_{d|n} \mu(d) \qquad \text{is multiplicative}$$

We check this on prime powers, for prime p and $e \geq 1$:

$$\begin{aligned} f(p^e) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^e) \\ &= 1 - 1 + 0 + \cdots + 0 = 0 \end{aligned}$$

so we're done since f is multiplicative and is 0 for all power of primes. □

Lemma 3.7

Let $i : \mathbb{Z}_+ \to \{1\}$ be the constant 1 function.

$$i * \mu = \mu * i = I$$

Proof. In the case of $n = 1$, we have $i(1)\mu(1) = 1$.

For $n > 1$, we have $(i * \mu)(n) = \sum_{d|n} \mu(d) = 0$ from above. □

We see here that summatory functions can be seen as Dirichlet products: the summatory function F of f is $F = f * i$. What we said about summatory functions being multiplicative boils down to Dirichlet convolutions preserving multiplicativity.

Recall: that summatory functions inherit multiplicativity. In fact, this holds for Dirichlet products as well. If f, g are multiplicative, then so is $f * g$.

The proof is parallel to the proof for summatory functions, for lemma 2.4.

Theorem 3.8 (Möbius Inversion)

Let

$$F(n) = \sum_{d|n} f(d)$$

Then we have

$$f(n) = \sum_{d|n} \mu(d) \cdot F(n/d) = \mu * F.$$

Proof. $F = f * i$, then

$$F * \mu = (f * i) * \mu = f * (i * \mu) = f * I = f.$$

which was simpler than I expected... □

Corollary 3.9

If F is the summatory function of f, and F is multiplicative, then f is also multiplicative, as $f = \mu * F$ and μ is multiplicative and convolutions with multiplicative functions are multiplicative.

Corollary 3.10

Corollary 3.9 gives another proof that ϕ is multiplicative, as

$$\sum_{d|n} \phi(d) = \phi * i = \mathrm{id}.$$

§3.3 Applications of Möbius Inversion

§3.3.1 Cyclotomic Polynomials

Recall: the n^{th} cyclotomic polynomial $\Phi_n(x)$ is the unique irreducible polynomial in $\mathbb{Z}[x]$ dividing $x^n - 1$ but no $x^k - 1$ for $k < n$.

Thus

$$\Phi_n(x) = \prod_{\substack{1 \le k < n \\ (k,n)=1}} \left(x - e^{2\pi i k/n}\right)$$

as the roots of this polynomial are exactly the primitive n^{th} roots of unity. We have that

$$\prod_{d|n} \Phi_d(x) = x^n - 1.$$

By Möbius inversion, if

$$G(n) = \prod_{d|n} g(d),$$

then we have that

$$g(n) = \prod_{d|n} G(d)^{\mu(n/d)}$$

In particular, taking $G(n) = x^n - 1$ (with particular $x \in \mathbb{C}$) as an arithmetic function, we have

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} \qquad (x \in \mathbb{C})$$

Applying this identity for enough $x \in \mathbb{C}$ yields this as an identity of polynomials.

§3.3.2 Dynatomic Polynomials

The roots of cyclatomic polynomials are roots of unity. Dynatomic polynomials have as roots the periodic points (of certain periods) of a polynomial.

Definition 3.11

Let K be a field, and let $f \in K[x]$ of degree $d \geq 2$. Let

$$f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}$$

then $P \in \overline{K}$[a] is said to be periodic under f if

$$f^n(P) = P \qquad \text{for some } n \geq 1$$

[a] Algebraic numbers in field K, the field you get by adjoining all roots of polynomials in $K[x]$.

Example 3.12

Let $f(x) = x^2 - 1$. 0 is a period point under f:

$$0 \longmapsto -1 \longmapsto 0$$

and its period is 2.

> **Remark.** If n is the smallest positive integer such that $f^n(p) = p$ (p periodic), then we call n the exact period of p under f.

Definition 3.13

The n^{th} dynatomic polynomial of f is

$$\Phi_{f,n}(x) := \prod_{d|n} \left(f^d(x) - x\right)^{\mu(n/d)}$$

We hope that $\Phi_{f,n}(x)$ has as its roots the points of exact period n... This hope is dashed...

Example 3.14

$f(x) = x^2 - \frac{3}{4}$.

$$f^2(x) - x = \left(x - \frac{3}{2}\right)\left(1 - \frac{1}{2}\right)^3$$
$$f(x) - x = \left(x - \frac{3}{2}\right)\left(x + \frac{1}{2}\right)$$

Thus

$$\frac{f^2(x) - x}{f(x) - x} = \left(x + \frac{1}{2}\right)^2$$

But $x = -\frac{1}{2}$ is fixed under f.

§4 February 10, 2022

§4.1 Congruences *continued*

Recall: that for $m \in \mathbb{Z}_+$, $a, b \in \mathbb{Z}$, the linear congruence

$$ax \equiv b \mod m$$

has a solution if and only if $(a, m) \mid b$. Unwinding this gives Bezout's identity.

Q: How do we actually find a solution?

A: Either guess and check; or apply the following algorithm:

1) Divide all terms in the congruence by $d = (a, m)$.

2) If step 1 yields

$$a'x \equiv b' \mod m'$$

with $(a', m') = 1$, then $d := (a', b')$ is a unit mod m', so we can divide both sides by d'.

$$a'd'^{-1}x \equiv b'd'^{-1} \mod m'$$

3) Let $a''x \equiv b'' \mod m$ be the result so far. We replace b'' by some $b'' + km'$[3] such that $(a'', b'' + km') > 1$ allows us to repeat step 2. This results in some a''' such that $|a'''| < |a''|$.

Given that we repeat this process, this must eventually terminate, since the absolute values of the a terms are strictly decreasing each time.

Example 4.1

Let $10x \equiv 6 \mod 14$.

1) $(a, m) = (10, 14) = 2$ so we divide through by 2.

$$5x \equiv 3 \mod 7$$

2) Irrelevant since $(5, 3)$ are coprime.

3) Consider integers of form $3 + 7k$, and see which are divisible by 5. We can take $k = 1$. We

[3] Since made a' and m' coprime, we have $(a', m') = 1$ so we can indeed solve congruence $a''q \equiv b'' + km'$ gives noncoprime pairs.

get

$$5x \equiv 10 \mod 7$$

2) Divide by $(5, 10) = 5$ so we have $x \equiv 2 \mod 7$.

§4.2 Simultaneous Linear Congruences

Recall: the CRT/Sun-tzu's theorem.

Theorem 4.2 (Sun-tzu's Theorem / Chinese Remainder Theorem)
Suppose that $m = m_1 m_2 \cdots m_t$ with $(m_i, m_j) = 1 \forall i \neq j$.

Let $b_1, b_2 \ldots, b_t$ be integers, and consider the system of congruences

$$\begin{aligned} x_1 &\equiv b_1 \mod m_1 \\ x_2 &\equiv b_2 \mod m_2 \\ &\vdots \\ x_t &\equiv b_t \mod m_t \end{aligned} \tag{$*$}$$

Then this system has a unique solution modulo m[a].

[a] That is, we have at least one solution, and we can shift it by *any* multiple of m.

Proof. Let $n_i = m_1 m_2 \cdots \cancel{m_i} \cdots m_t = \frac{m}{m_i}$ for each i. Since m_i is coprime to m_j, $\forall j \neq i$, we have $(n_i, m_i) = 1 \forall i$. Then, there exists solutions $r_i, s_i \in \mathbb{Z}$ such that

$$r_i m_i + s_i n_i = 1$$

Let $e_i = s_i n_i$. Then for each i,

$$e_i \equiv 1 \mod m_i$$

and $e_i \equiv 0 \mod m_j$, $\forall j \neq i$.

Our goal is to ultimately show

$$\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_t\mathbb{Z}$$

with each e_i generating the "$\mathbb{Z}/m_i\mathbb{Z}$ piece".

Set

$$x_0 = \sum_{i=1}^{t} b_i e_i$$

so that $x_0 \equiv b_i \pmod{m_i}$ $\forall i$, so x_0 is a solution to eq. $(*)$.

Suppose x_1 is another solution. Then we have

$$x_1 - x_0 \equiv 0 \mod m_i \ \forall i, 1 \leq i \leq t$$

Since the m_i are pairwise coprime, we get $m \mid x_1 - x_0$. □

§4.3 Structure of Unit Groups

Recall: in Math 1530, we learned Lagrange's theorem

Theorem 4.3 (Lagrange's Theorem)
If G is a finite group, then for every subgroup H of G, we have $|H| \mid |G|$.

Corollary 4.4
If G is a finite group of order n, and $a \in G$, then $a^n = e$, where e is the identity of the group.

We've seen that $|U(m)| = \phi(m)$.[4] Applying Lagrange's theorem, we have Euler's theorem:

Theorem 4.5 (Euler's Theorem)
For any $a \in \mathbb{Z}$ with $(a, m) = 1$, we have $a^{\phi(m)} \equiv 1 \mod m$.

Definition 4.6
A subset R of $\mathbb{Z}$ is said to be a reduced set of residues mod m if R contains exactly one element from each of the $\phi(m)$ congruence classes that are units mod m.

Alternate proof of theorem 4.5. Let $R = \{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a reduced set of residues mod m. If $(a, m) = 1$, then aR is also a reduced set of residues mod m. Thus, if $x_1, x_2, \ldots, x_{\phi(m)} \in aR$ (pairwise distinct), then

$$\begin{aligned} x_1 x_2 \cdots x_{\phi(m)} &\equiv r_1 r_2 \cdots r_{\phi(m)} \mod m \\ (ar_1)(ar_2)\cdots(ar_{\phi(m)}) &\equiv r_1 r_2 \cdots r_{\phi(m)} \mod m \\ a^{\phi(m)}(r_1 r_2 \cdots r_{\phi(m)}) &\equiv r_1 r_2 \cdots r_{\phi(m)} \mod m \end{aligned}$$

since all the r_i are units mod m, we divide through

$$a^{\phi(m)} \equiv 1 \mod m$$

Which is as desired. □

[4] For notation, we use $U(m) := (\mathbb{Z}/m\mathbb{Z})^\times$.

We'll be studying roots of polynomials over $\mathbb{Z}/m\mathbb{Z}$, especially polynomials of the form $x^d - a$.

By Sun-tzu's theorem, the case of m being a prime power is especially important. This turns out to have a lot to do with the case that $m = p$ is a prime itself.

First something further *afield*:

Proposition 4.7

If p is a prime and $p \nmid d$ for $d \in \mathbb{Z}_+$, then the polynomial

$$x^d - a \in (\mathbb{Z}/p\mathbb{Z})[x], \qquad a \not\equiv 0 \pmod{p}$$

has exactly d roots in some extension of $\mathbb{F}_p$.

Conversely, if $p \mid d$, then there are fewer than d roots in any extension of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

The proof uses the following proposition:

Proposition

A nonzero polynomial $f \in K[x]$ is separable if and only if it is relatively prime to its derivative f'. (A separable polynomial whose roots in its algebraic closure $\overline{K}$ whose roots are all distinct).

Proof.

$\Rightarrow$ **Right Direction:** Suppose f is separable and α be any root of f. Then $f(x) = (x - \alpha)h(x)$, where $h(\alpha) \neq 0$ since α is a non-repeated root.

We have $f'(\alpha) = h(\alpha) \neq 0$, so α is not a root of f'. Thus f and f' have no common roots, so they are coprime.

$\Leftarrow$ **Left Direction:** Prove by contrapositive. Suppose f is not separable. i.e. it has some repeated root which we call α.

Then $f(x) = (x-\alpha)^2 g(x)$, so $f'(x) = (x-\alpha)^2 g'(x) + 2(x-\alpha)g(x)$. We see that $x - \alpha$ divides both f and f' so $(f, f') \neq 1$.

Which concludes the bidirectional. □

Proof of proposition 4.7. We have $f(x) = x^d - a$, $a \not\equiv 0 \pmod{p}$ has d distinct solutions in some extension of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, because

$$f'(x) = dx^{d-1} \pmod{p}$$

and with 0 as its only root but 0 is not a root of f. By above we have that f is separable.

Conversely, if $p \mid d$, then

$$f'(x) \equiv 0 \pmod{p},$$

so $(f, f') \neq 1$, meaning that f is not separable. □

Proposition 4.8 (4.1.2 of text)
If p is a prime and if $d \mid p-1$, then the polynomial

$$x^{d-1} \in (\mathbb{Z}/p\mathbb{Z})[x]$$

has exactly d roots in the base field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Proof. We know this is true in the case of $d = p-1$ because of Fermat's Little Theorem (also Euler's Theorem).

We also note that $(x^d - 1) \mid (x^{p-1} - 1)$. Since $x^{p-1} - 1$ has all roots in the base field by FLT, $x^d - 1$ had better also retain its roots in the base field $\mathbb{F}_p$ by contradiction. □

§5 February 15, 2022

§5.1 Cyclicity of Groups

§5.1.1 mod odd p

Recall: from last class, we had proposition 4.8:

Proposition
If p is a prime and if $d \mid p-1$, then the polynomial

$$x^{d-1} \in (\mathbb{Z}/p\mathbb{Z})[x]$$

has exactly d roots in the base field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Corollary 5.1
$G := (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Proof. For $d \mid (p-1)$, we write $\psi(d)$ for the number of elements of G having order d.

Proposition 2 implies that[5]

$$\sum_{c|d} \psi(c) = d \qquad (\psi * i = \mathrm{id}, \psi = \mathrm{id} * \mu)$$

Möbius inversion gives

$$\psi(d) = \sum_{c|d} \mu(c) \frac{d}{c}.$$

On the other hand, we have $\mathrm{id} = \phi * i \Rightarrow \phi = \mu * \mathrm{id}$. Thus $\psi(d) = \phi(d)$ for all $d \mid (p-1)$. So in particular, $\psi(p-1) = \phi(p-1) \geq 1$ for any prime p. □

§5.1.2 mod odd power p^e

Theorem 5.2

Let $p \in \mathbb{Z}_+$ be an odd prime, and let $e \geq 1$. Then $U(p^e)$ is cyclic.

Proof overview:

1. Pick a primitive root mod p. We call it g (for generator).

2. Show that either g or $g + p$ is a primitive root mod p^2.

3. Show that if h is any primitive root mod p^2, then h is a primitive root mod p^e $\forall e \geq 2$.

Proof of theorem 5.2.

Step 1. Let g be a primitive root modulo p given by corollary 5.1.

Step 2. Let d be the order of g mod p^2. Since $\phi(p^2) = p(p-1)$, we have that

$$d \mid p(p-1) \qquad \text{by Lagange.}$$

By definition of d,

$$g^d \equiv 1 \mod p^2$$

so we also have

$$g^d \equiv 1 \mod p$$

Thus $(p-1) \mid d$ since g has order $p-1$ mod p. Altogether, d is either $p-1$ or $p(p-1)$. If $d = p(p-1)$, then we are done with step 2. So we assume the former that $d = p-1$.

Let $h = g + p$. We know that h is a primitive root mod p, so we do the same [yoga] as above and conclude that the order of h mod p^2 is either $p-1$ or $p(p-1)$.

[5] We throw in Lagrange's theorem, and essentially count the number of solutions to $x^d \equiv 1$.

By our new hypothesis,

$$g^{p-1} \equiv 1 \pmod{p^2}$$

so modulo p^2, we have

$$h^{p-1} = (g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + \cdots + p^{p-1}$$

Modulo p^2, the only terms that survive are (expand and all p^2 terms die):

$$\equiv 1 - pg^{p-2} \pmod{p^2}$$

But $p \nmid g$, so $pg^{p-2} \not\equiv 0 \mod p$, and hence $h^{p-1} \not\equiv 1 \mod p^2$. Thus the order of h mod p^2 is $p(p-1)$, so h generates $U(p^2)$.

So we are done with step 2. If g is a primitive root mod p, then either g or $g+p$ is a primitive root mod p^2.

Step 3. We wish to show that a primitive root mod p^2 is also a primitive root mod p^e $\forall e \geq 2$. We induct on e.

Let h be a primitive root mod p^e for some fixed $e \geq 2$. Let d be the order of h mod p^{e+1}. By Lagange, we have that $d \mid \phi(p^{e+1}) = p^e(p-1)$, and from step 2,

$$\phi(p^e) = p^{e-1}(p-1) \mid d$$

Hence $d = p^e(p-1)$ or $p^{e-1}(p-1)$. If it's the former then we are done, so we assume latter.

We want to show that

$$h^{p^{e-1}(p-1)} \not\equiv 1 \mod p^{e+1}$$

implying that $d = p^e(p-1)$ after all.

Since h has order $\phi(p^e) = p^{e-1}(p-1)$ in $U(p^e)$, we have

$$h^{p^{e-2}(p-1)} \not\equiv 1 \mod p^e \tag{$\star$}$$

However,

$$h^{p^{e-2}(p-1)} \equiv 1 \mod p^{e-1} \tag{$\star\star$}$$

Combining eq. ($\star$) and eq. ($\star\star$) yields

$$h^{p^{e-2}(p-1)} = 1 + kp^{e-1}$$

where $p \nmid k$. Therefore, we have

$$\begin{aligned} h^{p^{e-1}(p-1)} &= (1+kp^{e-1})^p \\ &= 1 + pkp^{e-1} + \binom{p}{2}k^2p^{2e-2} + \cdots \end{aligned}$$

Subsequent terms are all divisible by $p^{3e-3} = (p^{e-1})^3$, and hence divisible by p^{e+1} as $e(e-1) \geq 2+1$ $\forall e \geq 2$. Thus

$$h^{p^{e-1}(p-1)} = 1 + kp^e + \frac{1}{2}k^2p^{2e-1}(p-1) \mod p^e + 1$$

p is odd, so

$$\frac{1}{2}k^2p^{2e-1}(p-1)$$

is divisible by p^{e+1}, since $2e-1 \geq e+1$. Thus

$$h^{p^{e-1}(p-1)} \equiv 1 + kp^e \mod p^e + 1$$

Since $p \nmid k$, we get that $kp^e \not\equiv 0$ so

$$h^{p^{e-1}(p-1)} \not\equiv 1 \mod p^e + 1$$

This proves that $d = p^e(p-1)$, which is to say that h is a primitive root mod p^{e+1}.

Altogether, we have that $U(p^e)$ is cyclic. □

§5.1.3 mod powers of 2

Theorem 5.3
$U(2^e)$ is cyclic iff $e = 1$ or $e = 2$.

Proof. Clearly $U(2)$ and $U(4)$ are cyclic[6].

We show that $U(2^e)$ is *not* cyclic for all $e \geq 3$. Notice: it suffices to show that $U(8)$ is not cyclic, since we can find group homomorphisms down powers of 2.

$$U(8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$$

and $\overline{1}^2 = \overline{3}^2 = \overline{5}^2 = \overline{7}^2 \mod 8$. □

§5.2 Classification of all cyclic unit groups

Corollary 5.4
$U(m)$ is cyclic if and only if $m = 1, 2, 4, p^e$ or $2p^e$ for some odd prime p.

Proof. Recall that a product G of finite cyclic groups G_1 and G_2 is cyclic iff $(|G_1|, |G_2|) = 1$.[7] On the other hand, $\phi(m)$ is even $\forall m \geq 3$. So only one of G_1 and G_2 needs odd power.

Combined with our structure theorems on $U(p^e)$ for primes p, this proves the corollary since these are the only possibilities. □

[6] We don't have much choice since there is only one trivial group and one group of order 2, both cyclic.
[7] Secretly, Chinese Remainder Theorem.

§6 February 17, 2022

§6.1 Special Integers

§6.1.1 Fermat and Mersenne Primes

We make the observation that many small primes are of the form $2^m \pm 1$ for some natural number m, for example

$$3, 5, 7, 17, 31$$

We deal with the $+1$ and -1 cases separately.

Lemma 6.1

If $2^m + 1$ is prime, then $m = 2^n$ for some $n \geq 0$.

Proof. We show the contrapositive. Suppose m is not a power of 2. We write $m = 2^n \cdot q$ for some odd $q > 1$.

The polynomial

$$f(t) = t^q + 1$$

has $t = -1$ as a root, so

$$f(t) = (t+1)g(t) \quad \text{where } \deg f = q > 1$$

Thus

$$\begin{aligned} x^m + 1 &= f(x^{2^n}) \\ &= (x^{2^n} + 1)g(x^{2^n}) \text{ where } m > 2^n \end{aligned}$$

Plugging in $x = 2$ gives

$$2^{2^n} + 1 \mid 2^m + 1, \text{ and } 2^{2^n} + 1 < 2^m + 1$$

so $2^m + 1$ is not prime. □

Definition 6.2 (Fermat Numbers)

Numbers of the form $2^{2^n} + 1$ are called Fermat numbers.

Fermat numbers that are prime are called Fermat primes.

The first few Fermat numbers happen to be prime: $3, 5, 17, 257, 65537$.

Conjecture

Fermat conjectured that Fermat numbers are prime.

This is very false! Euler found that

$$2^{2^5} + 1 = 641 \times 6700417$$

We now turn to Mersenne numbers.

Lemma 6.3

If $m > 1$ and $a^m - 1$ is prime, then $a = 2$ and m is prime.

Proof. Suppose m is composite and, so $m = nk$, $1 < k, n < m$. Then

$$\begin{aligned} a^m - 1 &= (a^k)^m - 1 \\ &= (a^k - 1)(a^{k(n-1)} + \cdots + 1) \end{aligned}$$

This implies that $a^m - 1$ is composite. Hence m had better be prime.

Now $a^m - 1 = (a-1)(a^{m-1} + \cdots + 1)$, so we further have that $a = 2$. □

Definition 6.4 (Mersenne Numbers)

Integers of the form $2^p - 1$ where p is a prime are called Mersenne numbers.

Mersenne numbers that are prime are called Mersenne primes.

There is a current ongoing search for more Mersenne primes on the internet. Currently, the largest known Mersenne prime (and largest known prime number) is

$$M(82,589,933)$$

That is,

$$2^{82,589,933} - 1$$

Mersenne primes are related to perfect numbers. There is a one-to-one correspondence with Mersenne primes and even perfect numbers.

Definition 6.5 (Perfect Number)
$n \in \mathbb{Z}_+$ is called perfect if

$$n = \sum_{\substack{d|n \\ d<n}} d$$

Example 6.6
We have

$$6 = 1 + 2 + 3$$
$$28 = 1 + 2 + 4 + 7 + 14$$

Proposition 6.7
If $n^{2^{p-1}}(2^p - 1)$ where $p \in \mathbb{Z}_+$, and $p, 2^p - 1$ are prime, then n is perfect.

Proof. The function $\sigma(n) = \sum_{d|n} d$ is multiplicative. So if

$$n = 2^{p-1}(2^p - 1)$$

then

$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1).$$

since they are coprime. Now we also

$$\sigma(2^{p-1}) = \frac{2^p - 1}{2 - 1} = 2^p - 1$$
$$\sigma(2^p - 1) = 1 + (2^p - 1) = 2^p$$

Hence $\sigma(n) = (2^{p-1}) \cdot 2^p = 2n$.

So n is a perfect number. □

Proposition 6.8
If $n \in \mathbb{Z}_+$ is even and perfect, then $n = 2^{p-1}(2^p - 1)$ where p and $2^p - 1$ are both prime.

Proof. This is a homework exercise! □

It is currently conjectured that there are no odd perfect numbers.

§6.1.2 Pseudoprimes and Carmichael Numbers

Homework 2 includes a problem for which a special case is Wilson's Theorem.

Theorem 6.9 (Wilson's Theorem)
If p is a prime, then

$$(p-1)! \equiv -1 \pmod{p}$$

The converse is also true.

Proposition 6.10
If $n \in \mathbb{Z}_+$ where $n \geq 2$ is such that

$$(n-1)! \equiv 1 \pmod{n} \qquad (*)$$

then n is prime.

We can think of eq. $(*)$ as a rudimentary 'primality test'.

However, this is not a great primality test, because factorials are expensive to compute.

Recall Fermat's little theorem.

Theorem 6.11 (Fermat's Little Theorem)
If $p \in \mathbb{Z}_+$ is a prime and $a \in \mathbb{Z}$, then

$$a^p \equiv a \mod p$$

Thus $n \in \mathbb{Z}_+$ and

$$a^n \equiv a \mod n$$

for some $a \in \mathbb{Z}_+$, then n is composite.

Example 6.12
If $a = 2$, then

$$2^n \not\equiv 2 \mod n \Rightarrow n = 2 \text{ is composite}$$

Question. We might wonder whether a converse to this holds. Disappointingly, no.

Example 6.13

$2^{10} = 1024 = 1 \pmod{341}$, so $2^{341} = (2^{10})^3 4 \cdot 2 = 2 \mod 341$.

But $341 = 11 \cdot 31$, so 341 is composite.

Definition 6.14 (Pseudoprime)

We call n a pseudoprime to the base a if n is composite and happens to satisfy

$$a^n \equiv a \mod n.$$

Example 6.15

341 is a pseudoprime to the base 2.

We might hope that if this test failed for a particular a, there exists some other a that can test whether n is composite. However, this is not the case.[8]

It is not true that given a composite n, there exists an $a \in \mathbb{Z}_+$ such that n is not a pseudoprime to the base a.

Definition 6.16 (Carmichael Numers)

$n \in \mathbb{Z}_+$ is called a Carmichael number if n is composite and

$$a^n \equiv a \mod n, \quad \forall a \in \mathbb{Z}$$

Example 6.17

The smallest Carmichael number is 561.

Question. There are variants on this question? Can you have pseudoprimes that satisfy all but one base?

Proposition 6.18

If a composite number n is *not* a Carmichael number, then at least half of the congruence classes $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ are such that n is *not* a pseudoprime to the base a.

Proof. Suppose n is a pseudoprime to the base:

$$a_1, a_2, \ldots, a_r \in (\mathbb{Z}/n\mathbb{Z})^\times$$

[8] We learn in life to not be too hopeful.

and suppose we have some a such that

$$a^n \not\equiv a \mod n$$

Then for all i,

$$\begin{aligned}(a \cdot a_i)^{n-1} &= a^{n-1}a_i^{n-1} \\ &\equiv a^{n-1} \mod n \\ &\not\equiv 1 \mod n\end{aligned}$$

Thus n is not a pseudoprime to the bases $a \cdot a_1, a \cdot a_2, \ldots, a \cdot a_r$. □

Remark 6.19. The bases for pseudoprimes form a subgroup of the group of units.

Someone check me on this.

§7 March 1, 2022

§7.1 Power Residues

For this section, corresponds to pages 45-46 of Ireland & Rosen [**?**] are a good reference.

Definition 7.1 (Power Residue)

If $m, n \in \mathbb{Z}_+$ and $a \in \mathbb{Z}$ such that $(a, m) = 1$, then we say that a is an n^{th} power residue modulo m if and only if the congruence

$$x^n \equiv a \mod m \tag{7.1}$$

has solutions.

Given eq. (7.1), we're interested in two questions:

1) Does eq. (7.1) have a solution?

2) If yes, then how many?

Proposition 7.2

If $m \in \mathbb{Z}_+$ is such that $U(m)$ is cyclic, and $a \in \mathbb{Z}$ is such that $(a, m) = 1$, then

$$x^n \equiv a \mod m$$

has solutions if and only if

$$a^{\phi(m)/d} \equiv 1 \mod m$$

where $d = (\phi(m), n)$.

If there are solutions, then there are exactly d solutions.

Proof. Let g be a primitive root mod m, and let

$$a = g^b.$$

Suppose $x = g^y$. Then

$$\begin{aligned} x^n &\equiv a \mod m \\ \iff g^{ny} &\equiv g^b \mod m \\ \iff ny &\equiv b \mod \phi(m) \end{aligned}$$

This is solvable if and only if $d = (\phi(m), n) \mid b$. If there is at least one solution, then there are exactly d solutions.

Now we show that $d \mid b \Leftrightarrow a^{\phi(m)/d} \equiv 1 \mod m$.

Forward direction:

$$a^{\phi(m)/d} = g^{b \cdot \phi(m)/d} = \left(g^{\phi(m)}\right)^{b/d} = 1 \mod m$$

Backward direction:

$$a^{\phi(m)/d} \equiv 1 \mod m \Rightarrow g^{b \cdot \phi(m)/d} \equiv 1 \mod m \Rightarrow \phi(m) \mid b \cdot \phi(m)/d \Rightarrow \frac{b}{d} \in \mathbb{Z}$$

□

We can prove this using a similar group theory theorem that we can apply directly.

Theorem 7.3

Let G be a cyclic group of order n, suppose $k \in \mathbb{Z}_+$ and $a \in G$. Then $a = b^k$ (a is a k^{th} power in G) iff $a^{n/(k,n)} = e$ iff $x^k = a$ has (n, k) solutions in G.

The proof of this theorem uses the following lemma:

Lemma 7.4

Let G be a cyclic group of order n and let H be a subgroup of G of order d. Then $x \in H$ iff $x^d = e$ iff $\text{ord}(x) \mid d$.

Proof of theorem 7.3. Let H be a subgroup of k^{th} powers in G[9], and let $g \in G$ be such that $G = \langle g \rangle$.

Then $H = \{g^{jk} \mid j \in \mathbb{Z}\} = \langle g^k \rangle$. Since $\text{ord}(g^k) = \frac{n}{(k,n)}$ (*exercise*), we that $|H| - \frac{n}{(k,n)}$.

Consider $\phi : G \to G$ that powers by k, $\phi : x \mapsto x^k$. Then $\text{im}(\phi) = H$, so this implies that ϕ is a (k,n)-to-1 mapping (so gives us the number of solutions to each power, and how many k powers there are). □

Knowing how to solve these modulo a group of units gives us ways using CRT/Sunzi's Theorem to solve mod composite numbers.

We write $m = 2^e p_1^{e_1} \cdots p_r^{e_r}$ where p_i are pairwise distinct odd primes. Then

$$x^n \equiv a \mod m, \quad (a,m) = 1$$

is solvable if and only if the system

$$\begin{aligned} x^n &\equiv a \mod 2^e \\ x^n &\equiv a \mod p_i^{e_i} \\ &\vdots \\ x^n &\equiv a \mod p_r^{e_r} \end{aligned}$$

is solvable.

We have that $U(p_i^{e_i}), U(2), U(4)$ are all cyclic. Hence our prior discussion can be applied to those.

Question. How do we solve

$$x^n \equiv a \mod m$$

where $e \geq 3$ (for powers of 2)?

Proposition 7.5 (4.2.2 from Text)

Let $a \in \mathbb{Z}$ be odd, $e \geq 3$, and consider $x^n \equiv a \mod 2^e$.

If n is odd, then a solution exists and is unique. If n is even, a solution exists if and only if $a \equiv 1 \mod 4$ and $a^{2^{e-2}/d} \equiv 1 \mod 2^e$ where $d = (n, 2^{e-2})$. When a solution exists, there are exactly $2d$ solutions.

Proof. Exercise to come. □

[9] This is indeed a subgroup. We use the fact that G is Abelian.

§7.2 Quadratic Residues

Things are a lot simpler and nicer when we consider only quadratic congruences (as opposed to arbitrary residues).

Definition 7.6 (Quadratic Residue)
Let $a \in \mathbb{Z}$, $m \in \mathbb{Z}_+$, $(a, m) = 1$. We say that a is a quadratic residue mod m if the congruence

$$x^2 \equiv a \mod m \tag{7.2}$$

has a solution.

Conversely, if a is not a quadratic residue (that is, eq. (7.2) does not have a solution), we call it a nonresidue or a quadratic nonresidue.

We extract the consequences of previous propositions to get special cases of propositions 4.2.3 and 4.2.4 from text.

1) Let $p \in \mathbb{Z}_+$ be an odd prime, and suppose $a \in \mathbb{Z}$ with $p \nmid a$. Then

$$x^2 \equiv a \mod p$$

is solvable iff

$$x^2 \equiv a \mod p^e$$

is solvable for all $e \geq 1$.

2) Let $a \in \mathbb{Z}$ be odd. Then

$$x^2 \equiv a \mod 8$$

is solvable iff

$$x^2 \equiv a \mod 2^e$$

is solvable for all $e \geq 3$.

Proposition 7.7 (5.1.1 from Text)
Let

$$m = 2^e p_1^{e_1} \cdots p_r^{e_r}$$

be the prime factorization of $m \in \mathbb{Z}_+$, and suppose $(a, m) = 1$.

Then

$$x^2 \equiv a \mod m \tag{7.3}$$

is solvable if and only if three conditions are satisfied:

i. If $e = 2$, then $a \equiv 1 \mod 4$.

ii. If $e \geq 3$, then $a \equiv 1 \mod 8$.

iii. For each i, have

$$a^{(p_i-1)/2} \equiv 1 \mod p_i$$

Proof. Sunzi's theorem tells us that eq. (7.3) is solvable iff

$$\begin{aligned} x^2 &\equiv x \mod 2^e \\ x^2 &\equiv a \mod p_1^{e_1} \\ &\vdots \\ x^2 &\equiv a \mod p_r^{e_r} \end{aligned}$$

are *all* solvable.

First consider the first equation $x^2 \equiv 1 \mod 2^e$. 1 is the only quadratic residue mod 4 and the same thing is true mod 8. On the other hand, black box 2 gives us $x^2 \equiv a \mod 8$ is solvable iff $x^2 \equiv a \mod 2^e$ for $e \geq 3$. This gives us conditions i and ii.

Now consider $x^2 \equiv a \mod p_i^{e_i}$. Proposition 7.2 gives that $x^2 \equiv a \mod p_i$ is solvable iff $a^{(p_i-1)/2} \equiv 1 \mod p_i$. Black box 1 then tells us that

$$\begin{aligned} & x^2 \equiv a \mod p_i \quad \text{is solvable} \\ \iff \quad & x^2 \equiv a \mod p_i^{e_i} \quad \text{is solvable.} \end{aligned}$$

which concludes our proof. □

Remark. Studying these quadratic congruences amounts to studying them modulo primes.

§7.3 The Legendre Symbol

Definition 7.8 (The Legendre Symbol)
Let p be an odd prime, and let $a \in \mathbb{Z}$.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ 0 & \text{if } p \mid a \\ -1 & \text{otherwise} \end{cases}$$

This symbol $\left(\frac{a}{p}\right)$ is called the Legendre symbol.

Proposition 7.9 (5.1.2 of Text)
We have the following properties of the Legendre symbol:

(a)
$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \mod p$$
This is called *Euler's Criterion*.

(b)
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$
which is to say that the Legendre symbol is totally multiplicative.

(c) If $a \equiv b \mod p$, then
$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

§8 March 3, 2022

§8.1 Quadratic Residues *continued*

Recall: definition 7.8 and proposition 7.9 from last class (right above).

We now prove the earlier proposition:

Proof of proposition 7.9.

(c) is clear.

(a) By Fermat's Little Theorem, if $p \nmid a$, we have $a^{p-1} \equiv 1 \mod p$, so

$$(a^{(p-1)/2}+1)(a^{(p-1)/2}-1) \equiv 0 \mod p$$

Since mod p we have an integral domain, then we have that $a^{(p-1)/2} \equiv \pm 1 \mod p$. We know that $a^{(p-1)/2} \equiv 1 \mod p$ if and only if a is a quadratic residue mod p,

(b) This applies (a).

$$\left(\frac{ab}{p}\right) = (ab)^{(p-1)/2} = a^{(p-1)/2} \cdot b^{(p-1)/2} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

□

Corollary 8.1

We have some corollaries:

1) There are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues mod p.

2) The product of two residues is a residue, the product of a residue and a non-residue is a non-residue, and the product of a non-residue and a non-residue is a residue.

3) If g is a primitive root modulo p, then

$$\left(\frac{g^i}{p}\right) = (-1)^i.$$

4) We have

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

which has a fancy name. This is the *"First Supplemental Law of Quadratic Reciprocity"*.

§8.2 Gauss's Lemma

We now discuss a characterization of the Legendre symbol due to Gauss.

Definition 8.2

For $p \in \mathbb{Z}_+$ an odd prime,

$$S = \left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 1, 2, \ldots, \frac{p-1}{2}\right\}$$

is called the set of least residues mod p.

Definition 8.3

Let $a \in \mathbb{Z}$ such that $p \nmid a$. Define μ to be the number of negative least residues of the integers

$$a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right) a$$

Example 8.4

If $p = 7$ and $a = 4$, then $\frac{p-1}{2} = 3$, and $1 \cdot 4, 2 \cdot 4, 3 \cdot 4$ are congruent to $-3, 1, -2 \bmod 7$. Thus $\mu = 2$.

Lemma 8.5 (Gauss's Lemma)

Let $p \in \mathbb{Z}_+$ be an odd prime and let $a \in \mathbb{Z}$ be such that $p \nmid a$. Then

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

Proof. It is convenient for us to partition the list S as

$$P = \{1, 2, \cdots, \frac{p-1}{2}\}$$
$$N = \{-1, -2, \cdots, -\frac{p-1}{2}\}$$

so that $\mu = |aP \cap N|$[10].

A key observation is that if $x, y \in P$ with $x \neq y$, then

$$ax \not\equiv \pm ay \mod p$$

for otherwise,

$$a \equiv \pm y \mod p$$

which is impossible since x and y are distinct elements of P (positive residue classes, so not in N).

Thus $aP = \{\varepsilon_i i \mid 1 \leq u \leq \frac{p-1}{2}\}$ for some $\varepsilon_i = \pm 1$.

Now we mimic the elementary proof of Euler's Theorem:

$$a^{(p-1)/2} \cdot \left(\frac{p-1}{2}\right)! \equiv \left(\prod_{i=1}^{(p-1)/2} \varepsilon_i\right) \cdot \left(\frac{p-1}{2}\right)!$$
$$a^{(p-1)/2} \equiv \left(\prod_{i=1}^{(p-1)/2} \varepsilon_i\right)$$
$$\equiv (-1)^{\mu}$$

[10] There's an abuse of notation here, but we conflate integers with their equivalence classes in S.

since μ is equal to the order of the set that is contributing every -1 as ε_i.

Applying proposition 7.9 (Euler's criterion), this concludes the proof. □

We'll use this lemma to prove Quadratic Reciprocity later.

We now use it to prove the *Second Supplemental Law* of Quadratic Reciprocity.

Proposition 8.6 (5.1.3, the *Second Supplemental Law of Quadratic Reciprocity*)
For $p \in \mathbb{Z}_+$ be an odd prime.

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

We note $\dfrac{p^2-1}{8} = \dfrac{(p-1)(p+1)}{2 \cdot 4}$. From this, it follows that we're really saying

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{when } p = \pm 1 \mod 8 \\ -1 & \text{when } p = \pm 3 \mod 8 \end{cases}$$

Proof. We apply Gauss's Lemma with $a = 2$.

$$2P = \{2, 4, 6, \ldots, p-1\}$$

First suppose that $p \equiv 1 \mod 4$. Then $\frac{p-1}{2}$ is even, so

$$2P = \left\{ \underbrace{2, 4, 6, \ldots, \frac{p-1}{2}}_{\in P}, \underbrace{\frac{p+3}{2}, \ldots, p-1}_{\in N} \right\}$$

with the first $\frac{p-1}{4}$ elements in P and the last $\frac{p-1}{4}$ elements in N. So $\mu = |2P \cap N| = \frac{p-1}{4}$, so Gauss's Lemma gives

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}} = \left((-1)^{\frac{p-1}{4}}\right)^{\frac{p+1}{2}} = (-1)^{\frac{p^2-1}{8}}$$

since $\frac{p+1}{2}$ is odd.

Now suppose $p \equiv 3 \mod 4$. Then

$$2P = \left\{ \underbrace{2, 4, 6, \ldots, \frac{p-3}{2}}_{\in P}, \underbrace{\frac{p+1}{2}, \ldots, p-1}_{\in N} \right\}$$

The first $\frac{p-3}{4}$ elements are in P, and the last $\frac{p+1}{4}$ elements are in N. Then $\mu = \frac{p+1}{4}$, so

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}} = \left((-1)^{\frac{p+1}{4}}\right)^{\frac{p-1}{2}} = (-1)^{\frac{p^2-1}{8}}$$

□

§8.3 Quadratic Reciprocity

Theorem 8.7 (Law of Quadratic Reciprocity)
Let $p, q \in \mathbb{Z}_+$ be distinct odd positive primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

In other words,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

if and only if at least one of p, q is congruent to 1 mod 4.

Proof. coming soon! □

Here's the motivation behind this: we used Euler's Criterion to easily calculate the quadratic character of some a mod p. With Quadratic Reciprocity, we can solve the question "If we fix odd prime q, for which p is q a quadratic residue?"

Example 8.8
Which odd primes $p \in \mathbb{Z}_+$ have 3 as a quadratic residue?

Suppose $p \equiv 1 \mod 4$. Then

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 3 \\ -1 & \text{if } p \equiv -1 \mod 3 \end{cases}$$

Then $p \equiv 1 \mod 4$ and $p \equiv 1 \mod 3$ so $p \equiv 1 \mod 12$ gives us $\left(\frac{3}{p}\right) = 1$ and $p \equiv 5 \mod 12$ gives $\left(\frac{3}{p}\right) = -1$. ***(Format)

Now suppose $p \equiv 3 \mod 4$. Then

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv -1 \mod 3 \\ -1 & \text{if } p \equiv 1 \mod 3 \end{cases}$$

Thus,

$$p \equiv 11 \mod 12 \text{ gives } \left(\frac{3}{p}\right) = 1, \text{ and}$$
$$p \equiv 7 \mod 12 \text{ gives } \left(\frac{3}{p}\right) = -1$$

So we conclude that $\left(\frac{3}{p}\right) = 1$ iff $p \equiv \pm 1 \mod 12$.

§9 March 8, 2022

§9.1 Legendre Symbol *continued*

Example 9.1

Determine if 219 is a quadratic residue mod 383 (we note that 383 is a prime).

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right) \cdot \left(\frac{73}{383}\right)$$

We now flip the Legendre Symbols using quadratic reciprocity:

$$\begin{aligned} &= -\left(\frac{383}{3}\right) \cdot \left(\frac{383}{73}\right) \\ &= -\left(\frac{2}{3}\right) \cdot \left(\frac{18}{73}\right) \\ &= 1 \cdot \left(\frac{18}{73}\right) \\ &= \left(\frac{2}{73}\right) \cdot \left(\frac{9}{73}\right) \\ &= \left(\frac{2}{73}\right) = \boxed{1} \end{aligned}$$

Remark. We must factor the top argument before beginning to flip using quadratic reciprocity.

§9.2 Proof of Quadratic Reciprocity

Recall theorem 8.7:

Theorem (Law of Quadratic Reciprocity)
Let $p, q \in \mathbb{Z}_+$ be distinct odd positive primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

In other words,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

if and only if at least one of p, q is congruent to 1 mod 4.

Proof of Quadratic Reciprocity (theorem 8.7), using Gauss's Lemma (lemma 8.5). WLOG, let

$$P = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}, \quad N = -P,$$
$$Q = \left\{1, 2, \ldots, \frac{q-1}{2}\right\}$$

We write $\tilde{P}, \tilde{N}$ for $P \pmod p$ and $N \pmod p$ respectively, so that Gauss's lemma gives

$$\left(\frac{q}{p}\right) = (-1)^{\mu}, \quad \text{where } \mu = |q\tilde{P} \cap \tilde{N}|$$

In other words, μ is exactly the number of $x \in P$ such that $qx \equiv n \pmod p$ for some $n \in N$, and hence the number of $x \in P$ such that for $y \in \mathbb{Z}$,

$$-\frac{p}{2} < qx - py < 0.$$

We now specify more precisely which y can possibly satisfy this condition. Solving these inequalities for y gives

$$\frac{qx}{p} < y < \frac{qx}{p} + \frac{1}{2}.$$

OTOH, since $x \leq \frac{p-1}{2}\ \forall x \in P$, this gives

$$\begin{aligned} y < \frac{qx}{p} + \frac{1}{2} &\leq \frac{q(p-1)}{2p} + \frac{1}{2} \\ &< \frac{q+1}{2}. \end{aligned}$$

Thus $0 < y < \frac{q+1}{2}$, which means that

$$y \in Q = \left\{1, 2, \ldots, \frac{q-1}{2}\right\}.$$

We've shown that μ is the number of points $(x, y) \in P \times Q$ such that

$$\frac{p}{2} < qx - py < 0.$$

Switching p and q, we also have

$$\left(\frac{p}{q}\right) = (-1)^{\eta}$$

where η is the number of pairs

$$(y, x) \in Q \times P$$

such that

$$-\frac{q}{2} < py - qx < 0$$

which is exactly the number of pairs

$$(x, y) \in P \times Q$$

satisfying

$$0 < qx - py < \frac{q}{2}$$

(reflecting the inequality over 0).

We note that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu}(-1)^{\eta} = (-1)^{\mu+\eta}$$

so all that remains is counting μ and η. And we have that $\mu + \eta$ is the number of ordered pairs $(x, y) \in P \times Q$ such that either

$$-\frac{p}{2} < qx - py < 0 \text{ or } 0 < qx - py < \frac{q}{2}$$

Noting that $qx - py \neq 0$ since x and y are from P and Q respectively, hence we can reduce this to

$$-\frac{p}{2} < qx - py < \frac{q}{2}.$$

Graphically, we are looking at: ***(Picture!)

where $\mu + \eta$ is the number of lattice points in the shaded region.

If α is the number of lattice points in A and β the number of lattice points in B. Then

$$\mu + \eta = \frac{p-1}{2}\frac{q-1}{2} - (\alpha + \beta)$$

We show that $\alpha = \beta$ so that $\alpha + \beta \equiv 0 \pmod 2$.

Let ρ be the rotation given by rotating the rectangle about its center leaves it invariant.

$$\rho(x, y) = \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right)$$

Quick check that

$$qx - py < \frac{-p}{2} \Leftrightarrow qx' - py' > \frac{q}{2}$$

Since ρ maps lattice points to lattice points, then $\alpha = \beta$ which concludes the proof with a little extra handiwork. □

§9.3 Jacobi Symbol

The Jacobi symbol generalizes the Legendre symbol.

Definition 9.2 (Jacobi Symbol)

Let b be an odd positive integer and let $a \in \mathbb{Z}$. Write $b = p_1 p_2 \cdots p_m$, where p_i are (not necessarily distinct) primes. Then we write

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_m}\right)$$

is called the Jacobi symbol.

We note some basic properties that the Jacobi symbol is totally multiplicative (on top and bottom!):

$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$$
$$\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$$

Remark. Note that they're multiplicative *fixing* either top or bottom. That is, they don't multiply like fractions.

Warning! $\left(\frac{a}{b}\right) = 1$ does not imply that a is a quadratic residue modulo b (since we could have -1's from the factorization cancel out).

However, $\left(\frac{a}{b}\right) = -1$ *does* imply that a is a non-residue modulo b. (it is a non-residue mod at least one of prime factors of b).

Example 9.3

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$$

but 2 is not a quadratic residue modulo 15.

Proposition 9.4 (5.2.2 of Text)
We have the following properties about the Jacobi symbol:

(a)
$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$$

(b)
$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$$

(c) If $a, b \in \mathbb{Z}_+$, then
$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$$

§10 March 10, 2022

§10.1 Jacobi Symbol *continued*

Recall:

Definition (Jacobi Symbol)
Let $b \in \mathbb{Z}_+$ be odd, and let $a \in \mathbb{Z}$. We write $b = p - 1p_2 \cdots p_m$, where p_i are primes (not necessarily distinct). Then we have
$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_m}\right)$$
is called the Jacobi symbol.

This generalizes the Legendre symbol. We have basic properties that
$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$$
$$\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$$

We noted that $\left(\frac{a}{b}\right) = -1$ implies that a is *not* a quadratic residue mod b but $\left(\frac{a}{b}\right) = 1$ does not imply a is a quadratic residue mod b.

We also stated analogues of the reciprocity laws for the Legendre symbol.

Lemma 10.1

Let $r, s \in \mathbb{Z}_+$ be odd. Then

(a) $\dfrac{rs-1}{2} \equiv \dfrac{r-1}{2} + \dfrac{s-1}{2} \mod 2.$

(b) $\dfrac{r^2s^2-1}{8} \equiv \dfrac{r^2-1}{8} + \dfrac{s^2-1}{8} \mod 2.$

Proof.

(a) $(r-1)(s-1) \equiv 0 \mod 4$. Hence

$$\begin{aligned} rs-1 &\equiv (r-1)(s-1) + r + s - 2 \mod 4 \\ &\equiv r + s - 2 \mod 4 \\ &\equiv (r-1) + (s-1) \mod 4 \\ &\equiv \frac{r-1}{2} + \frac{s-1}{2} \mod 2 \end{aligned}$$

which gives (a).

(b) We follow the same procedure, more or less. $(r^2-1)(s^2-1) \equiv 0 \mod 16$, so

$$\begin{aligned} r^2s^2-1 &\equiv (r^2-1)(s^2-1) + r^2 + s^2 - 2 \mod 16 \\ &\equiv (r^2-1) + (s^2-1) \mod 16 \\ &\equiv \frac{r^2-1}{8} + \frac{s^2-1}{8} \mod 2 \end{aligned}$$

which gives (b).

□

Corollary 10.2

let $r_1, r_2, \ldots, r_m \in \mathbb{Z}_+$ be odd. Then

(a) $\displaystyle\sum_{i=1}^{m} \frac{r_i - 1}{2} \equiv \frac{r_1 r_2 \cdots r_m - 1}{2} \mod 2.$

(b) $\displaystyle\sum_{i=1}^{m} \frac{r_i^2 - 1}{2} \equiv \frac{r_1^2 r_2^2 \cdots r_m^2 - 1}{8} \mod 2.$

Proof. By induction on m from lemma 10.1. □

We restate the reciprocity laws but for Jacobi symbols, proposition 9.4:

Proposition (5.2.2 of Text)

We have the following properties about the Jacobi symbol:

(a)
$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$$

(b)
$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$$

(c) If $a, b \in \mathbb{Z}_+$, then
$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$$

Proof of proposition 9.4.

(a) + (b) are immediate from the corollary (factor b, sum exponents and take the parity of the exponent) and the supplemental laws of quadratic reciprocity.

(c) Let
$$\begin{aligned} a &= q_1 q_2 \cdots q_l \\ b &= p_1 p_2 \cdots p_m. \end{aligned}$$

Then
$$\begin{aligned} \left(\frac{a}{b}\right)\left(\frac{b}{a}\right) &= \prod_i \prod_j \left(\frac{q_i}{p_j}\right)\left(\frac{p_i}{q_j}\right) \\ &= (-1)^{\sum_i \sum_j \left(\frac{q_i-1}{2}\right)\left(\frac{p_j-1}{2}\right)} \end{aligned}$$

Applying the corollary,
$$\begin{aligned} &= (-1)^{\left(\sum_i \frac{q_i-1}{2}\right)\left(\sum_j \frac{p_j-1}{2}\right)} \\ &= (-1)^{\left(\frac{(\sum_i q_i)-1}{2}\right)\left(\frac{(\sum_j p_j)-1}{2}\right)} \\ &= (-1)^{\left(\frac{a-1}{2}\right)\left(\frac{b-1}{2}\right)} \end{aligned}$$

which is as desired!

□

Example 10.3

We try to compute with the Jacobi symbol. Recall example 9.1

$$\left(\frac{219}{383}\right)$$

where we repeatedly factored and flipped. With a Jacobi symbol, we don't need to start with factoring; we can forego factorization of top argument and simply repeatedly flip:

$$\begin{aligned}\left(\frac{219}{383}\right) &= -\left(\frac{383}{219}\right) = -\left(\frac{164}{219}\right) = -\left(\frac{4}{219}\right)\left(\frac{41}{219}\right) = -\left(\frac{41}{219}\right)\\ &= -\left(\frac{219}{41}\right) = -\left(\frac{14}{41}\right) = -\left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = -\left(\frac{7}{41}\right)\\ &= -\left(\frac{41}{7}\right) = -\left(\frac{-1}{7}\right) = \boxed{1}.\end{aligned}$$

What we did here is to exploit the fact that *all* Legendre symbols agree with Jacobi symbols, we treat it as a Jacobi symbol and do 'Jacobi-*like*' manipulations on it.

This marks the dividing line between the first half and latter half of the course! Everything up to this point is fair game on the midterm. We also now switch to Stewart and Tall.

§10.2 Number Fields

Definition 10.4 (Algebraic Numbers)
A complex number x is called algebraic if it is algebraic over $\mathbb{Q}$, i.e., if it satisfies a nonzero polynomial equation over $\mathbb{Q}$.

We denote the set of algebraic numbers over $\mathbb{Q}$ as $\overline{\mathbb{Q}}$.

Proposition 10.5
The set $\overline{\mathbb{Q}}$ of algebraic numbers is a subfield of $\mathbb{C}$. That is, addition and multiplication is closed, and we have inverses for nonzero elements.

Proof. The key point is that if L/K is a field extension, then $\alpha \in L$ is algebraic over K iff $K(\alpha)/K$ is finite.

So suppose $\alpha, \beta \in \overline{\mathbb{Q}}$. Then $\mathbb{Q}(\alpha)/\mathbb{Q}$ and $\mathbb{Q}(\beta)/\mathbb{Q}$ are finite. Thus $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ is finite (and all pieces of the associated diamond are finite extensions as well).

***(Diamond diagram)

Since $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ and for $\beta \neq 0$, $\alpha/\beta \in \mathbb{Q}(\alpha, \beta)$. This means that all of these elements are algebraic over $\mathbb{Q}$. □

Definition 10.6
A number field is a subfield K of $\mathbb{C}$ such that $[K : \mathbb{Q}] < \infty$.

Thus every element of a number field is algebraic, so $K \subseteq \overline{Q}$.

By the definition of a finite extension, every number field has the form

$$K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_N) \text{ for some } \alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$$

However, something stronger than this holds.

Theorem 10.7 (Primitive Element Theorem)
If K is a number field, then $K = \mathbb{Q}(\theta)$ for some $\theta \in \overline{\mathbb{Q}}$.

Proof sketch. It is enough to show that if

$$K = K_1(\alpha, \beta),$$

then $K = K_1(\theta)$ for some $\theta \in \overline{\mathbb{Q}}$.

Suppose the minimum polynomials (over $\mathbb{Q}$) of α and β respectively are (factored over roots in $\mathbb{C}$):

$$\begin{aligned}(t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_n) \qquad & \alpha_1 = \alpha \\ (t-\beta_1)(t-\beta_2)\cdots(t-\beta_n) \qquad & \beta_1 = \beta\end{aligned}$$

These polynomials are separable. Hence for each i and each $k \neq 1$, there exists at most one $x \in K_1$ such that

$$\alpha_i + x\beta_k = \alpha_1 + x\beta_1.$$

(This only holds for more x when you have β_k and β_1 colliding). There are only finitely many of these equations, so we can choose a nonzero $c \in K_1$ such that

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1$$

for any $1 \leq i \leq n$ and $2 \leq k \leq m$.

Define $\theta = \alpha + c\beta$. We claim that

$$K_1(\alpha, \beta) = K_1(\theta)$$

for which the proof is on page 39 of Stewart Tall. □

§11 March 15, 2022

§11.1 Number Fields *continued*

Recall: from last class...

Definition

A complex number α is called algebraic if it is algebraic over $\mathbb{Q}$.

Proposition

The set $\overline{\mathbb{Q}}$ of algebraic numbers is a subfield of $\mathbb{C}$.

Definition

A number field is a subfield K of $\mathbb{C}$ such that $[K : \mathbb{Q}] < \infty$.

Theorem (Primitive Element Theorem)
If K is a number field, then $K = \mathbb{Q}(\theta)$ for some $\theta \in \overline{\mathbb{Q}}$.

Crux of proof. Suppose $K = K_1(\alpha, \beta)$. Thus $K = K_1(\theta)$ for some θ that is easily found as a function of α and β.

Write the minimum polynomials of α, β over K_1(factored over $\mathbb{C}$)

$$(t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_n) \quad \alpha_i \in \overline{\mathbb{Q}}, \text{ and } \alpha =: \alpha_1$$
$$(t-\beta_1)(t-\beta_2)\cdots(t-\beta_m) \quad \beta_i \in \overline{\mathbb{Q}}, \text{ and } \beta =: \beta_1$$

These are separable. Hence for each i and each $k \neq 1$, there exists at most one $x \in K$ such that

$$\alpha_i + x\beta_k = \alpha_1 + x\beta_1$$

Hence, since there are only finitely many of these equations, we can choose $0 \pm c \in K$, such that

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1$$

for any $1 \leq i \leq n$ and $2 \leq k \leq m$. We define $\theta = \alpha + c\beta$. We claim $K = K_1(\theta)$. □

The proof up to this claim is actually useful in finding a primitive element.

Example 11.1 (p.39 [?])
Let $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$.

$$\alpha_1 = \sqrt{2}, \beta_1 = \sqrt[3]{5}$$

We then have $\alpha_2 = -\sqrt{2}$ and we can let $\beta_2 = \zeta_3\sqrt[3]{5}, \beta_2 = \zeta_3^2\sqrt[3]{5}$ where ζ_3 is the primitive 3rd root of unity.

$c = 1$ has the property that

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1$$

for $1 \leq i \leq 2$ and $2 \leq k \leq 3$.

Therefore, we can conclude that $\sqrt{2} + \sqrt[3]{5}$ is a primitive element for $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})/\mathbb{Q}$.

§11.2 Conjugates of Algebraic Numbers

Theorem 11.2 (p.40 [?])
Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. Then there exists exactly n distinct field embedding of K into $\mathbb{C}$. (We label these $\sigma_i : K \hookrightarrow \mathbb{C}, 1 \leq i \leq n$.)

The $\sigma_i(\theta) =: \theta_i$ are the zeros in $\mathbb{C}$ of the minimal polynomial of θ over $\mathbb{Q}$.

Proof. Suppose $\sigma : K \hookrightarrow \mathbb{C}$ is an embedding. We have that σ is the identity on $\mathbb{Q}$ (since $\sigma(1) = 1$), so

$$0 = \sigma(f(\theta)) = f(\sigma(\theta)) \qquad \text{where } f := \mathsf{minpoly}_{\mathbb{Q}}(\theta).$$

Hence $\sigma(\theta)$ is a root of f.

Conversely, for each root θ_i of f, there is a field isomorphism[11] taking

$$\mathbb{Q}(\theta) \xrightarrow{\sigma_i} \mathbb{Q}(\theta_i)$$

such that $\sigma_i(\theta) = \theta_i$. Therefore we've shown a bijection between the roots of f and the embeddings of K into $\mathbb{C}$. □

§11.3 Discriminants of Bases, Vandermonde Determinant

Let $K = \mathbb{Q}(\theta)$ be a number field of degree n, and let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a basis of K as a vector space over $\mathbb{Q}$. Let $\sigma_i : K \hookrightarrow \mathbb{C}$, $1 \leq i \leq n$ be the embeddings of K into $\mathbb{C}$.

Definition 11.3

The discriminant of $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is

$$\begin{aligned}\Delta[\alpha_1, \alpha_2, \ldots, \alpha_n] &= \det\left(\sigma_i(\alpha_j)\right)^2 \\ &= \det \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}^2\end{aligned}$$

If $\{\beta_1, \ldots, \beta_n\}$ is another basis, then $\forall 1 \leq k \leq n$,

$$\beta_k = \sigma_{i=1}^n C_{ik}\alpha_i, \quad C_{ik} \in \mathbb{Q},$$

where $\det(C_{ik}) \neq 0$. Then it is a fact that

$$\Delta[\beta_1, \ldots, \beta_n] = (\det(C_{ik}))^2 \cdot \Delta[\alpha_1, \ldots, \alpha_n]$$

Theorem 11.4 (p.42 [?])

The discriminant of any basis for $K = \mathbb{Q}(\theta)$ is rational and nonzero.

Proof. It suffices to show that this holds for $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ by the above fact.

[11] We find isomorphisms $\mathbb{Q}(\theta) \xrightarrow{\sim} \mathbb{Q}[x]/f$ and similarly $\mathbb{Q}(\theta_i) \xrightarrow{\sim} \mathbb{Q}[x]/f$ where $f := \mathsf{minpoly}_{\mathbb{Q}}(\theta) = \mathsf{minpoly}_{\mathbb{Q}}(\theta_i)$.

Write $\theta = \theta_1$, $\theta_1, \theta_2, \ldots, \theta_n$ for the conjugates of θ_1. Then

$$\Delta[1, \theta, \theta^2, \ldots, \theta^{n-1}] = \left(\det(\theta_i^j)\right)^2$$

We use a general observation

Definition 11.5 (Vandermonde Matrix)
A (square) Vandermonde matrix is a matrix of the form

$$V = \begin{pmatrix} 1 & t_1 & t_1^2 & \ldots & t_1^{n-1} \\ 1 & t_2 & t_2^2 & \ldots & t_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & t_n & t_n^2 & \ldots & t_n^{n-1} \end{pmatrix}$$

Claim 11.6 — The determinant of V is

$$\prod_{1 \le i < j \le n} (t_i - t_j).$$

Going back to the proof of our claim about discriminants, we can take $t_i = \theta_i := \sigma_i(\theta)$ to get

$$\begin{aligned} \Delta[1, \theta, \ldots, \theta^{n-1}] &= \prod_{i<j} (\theta_i - \theta_j)^2 \\ &= \mathsf{disc}(\mathsf{minpoly}_{\mathbb{Q}}(\theta)) \end{aligned}$$

□

§12 March 17, 2022

§12.1 Midterm Review

General Advice

- 5-7pm. Location: Barus & Holley 168.
- There are 5 problems:
  - Each are weighted equally, some have multiple sections in them.
  - There is a bonus problem for a *token* number of points.
- Think about problems before starting! Don't begin immediately.

Key Topics

1) Unique factorization in $\mathbb{Z}$ (theorem 1.6). Key points:

   - Existence (using well-ordering of $\mathbb{Z}_+$)
   - Uniqueness (using prime elements being irreducible elements in $\mathbb{Z}$)

2) $\mathbb{Z}$ is a Euclidean domain with Euclidean function abs (absolute value) (corollary 1.8).

   - Argument uses well-ordering of $\mathbb{Z}_+$ applied to the set $S = \{a - bq \mid b \in \mathbb{Z}\}$ when trying to divide a by b.
   - Repeated application of this property yields the Euclidean algorithm for finding gcd's.

3) Bezout's Identity (*not* Bezout's Theorem)

   If $a, b \in \mathbb{Z}$ are integers (not both 0) and $c \in \mathbb{Z}$, then there exists $x, y \in \mathbb{Z}$ such that

   $$ax + by = c$$

   if and only if $\gcd(a, b) \mid c$.

   - We take set $S = \{ax + by \mid x, y \in \mathbb{Z}\}$ and use well-ordering to show that the smallest element has to be c.

4) From Bezout to solving linear congruences in 1 variable, the linear congruence

   $$ax \equiv b \pmod{m}$$

   is equivalent to

   $$ax - my = b$$

   for some $y \in \mathbb{Z}$. Applying Bezout's tells us that this equation is solvable if and only if $\gcd(a, b) \mid b$. When a solution exists, there are d solutions modulo m.

   - Showing there are d solutions: you divide a, b, m by $\gcd(a, m)$, then you have a modulus $\frac{m}{\gcd(a,m)}$ where we have a unique solution. We lift up to solutions modulo m.

5) Sunzi's theorem (theorem 4.2). For $m, n \in \mathbb{Z}_+$ with $(m, n) = 1$. And $a, b \in \mathbb{Z}$, then the simultaneous congruences

   $$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

   have a *unique* solution modulo mn.

   - We have $\pi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ be the natural projectsion where $\ker(\pi) = \{0\}$ since $(m, n) = 1$.

6) Structure of group of units (corollary 5.4). $U(m)$ is cyclic $\iff$ $m = 1, 2, 4, p^e, 2p^e$.

Practice Problems

Problem 12.1. Find the integer $0 \leq a \leq 36$ such that

$$3777^{\left(1144523^{56245501}\right)} \equiv a \pmod{37}$$

We can reduce the base $3777 \equiv 3 \pmod{37}$. We reduce $1144523 \equiv 11 \pmod{\phi(37)}$. We can reduce the upper power $56245501 \equiv 1 \pmod{\phi(\phi(37))}$. This reduces to

$$3^{11} \equiv a \pmod{37}$$

which gives $a \equiv 28 \pmod{37}$.

Problem 12.2. Let $p \in \mathbb{Z}$ be a prime and let g be a primitive root mod p. Describe the set

$$\{g^k \mid g^k \text{ is a primitive root mod } p\}$$

Proof. We claim that $\gcd(k, p-1) = 1$. Then for any element $a = g^\alpha$, we can find power $(g^k)^\beta = g^\alpha$ since we have $g^{p-1} \equiv 1$ so $k\beta - x(p-1) = \alpha$ for some x, which only has solutions by Bezout's identity when $\gcd(k, p-1)$. □

Lemma

Prove that for any finite group G of order n and any $g \in G$, the cyclic group $\langle g^k \rangle$ for k such that $\gcd(k, \text{ord}(g)) = 1$ equals $\langle g \rangle$.

Proof. Let $d = (k, \text{ord}(g))$. Then there exists $x, y \in \mathbb{Z}$ such that

$$\text{ord}(g) \cdot x + k \cdot y = d$$

so

$$\begin{aligned} g^d &= g^{\text{ord}(g) \cdot x + ky} \\ &= g^{\text{ord}(g) \cdot x} \cdot g^{ky} \\ &= g^{ky} \end{aligned}$$

so $g^d \in \langle g^k \rangle \implies \langle g^d \rangle \subseteq \langle g^k \rangle$. We have $\langle g^k \rangle \subseteq \langle g^d \rangle$ since $d \mid k$. Thus $\langle g^d \rangle = \langle g^k \rangle$.

We also have that $(g^k)^{\text{ord}(g)/d} = (g^{\text{ord}\, g})^{k/d} = 1$ so if $d = (k, \text{ord}(g)) > 1$ then $\text{ord}(g^k) < \text{ord}(g)$.

So together we have that $\langle g \rangle = \langle g^k \rangle$ if and only if $(g, \text{ord}(g)) = 1$. □

Problem 12.3. Prove

Proposition
If $f : \mathbb{Z}_+ \to \mathbb{C}$ is a nonzero multiplicative function, then f^{-1} (the Dirichlet inverse) exists and is multiplicative.

Proof. Let h be given by

$$h(p^k) = f^{-1}(p^k) \qquad \text{prime powers } p^k$$
$$h(n) = h(p_1^{e_1}) \cdots h(p_k^{e_k})$$

then $(f \star h)(p^k) = I(p^k)$. Both $f \star h$ and I are multiplicative, so

$$(f \star h)(n) = I(n) \quad \forall n \in \mathbb{Z}$$

and $h = f^{-1}$.

(Existence, $f(1) = 1$ for any multiplicative function, so in particular our given f satisfies $f(1) \neq 0$.) □

Problem 12.4. Define $\lambda : \mathbb{Z}_+ \to \mathbb{C}$ by

$$\lambda(n) = (-1)^{e_1+e_2+\cdots}$$

where the e_i's are the exponents on the prime factorization of n. Let

$$g(n) = \sum_{d|n} \lambda(d)$$

Prove that

$$g(n) = \begin{cases} 1 & \text{if } n \text{ is square} \\ 0 & \text{otherwise} \end{cases}$$

Proof. We note that λ is multiplicative, and g is a summatory function of λ which is multiplicative. So we just prove on prime powers. If we have prime power with even exponent, then $p, p^2, \ldots, p^{e_1} \mid p^{e_1}$ gives $1 + (-1) + 1 + (-1) + \cdots + 1 = 1$. We have 0 otherwise. □

§13 March 22, 2022

§13.1 Discriminants of bases, Vandermonde determinants

We have some review from last time:

Let $K = \mathbb{Q}(\theta)$ be a number field of degree n, let $\{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Q}$-basis of K, and let $\sigma_i : K \hookrightarrow \mathbb{C}$, $1 \leq i \leq n$ be the embeddings of K into $\mathbb{C}$.

The discriminant of $\{\alpha, \ldots, \alpha_n\}$ is

$$\Delta[\alpha_i, \ldots, \alpha_n] = \det \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}^2$$

If $\{\beta_1, \ldots, \beta_n\}$ is another basis, then for all $1 \leq k \leq n$,

$$\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_i, \quad c_{ik} \in \mathbb{Q},$$

where $\det(c_{ik}) \neq 0$. Fact from homework is that

$$\Delta[\beta_i, \ldots, \beta_n] = \det(c_{ik})^2 \cdot \Delta[\alpha_i, \ldots, \alpha_n]$$

Theorem (2.7, p.42 [?])
The discriminant of any $\mathbb{Q}$-basis for K is rational and nonzero.

Proof. It suffices to prove this for $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$. □

We have the following observation:

Definition (Vandermonde Matrix)
A (square) Vandermonde matrix is a matrix of the form

$$V = \begin{pmatrix} 1 & t_1 & t_1^2 & \ldots & t_1^{n-1} \\ 1 & t_2 & t_2^2 & \ldots & t_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & t_n & t_n^2 & \ldots & t_n^{n-1} \end{pmatrix}$$

We then claimed (without proof) that

Claim — The determinant of V is

$$\prod_{1 \leq i < j \leq n} (t_j - t_i).$$

Proof. We know that $\det(V) = 0$ when $t_i = t_j$ for some $i \neq j$. So, $\det(V)$ (as a polynomial in $t_1, \ldots, t_n$) is divisible by $t_i - t_j$ for $i < j$. We have that the total degree of $\det(V)$ as a polynomial

in $t_1, \dots, t_n$ is

$$\sum_{i=1}^{n-1} i = \frac{n(n-1)}{2}.$$

On the other hand, the total degree of D is also $\binom{n}{2} = \frac{n(n-1)}{2}$. Hence, $\det(V)$ is a scalar multiple of D (since).

But $\det(V)$ and D are both monic as polynomials (*kinda*) in $\mathbb{Q}(t_2, \dots, t_n)[t_1]$. Thus $\det(V) = D$. *Or something like that.* □

Going back to the proof of theorem 11.4, we take $t_i = \theta_i := \sigma_i(\theta)$ to get

$$\begin{aligned}\Delta[1, \theta, \dots, \theta^{n-1}] &= \prod_{i<j} (theta_i - \theta_j)^2 \\ &= \mathsf{disc}(\mathsf{minpoly}_{\mathbb{Q}}(\theta)).\end{aligned}$$

which is clearly rational and nonzero in $\mathbb{Q}^+$.

Example 13.1

Let

$$K = \mathbb{Q}(\sqrt{5})$$

with the obvious basis $\{1, \sqrt{5}\}$. We have

$$\begin{aligned}\Delta[1, \sqrt{5}] &= \begin{vmatrix} 1 & \sqrt{5} \\ 1 & -\sqrt{5} \end{vmatrix}^2 \\ &= (-2\sqrt{5})^2 \\ &= 20\end{aligned}$$

and another basis is $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ and

$$\begin{aligned}\Delta\left[1, \frac{1+\sqrt{5}}{2}\right] &= \begin{vmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & -\frac{1+\sqrt{5}}{2} \end{vmatrix}^2 \\ &= (-2\frac{\sqrt{5}}{2})^2 \\ &= (\sqrt{5})^2 = 5\end{aligned}$$

Example 13.2

Let

$$K = \mathbb{Q}(\sqrt[3]{2})$$

A basis is $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\} =: B$

$$\Delta(B) = \begin{vmatrix} 1 & \sqrt[3]{2} & (\sqrt[3]{2})^2 \\ 1 & \zeta_3\sqrt[3]{2} & (\zeta_3\sqrt[3]{2})^2 \\ 1 & \zeta_3^2\sqrt[3]{2} & (\zeta_3^2\sqrt[3]{2})^2 \end{vmatrix}$$

computation left as exercise...

§13.2 Algebraic Integers

Definition 13.3 (Algebraic Integer)

A complex number is an algebraic integer if it is a root of a *monic* polynomial with integer coefficients.

We denote the set of algebraic integers by $\overline{\mathbb{Z}}$. By definitions, $\overline{\mathbb{Z}} \subseteq \overline{\mathbb{Q}}$.

Example 13.4

The following are some algebraic integers:

- $\sqrt{2} \in \overline{\mathbb{Z}}$ since $\sqrt{2}$ is a root of $x^2 - 2$.
- $\tau = \frac{1}{2}(1 + \sqrt{5})$, since $\tau^2 - \tau - 1 = 0$.

Non-examples:

- $\frac{22}{7}$ is not an algebraic integer. *Why?* We look at the 7-adic valuation of the monic polynomial when we plug $\frac{22}{7}$ in. What are some other ways to reason about this?

Key algebra fact: If $f(x) \in \mathbb{Z}[x]$ is a monic polynomial with $f(x) = g(x) \cdot h(x)$ where $g(x)$, $h(x)$ are monic polynomials in $\mathbb{Q}[x]$, then $g(x), h(x) \in \mathbb{Z}[x]$. (Gauss's Lemma).

Hence, if $\frac{22}{7}$ is an algebraic integer, if has some $f(x) \in \mathbb{Z}[x]$ for which it is a root. But it is also a root of $g(x) = x - \frac{22}{7}$ where $f(x) = g(x) \cdot h(x)$ forcing $g(x)$ to be in $\mathbb{Z}[x]$. So the fact that $\mathsf{minpoly}_{\mathbb{Q}}\left(\frac{22}{7}\right) = x - \frac{22}{7}$ implies that $\frac{22}{7} \notin \overline{\mathbb{Z}}$.

Definition (Algebraic Integer')

An algebraic number θ is an algebraic integer iff $\mathsf{minpoly}_{\mathbb{Q}}(\theta) \in \mathbb{Z}[x]$.

§14 March 24, 2022

§14.1 Algebraic Integers *continued*

Recall: our definition for algebraic integers...

Definition (Algebraic Integer)

A complex number that satisfies $f(x) = 0$ for a non-constant *monic* polynomial $f(x) \in \mathbb{Z}[x]$ is an algebraic integer.

An algebraic number is an algebraic number whose minimal polynomial over $\mathbb{Q}$ has integer coefficients.

We denote this set by $\overline{\mathbb{Z}}$.

Clearly, we have that $\overline{\mathbb{Z}} \subseteq \overline{\mathbb{Q}}$.

Claim — We want to show that $\overline{\mathbb{Z}}$ is, in fact, a subring of $\overline{\mathbb{Q}}$.

Lemma 14.1 (Setup Lemma, p.44 [?])

$\theta \in \mathbb{C}$ is an algebraic integer iff the additive group generated by all powers $1, \theta, \theta^2, \ldots,$ $\mathbb{Z}[\theta, \theta^2, \ldots]$, is finitely generated.

Proof. **Forward Direction.** Suppose $\theta \in \overline{\mathbb{Z}}$. Then for some n,

$$\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_0 = 0,$$

where $a_i \in \mathbb{Z}, \forall\ 0 \leq i \leq n-1$.

Claim — Every power of θ lies in the additive group Γ generated by $1, \theta, \theta^2, \ldots, \theta^{n-1}$.

Suppose inductively that $m \geq n$, and that $1, \theta, \theta^2, \ldots, \theta^m \in \Gamma$. We express

$$\begin{aligned}\theta^{n+1} = \theta^{m+1-n}\theta^n &= \theta^{m+1-n}(-a_{n-1}\theta^{n-1} - \cdots - a_0) \\ &= -a_{n-1}\theta^m - \text{lower degree stuff} \in \Gamma\end{aligned}$$

Backward Direction. Suppose every power of θ lies in a finitely generated additive group G. Then the subgroup Γ of G generated by $\{1, \theta, \theta^2, \ldots\}$ must also be finitely generated.

Let $v_1, \ldots, v_n$ be generators of Γ. (WLOG can assume not all zero). Each $v_i \in \mathbb{Z}[\theta]$ (polynomial in θ with integer coefficients), so $\theta v_i \in \mathbb{Z}[\theta]$ $\forall i$. Hence there exists integers b_{ij} such that

$$\theta v_i = \sum_{j=1}^{n} b_{ij} v_j \quad \forall i.$$

This gives us a system of linear equations

$$\begin{aligned}(b_{11} - \theta)v_1 + b_{12}v_2 + \cdots + b_{1n}v_n &= 0\\ b_{21}v_1 + (b_{22} - \theta)v_2 + \cdots + b_{2n}v_n &= 0\\ &\vdots\\ b_{n1}v_1 + b_{n2}v_2 + \cdots + (b_{nn} - \theta)v_n &= 0\end{aligned}$$

So now we have $A\vec{v} = \vec{0}$ so $\det A = 0$.

The $v_1, \ldots, v_n \in \mathbb{C}$ give a nontrivial solution to the obvious associated system of linear equations, so the determinant

$$\begin{vmatrix} b_{11} - \theta & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} - \theta & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} - \theta \end{vmatrix}$$

is zero. So the determinant, expanding as minors as a polynomial, is a monic[12] polynomial (in θ) with integral entries b_{ij} of which θ satisfies. So θ is an algebraic integer.

Both directions of which are as desired. □

Note we prove something stronger and more intuitive:

Lemma

$\theta \in \mathbb{C}$ is an algebraic integer iff the additive subgroup generated by $1, \theta, \theta^2, \ldots$ is in fact generated by $1, \theta, \theta^2, \ldots, \theta^{n-1}$ for some n.

Theorem 14.2

$\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.

Proof. Suppose that $\theta, \phi \in \overline{\mathbb{Z}}$. We want to show that $\theta + \phi, \theta\phi \in \overline{\mathbb{Z}}$.

By the lemma, all powers of θ lie in a finitely generated subgroup Γ_θ of $\mathbb{C}$ and similarly, all powers of ϕ lie in a finitely generated subgroup Γ_ϕ of $\mathbb{C}$.

[12] The highest degree of θ comes from the diagonal which monic up to sign. We also have that this is the characteristic of the b_{ij} matrix which is monic.

OTOH, all powers of $\theta+\phi$ and $\theta\phi$ are integer linear combinations of the elements

$$\theta^k\phi^l \in \Gamma_\theta\Gamma_\phi$$

where $\Gamma_\theta\Gamma_\phi :=$ the additive group generated by v_iw_j where $1 \le i \le n$ and $1 \le j \le m$ with

$$\Gamma_\theta = \langle v_1, \ldots, v_n\rangle$$
$$\Gamma_\phi = \langle w_1, \ldots, w_m\rangle$$

We note that $\Gamma_\theta\Gamma_\phi$ is finitely generated, and since each power of $\theta+\phi$ and $\theta\phi$ lie in this finitely generated subgroup[13], by our lemma $\theta+\phi$ and $\theta\phi$ are both algebraic integers. □

Theorem 14.3 (p.44 or p.45 [?])
Let $\theta \in \mathbb{C}$ satisfy a monic polynomial equation with coefficients in $\overline{\mathbb{Z}}$ (not just in $\mathbb{Z}$). Then θ is an algebraic integer.

Proof. One imitates the proof of the forward direction in our previous setup lemma, applying a bit of module theory. □

§14.2 Ring of Integers of a Number Field

Definition 14.4 (Ring of Integers of Number Field K)
If K is a number field, then

$$\mathcal{O}_K := K \cap \overline{\mathbb{Z}}$$

is called the ring of integers of K.[a]

[a] In textbooks, it's *fraktor* $\mathfrak{O}$. In papers, usually mathcal $\mathcal{O}$. In handwriting, usually fancy loopy O.

$\mathcal{O}_K$ is a ring because K and $\overline{\mathbb{Z}}$ are subrings of $\mathbb{C}$. The relationship between K and $\mathcal{O}_K$ is the same as that of $\mathbb{Q}$ and $\mathbb{Z}$.

Lemma 14.5
If $\alpha \in K$, then $c\alpha \in \mathcal{O}_K$ for some $c \in \mathbb{Z}$.

Proof. Let $\alpha \in K$ and $f(x) = \mathsf{minpoly}_{\mathbb{Q}}(\alpha)$, with $\deg f = n$. Let $0 \neq c \in \mathbb{Z}$ and let $g_c := c^n \cdot f\left(\frac{x}{c}\right)$.

Observe:

1) The roots of g_c are the $c\alpha_i$ where α_i are the roots of f.

[13] The subgroup that they generate had better be finitely generated.

2) g_c is monic.

3) If we choose c to be the lcm of the denominators of the coefficients of f implies that g_c has integer coefficients.

So $c\alpha$ is an element of $\mathcal{O}_K$ since it is also an algebraic integer. □

Corollary 14.6

If K is a number field, then $K = \mathbb{Q}(\theta)$, for some algebraic integer $\theta \in \overline{\mathbb{Z}}$.

Warning! (pp.46-47 [**?**]) Though it is often the case that if $K = \mathbb{Q}(\theta)$ with $\theta \in \overline{\mathbb{Z}}$, then $\mathcal{O}_K = \mathbb{Z}[\theta]$, this need not be true.

Example 14.7

Let $K = \mathbb{Q}(\sqrt{5})$. However,

$$\mathbb{Z}[\sqrt{5}] \subsetneq \mathcal{O}_K$$

In fact,

$$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] = \mathcal{O}_K.$$

Furthermore, is it always the case that $\mathcal{O}_K$ is generated by a single element? *No!* $\mathcal{O}_K$ need not be of the form $\mathbb{Z}[\theta]$ for some $\theta \in \overline{\mathbb{Z}}$.

Example 14.8

The counterexample of this is

$$K = \mathbb{Q}(\theta)$$

when θ is a root of $x^3 - x^2 - 2x - 8$.

Number fields where such a θ does exist are called monogenic.

§15 April 5, 2022

§15.1 Integral Bases for Number Fields

Recall:

- We introduced embeddings of a number field K into $\mathbb{C}$, which was directly related to the notion of conjugates.

- Also introduced discriminants of $\mathbb{Q}$-bases of number fields.
- Also introduced algebraic integers (algebraic numbers whose minimal polynomials over $\mathbb{Q}$ have integral coefficients).
- We said that the ring of integers of K is by definition $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$.
  - If $K = \mathbb{Q}$, then $\mathcal{O}_K = \mathbb{Z}$.

Definition 15.1 (Integral Basis)

Suppose $\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Q}$-basis for K such that $\alpha_i \in \mathcal{O}_K \ \forall i$. We say that $\mathcal{B}$ is an integral basis for $\mathcal{O}_K$ if every element $\alpha \in \mathcal{O}_K$ can be expressed *uniquely* as

$$\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$$

where each $a_i \in \mathbb{Z}$.

Theorem 15.2

Every number field has an integral basis.

Example 15.3

Sometimes, we're lucky or it's obvious. For example, if $K = \mathbb{Q}(\sqrt{2})$ then the obvious basis $\mathcal{B} = \{1, \sqrt{2}\}$ is an integral basis.

Proof. Let K be a number field of degree n. We had noted that if $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Q}$-basis of K with $\alpha_i \in \mathcal{O}_K \ \forall i$, then

$$\Delta[\alpha_1, \alpha_2, \ldots, \alpha_n] \in \mathbb{Z}$$

We take the absolute value and apply a well-ordering argument. Let $\{\omega_1, \ldots, \omega_n\}$ be a $\mathbb{Q}$-basis with $\omega_i \in \mathcal{O}_K \ \forall i$ and

$$|\Delta[\omega_1, \ldots, \omega_n]| \leq |\Delta[\alpha_1, \ldots, \alpha_n]|$$

for any $\mathbb{Q}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ with $\alpha_i \in \mathcal{O}_K \ \forall i$ (it has the least absolute value of discriminant).

Claim — $\{\omega_1, \ldots, \omega_n\}$ is an integral basis for $\mathcal{O}_K$.

Suppose otherwise, that there is an $\omega \in \mathcal{O}_K$ such that $\omega = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$ where $\alpha_i \in \mathbb{Q}$ and at least one $a_i \notin \mathbb{Z}$.

WLOG suppose $a_1 \notin \mathbb{Z}$. Then we can write

$$\alpha_1 = a + r$$

where a is an integer and $0 \leq r \leq 1$.

Let

$$\psi_1 = \omega - a\omega_1$$
$$\psi_i = \omega_i$$

for the remaining indices. We check that these are integers $\psi_i \in \mathcal{O}_K \ \forall i$ which is immediate since $\mathcal{O}_K$ is a ring.

The matrix sending the ω_i's to the ψ_i (with respect to the ω_i-basis) is

$$M = \begin{pmatrix} a_1 - a & 0 & 0 & \cdots & 0 \\ a_2 & 1 & 0 & \cdots & 0 \\ a_3 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Since this matrix is lower triangular, the determinant is the product of the diagonal entries, namely: $a_1 - a = r$.[14]

Hence,

$$\begin{aligned} \Delta[\psi_1, \psi_2, \ldots, \psi_n] &= (\det M)^2 \Delta[\omega_1, \omega_2, \ldots, \omega_n] \\ &= r^2 \Delta[\omega_1, \omega_2, \ldots, \omega_n] \end{aligned}$$

contradicting the minimality of $\{\omega_1, \ldots, \omega_n\}$ with respect to $|\Delta|$.

Thus $\{\omega_1, \ldots, \omega_n\}$ is an integral basis for K. □

Remark 15.4. A bit of extra reflection shows that any integral basis has a discriminant achieving this minimal possible absolute value.

Question. How do you know if you're looking at an integral basis?

You can *sometimes* diagnose this from the discriminant.

Theorem 15.5 (p.50 [?])
Suppose $\{\alpha_1, \ldots, \alpha_n\}$, with $\alpha_i \in \mathcal{O}_K \ \forall i$ forms a $\mathbb{Q}$-basis for K. If $\delta[\alpha_1, \ldots, \alpha_n]$ is squarefree, then $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis.

Proof. Let $\{\beta_1, \beta_2, \ldots, \beta_n\}$ is an integral basis. Then $\exists c_{ij} \in \mathbb{Z}$ such that each

$$\alpha_i = \sum_j c_{ij}\beta_j \ \forall i.$$

[14] A nonzero determinant gives that M is indeed a *change-of-basis* matrix. So this is indeed a basis.

Then $M = (c_{ij})$ is the change of basis matrix from the α_i's to the β_i's.

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det M)^2 \Delta[\beta_1, \ldots, \beta_n]$$

We know both $\det M$ and $\Delta[\beta_1, \ldots, \beta_n]$ are integers and $\Delta[\alpha_1, \ldots, \alpha_n]$ is squarefree. This forces $\det M = \pm 1$ so in fact $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis. □

Example 15.6

Let $K = \mathbb{Q}(\sqrt{5})$. We previously observed that $\theta = \frac{1+\sqrt{5}}{2} \in \overline{\mathbb{Z}}$ hence $\theta \in \mathcal{O}_K$ (θ is a root of $x^2 - x - 1$).

$$\Delta\left[1, \frac{1+\sqrt{5}}{2}\right] = \begin{vmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{vmatrix} = (-\sqrt{5})^2 = 5$$

thus $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ is an integral basis for K.

We previously said that the discriminant of integral bases are invariant for each number field, so we give this a name:

Definition 15.7 (Discriminant of Number Field)

Let K be a number field. The discriminant associated to any integral basis of $\mathcal{O}_K$ is called the discriminant of K.

Example 15.8

The discriminant of $K = \mathbb{Q}(\sqrt{5})$ has $\mathsf{disc}(K) = 5$ (by previous computation).

Example 15.9

What about $K = \mathbb{Q}(\sqrt{2})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$? We have

$$\begin{vmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{vmatrix}^2 = (-2\sqrt{2})^2 = 8$$

What if we don't want to do linear algebra? Previously we had that with power bases and Vandermonde discriminants, the discriminant of the basis is the discriminant of the minimum polynomial. $\{1, \sqrt{2}\}$ yields minimum polynomial $x^2 - 2$ which has determinant 8.

Example 15.10

More interesting, $K = \mathbb{Q}(\theta)$ for θ a root of

$$x^3 - x^2 - 2x - 8$$

An integral basis for $\mathcal{O}_K$ is given by

$$\left\{1, \theta, \frac{\theta+\theta^2}{2}\right\}$$

which is a number field that doesn't have a power integral basis. We have no basis of form $\{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$. The discriminant of this number field is -503.

Note: the following are "synonyms":

1. $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some $\theta \in \overline{\mathbb{Z}}$, $\theta \in \mathcal{O}_K$.
2. $\mathcal{O}_K$ (or K) is monogenic.
3. $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ with $\deg \theta = n$ forms an integral basis for some $\theta \in \mathcal{O}_K$.
4. $\mathcal{O}_K$ (or K) has a power integral basis.

We'll look at in more detail quadratic fields and cyclotomic extensions.

§15.2 Quadratic Fields

Definition 15.11 (Quadratic Field)
A quadratic field is a number field of degree 2 over $\mathbb{Q}$. For K to be quadratic is for $K = \mathbb{Q}(\theta)$ where θ a root of $x^2 + ax + b$, $a, b \in \mathbb{Z}$.

This gives that $\theta = \frac{-a \pm \sqrt{a^2-4b}}{2}$. We can write $a^2 - 4b = r^2 d$ where $r, d \in \mathbb{Z}$ with d squarefree. This gives $\theta = \frac{-a \pm r\sqrt{d}}{2}$. Immediately,

Proposition 15.12
The quadratic fields are exactly those of the form $\mathbb{Q}(\sqrt{d})$ for a squarefree integer d.

Theorem 15.13 (p.64 of [?])
Let $d \in \mathbb{Z}$ be a squarefree integer and let $K = \mathbb{Q}(\sqrt{d})$. Then $\mathcal{O}_K$ equals

a) $\mathbb{Z}\left[\sqrt{d}\right]$ if $d \not\equiv 1 \pmod 4$.

b) $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $d \equiv 1 \pmod 4$.

Proof. *Next time.* □

§16 April 7, 2022

§16.1 Quadratic Fields *continued*

Definition

A quadratic field is a number field K of degree 2 over $\mathbb{Q}$.

Thus $K = \mathbb{Q}(\theta)$ for θ a zero of some

$$x^2 + ax + b$$

for $a, b \in \mathbb{Z}$.

Hence,

$$\theta = \frac{-a \pm \sqrt{a^2 - 4b}}{2}.$$

Thus from which it follows

Proposition

The quadratic fields are of the form $\mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z}$ is squarefree.

Theorem (p.64 of [?])

Let $d \in \mathbb{Z}$ be a squarefree integer and let $K = \mathbb{Q}(\sqrt{d})$. Then $\mathcal{O}_K$ equals

a) $\mathbb{Z}\left[\sqrt{d}\right]$ if $d \not\equiv 1 \pmod 4$.

b) $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $d \equiv 1 \pmod 4$.

Proof. Every $\alpha \in \mathbb{Q}(\sqrt{d})$ is of the form

$$\alpha = \frac{a \pm b\sqrt{d}}{c}$$

with $a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$. Now $\alpha \in \mathcal{O}_K$ iff the coefficients of

$$\left(x - \frac{a + b\sqrt{d}}{c}\right)\left(x - \frac{a - b\sqrt{d}}{c}\right)$$

are in $\mathbb{Z}$. This holds iff

$$\frac{a^2 - b^2 d}{c^2} \in \mathbb{Z} \qquad \text{and} \qquad \frac{2a}{c} \in \mathbb{Z}$$

If $(a,c) \neq 1$, then in our first expression, the fact that d is squarefree forces our common factor must also be shared with b. So $\gcd(a,b,c) \neq 1$. So $(a,c) = 1$. Looking at our second expression, c is forced to be 1 or 2.

If $c = 1$, then $\alpha \in \mathcal{O}_K$ anyway, so assume that $c = 2$. We have that $\gcd(b,c) = 1$ by the same reasoning as before, so $c = 2$ implies that a and b are both odd.

Moreover, $\alpha \in \mathcal{O}_K$ with these assumptions iff

$$\frac{a^2 - b^2 d}{c^2} = \frac{a^2 - b^2 d}{4} \in \mathbb{Z}$$

which happens iff $a^2 - b^2 d \equiv 0 \pmod 4$. Then a, b odd implies $a^2 \equiv b^2 \equiv 1 \pmod 4$ so we get that this is equivalent to $d \equiv 1 \pmod 4$.

Thus $c = 2$ and $\alpha \in \mathcal{O}_K$ implies that $d \equiv 1 \pmod 4$.

In sum, if $d \not\equiv 1 \pmod 4$, then $c = 1$, so we've shown that $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. If $d \equiv 1 \pmod 4$, then we can have $c = 2$ and a, b odd. Hence $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. □

Theorem 16.1 (p.65 [?])

We then have the following:

a) If $d \not\equiv 1 \pmod 4$, then $\{1, \sqrt{d}\}$ is an integral basis. If $d \equiv 1 \pmod 4$, then $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ is an integral basis.

b) If $d \not\equiv 1 \pmod 4$, then $\mathsf{disc}(K) = 4d$. If $d \equiv 1 \pmod 4$, then $\mathsf{disc}\, K = d$.

§16.2 Cyclotomic Extensions

Definition 16.2

A cyclotomic field/extension is a number field of the form

$$K = \mathbb{Q}(\zeta_n), \quad \zeta_n = e^{2\pi i/n}.$$

That is, ζ_n is the primitive n-th root of unity. We could just as easily take $\zeta_n = e^{2\pi ik/n}$ where $\gcd(k,n) = 1$.

Example 16.3

$n = 1$ is boring. $n = 2$ is boring. $n = 2$ gives a quadratic field.

Example 16.4
$K = \mathbb{Q}(i)$ for $n = 4$, $\zeta_4 = i$.

$K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}\left(\frac{1+\sqrt{-3}}{2}\right) = \mathbb{Q}(\zeta_3)$.

We note:

- Any embedding of $\mathbb{Q}(\zeta_n) \hookrightarrow \mathbb{C}$ has image contained in $\mathbb{Q}(\zeta_n)$. (In other words, these extensions are Galois over $\mathbb{Q}$.)
- We care about extensions of the form $\mathbb{Q}(\sqrt[n]{a})$ where $a \in \mathbb{Q}$. But these are not Galois in general.

  The solution is to "repair" the base field. Take $K = \mathbb{Q}(\zeta_n)$ and $L = K(\sqrt[n]{a})$. Then L/K is Galois. This is to say that the embeddings $L \hookrightarrow \mathbb{C}$ that fix K stabilize L (send L to itself).
- *Kronecker-Weber theorem* that every finite Abelian extension of $\mathbb{Q}$ is contained in some cyclotomic extension.

We have some key facts about cyclotomic extensions:

1) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

2) The field automorphisms $\sigma : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ form a cyclic group under composition, of order $\phi(n)$. (Our automorphisms send ζ_n to some other primitive n-th root of unity ζ_n'.)

   From now on, let $K = \mathbb{Q}(\zeta_n)$.

3) Then $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. The case where $n = p$ is in the textbook.

4) We have
$$\mathsf{disc}(K) = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod\limits_{\substack{p \mid n \\ p \text{ prime}}} p^{\phi(n)/(p-1)}}$$

   For $n = p$ prime, we get
$$\begin{aligned} \mathsf{disc}(\mathbb{Q}(\zeta_p)) &= (-1)^{(p-1)/2} \cdot \frac{p^{p-1}}{p} \\ &= (-1)^{(p-1)/2} \cdot p^{p-2} \end{aligned}$$

   In particular, if $p \in \mathbb{Z}$ is a prime with $p \nmid n$, then $p \nmid \mathsf{disc}(K)$.

§16.3 Prime Factorization in Number Fields

Useful to note that this is section 5.1 in [?].

Recall: the examples of non-UFDs given previously in Math 1530.

Example 16.5
In $\mathbb{Z}[\sqrt{-5}]$, we have $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. And we check that each term here is irreducible.

(2, for example, is not an associate of $1 + \sqrt{-5}$ or $(1 - \sqrt{-5})$. Simply reason by norms.)

Example 16.6
What about $\mathbb{Q}(\sqrt{15})$?

$$2 \cdot 5 = (5 + \sqrt{15})(5 - \sqrt{15})$$

in $\mathbb{Z}[\sqrt{15}]$.

Example 16.7
In $\mathbb{Q}(\sqrt{30})$,

$$2 \cdot 3 = (6 + \sqrt{30})(6 - \sqrt{30})$$

In $\mathbb{Q}(\sqrt{-10})$,

$$2 \cdot 7 = (2 + \sqrt{-10})(2 - \sqrt{-10})$$

Question. What's going wrong?

In example 16.6, we notice

$$5 + \sqrt{15} = \sqrt{5}(\sqrt{5} + \sqrt{3})$$
$$5 - \sqrt{15} = \sqrt{5}(\sqrt{5} - \sqrt{3})$$

Multiplying these together, we get

$$25 - 15 = 10 = 5 \cdot (\sqrt{5} + \sqrt{3}) \cdot (\sqrt{5} - \sqrt{3})$$

so the factors in

$$\sqrt{5} \qquad \sqrt{5} + \sqrt{3} \qquad \sqrt{5} - \sqrt{3}$$

are being grouped in 2 ways:

$$(a_1^2)(a_2 a_3) = (a_1 a_2)(a_1 a_3)$$

In other words, the problem goes away in $\mathcal{O}_L$ for $L = \mathbb{Q}(\sqrt{15}, \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ (we extend to get some other things in it).

We can check that the same thing underlies the other two examples.

Theorem 16.8 (Principal Ideal Theorem)
Let K be a number field. Then there is a finite extension L/K such that every nonzero $\alpha \in \mathcal{O}_K$ has a unique factorization into irreducibles in $\mathcal{O}_L$.

Caution! This does *not* say that $\mathcal{O}_L$ is a UFD. So it is not true that every number field K has a finite extension L/K such that $\mathcal{O}_L$ is a UFD.

§17 April 12, 2022

§17.1 Ideals and Fractional Ideals

Let R be a commutative ring with an identity.

Recall that if I, J are ideals of R, then

$$I + J := \{a_i + b_j \mid a_i \in I, b_j \in J\}$$

and

$$IJ := \left\{\sum a_i b_j \mid a_i \in I, b_j \in J\right\}$$

Let K be a number field. An ideal of $ri O_K$ is sometimes called an intgral ideal. This is to contrast them with fractional ideals.

Definition 17.1
A fractional ideal of $\mathcal{O}_K$ is a set of the form $c^{-1}\mathfrak{b}$ when $\mathfrak{b}$ is an ideal of $\mathcal{O}_K$ and $0 \neq c \in \mathcal{O}_K$.

Example 17.2
The fractional ideals of $\mathbb{Z}$ are of the form $r\mathbb{Z}$ where $r \in \mathbb{Q}$.

$\frac{2}{5}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$.

Caution! If $\mathcal{O}_K$ is a PID, then fractional ideals are of the form

$$c^{-1}\langle d\rangle$$

for $0 \neq c \in \mathcal{O}_K$ and $d \in \mathcal{O}_K$. This is just $c^{-1}d\mathcal{O}_K = \alpha\mathcal{O}_k$ where $\alpha = c^{-1}d$.

Addition/multiplication of fractional ideals works similarly as in the case of ideals:

If $\mathfrak{a}, \mathfrak{b}$ are fractional ideals, then

$$\mathfrak{ab} := \left\{\text{finite sums } \sum a_i b_j \mid a_i \in \mathfrak{a}, b_j \in \mathfrak{b}\right\}$$
$$\mathfrak{a} + \mathfrak{b} := \{a_i + b_j \mid a_i \in \mathfrak{a}, b_j \in \mathfrak{b}\}$$

If $a_1 = c_1^{-1}\mathfrak{b}_1$ and $a_2 = c_2^{-1}\mathfrak{b}_2$ where $\mathfrak{b}_1, \mathfrak{b}_2$ are integral ideals, then we have

$$\mathfrak{a}_1\mathfrak{a}_2 = (c_1c_2)^{-1}\mathfrak{b}_1\mathfrak{b}_2$$

The multiplication is obviously associative and commutative, with $\mathcal{O}_K$ as the identity.

Thus, the set of *nonzero* fractional ideals forms a monoid[15] under (commutative) multiplication.

If we want the structure of an Abelian group, we need to build the inverses in.

Theorem 17.3 (p. 109 [?])
The nonzero fractional ideals of $\mathcal{O}_K$ form a group under multiplication.

For each ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, define

$$\mathfrak{a}^{-1} := \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}_K\}$$

Automatically, this set contains all of $\mathcal{O}_K$.

If $\mathfrak{a} \neq 0$, then for any $0 \neq c \in \mathfrak{a}$, $c\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. Fixing such a c, we have that $c\mathfrak{a}^{-1} =: \mathfrak{b}$ is an ideal of $\mathcal{O}_K$. (Why? $c\mathfrak{a}^{-1}$ is an $\mathcal{O}_K$-submodule of $\mathcal{O}_K$, i.e. that is to say, an ideal of $\mathcal{O}_K$.)

Example 17.4
Let's take $K = \mathbb{Q}$ so that $\mathcal{O}_K = \mathbb{Z}$

$$\mathfrak{a} = 5\mathbb{Z}$$
$$\mathfrak{a}^{-1} = \frac{1}{5}\mathbb{Z}$$

Thus $\mathfrak{a}^{-1} = c^{-1}\mathfrak{b}$, so that $\mathfrak{a}^{-1}$ is a fractional ideal.

By definition,

$$\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathcal{O}_K$$

Harder to show: $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$. We blackbox this for the moment (p.110-112 [?], uses fact that $\mathcal{O}_K$ is a Dedekind domain). We can extend this discussion to fractional ideals $\mathfrak{a}$. Assuming this, we have shown theorem 17.3.

Theorem (p. 109 [?])
The nonzero fractional ideals of $\mathcal{O}_K$ form a group under multiplication.

[15] Also a commutative ring with addition, actually.

Proof. Let $\mathfrak{a}$ be a nonzero fractional ideal of $\mathcal{O}_K$. We have $\mathfrak{a} = c^{-1}\mathfrak{b}$ with $\mathfrak{b}$ integral. We define $\mathfrak{a}' = c\mathfrak{b}^{-1}$, which is a fractional ideal, and $\mathfrak{a}\mathfrak{a}' = \mathcal{O}_K$. So $\mathfrak{a}'$ is the inverse of $\mathfrak{a}$. □

Recall: A prime ideal of a commutative ring R can be defined in a couple of different ways:

Definition 17.5 (Prime Ideal)
An ideal $\mathfrak{p}$ is prime if $IJ \subseteq \mathfrak{p}$ implies $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$.

Definition (Prime Ideal (alternative))
$\mathfrak{p}$ is prime if $ab \in \mathfrak{p}$ implies that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

To prove unique factorization of nonzero ideals, we first need to prove $\mathcal{O}_K$ is a Dedekind domain.

Theorem 17.6 (p.108 [?])
The ring of integers $\mathcal{O}_K$:

a) is an integral domain,

b) is Noetherian (every ascending chain of ideals terminates[a], or every ideal is finitely generated),

c) is integrally closed in its field of fractions (that is, if $\alpha \in \mathsf{Frac}(\mathcal{O}_K) = K$ satisfies a monic polynomial equation with coefficients in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$),

d) has that every nonzero prime ideal of $\mathcal{O}_K$ is maximal.

We note that a ring satisfying (a)–(d) is called a Dedekind domain.

[a] A chain of ideals is a sequence of inclusions $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$; and for such a chain to terminate means that $\exists N$ such that $I_n = I_N$ for all $n \geq N$.

§18 April 14, 2022

Recall: Last time:

- we defined fractional ideals,
- define the inverse of a nonzero integral ideal (and noted at the end of the same definition holds for fractional ideals)[16]

[16] An integral domain has all of its nonzero fractional ideals invertible iff it is a Dedekind domain.

- we briefly stated the definition of a Dedekind domain.

§18.1 Dedekind Domains

We introduced last time...

Theorem (p.109 [?])
The ring of integers $\mathcal{O}_K$:

(a) is an integral domain;

(b) is Noetherian, that is to mean one of the following:

(i) every ascending chain of ideals terminates, or

(ii) every ideal is finitely generated;

(c) if $\alpha \in \mathsf{Frac}(\mathcal{O}_K) = K$ satisfies a nonzero monic polynomial equation with coefficients in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$ ($\mathcal{O}_K$ is integrally closed in its field of fractions);

(d) every nonzero prime ideal of $\mathcal{O}_K$ is maximal.

Proof.

(a) *We know this.*

(b) We know that if $[K : Q] = n$, then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n[17].

If $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, then $(\mathfrak{a}, +)$ is a free Abelian group of rank $\leq n$[18]. As a group, $\mathfrak{a}$ is finitely generated, so $\mathfrak{a}$ (with some glossing over) is finitely generated as an ideal.

(c) *Was noted in a previous lecture.*

(d) Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$. Let $0 \neq \alpha \in \mathfrak{p}$. Then $N := N_{K/\mathbb{Q}}(\alpha) = \alpha_1\alpha_2 \cdots \alpha_n$[19] where $\alpha_1 := \alpha$ and α_i are the conjugates of $\alpha = \alpha_1$.

Note that $\alpha_2\alpha_3 \cdots \alpha_n \in K$ since the whole product $\alpha_1\alpha_2 \cdots \alpha_n \in \mathbb{Q} \subseteq K$ and $\alpha_1 \in K$. In fact, $\alpha_2\alpha_3 \cdots \alpha_n \in \mathcal{O}_K$. Hence $N := N_{K/\mathbb{Q}}(\alpha) \in \mathfrak{p}$. Thus $N \cdot \mathcal{O}_K \subseteq \mathfrak{p}$. This means that, taking quotients[20],

$$\mathcal{O}_K/\mathfrak{p} \text{ is a quotient of } \mathcal{O}_K/N\mathcal{O}_K$$

[17] That is, a free Abelian group of rank n; or also to say possesses an integral basis of order n
[18] *Theorem 1.16* of [?] proves this fact about submodules of free modules.
[19] We know this lives in $\mathbb{Q}$ since it's a term of the polynomial.
[20] If $I \subseteq J \subseteq R$, then R/J is a quotient of R/I.

But $\mathcal{O}_K/N\mathcal{O}_K$ is a finitely generated Abelian group where every element has finite order, so $\mathcal{O}_K/N\mathcal{O}_K$ is finite.

Hence $\mathcal{O}_K/\mathfrak{p}$ is finite. So $\mathcal{O}_K/\mathfrak{p}$ is also an integral domain (by ring theory). Any finite integral domain is a field, so $\mathcal{O}_K/\mathfrak{p}$ is a field. So $\mathfrak{p}$ has to be maximal (again by ring theory).

Which proves part (a) through (d). □

Proposition 18.1 (p.112 [?])
Every nonzero ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ is a product of prime ideals.

Proof. [21] If not, let $\mathfrak{a}$ be maximal subject to the condition of not being a product of prime ideals.

> **Remark.** Recall Zorn's Lemma: in a partially ordered set where every chain has an upper bound, there is at least one maximal element. We apply Zorn's Lemma to ideals to find such a maximal ideal.

Then $\mathfrak{a}$ is not prime, but applying Zorn to the poset of ideals containing $\mathfrak{a}$ to conclude that $\mathfrak{a} \subseteq \mathfrak{p}$ for some maximal (hence prime) ideal $\mathfrak{p}$.

We have that $\mathcal{O}_K \subsetneq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$, since $\mathfrak{p}$ is a proper ideal of $\mathcal{O}_K$, and $\mathfrak{a} \subseteq \mathfrak{p}$.

It follows that[22]

$$\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$$

By the maximality of $\mathfrak{a}$, we have that

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2\mathfrak{p}_3 \cdots \mathfrak{p}_r$$

where $\mathfrak{a}\mathfrak{p}^{-1}$ is a product of prime ideals $\mathfrak{p}_2, \mathfrak{p}_3, \ldots, \mathfrak{p}_r$, so

$$\mathfrak{a} = \mathfrak{p}\mathfrak{p}_2\mathfrak{p}_3 \cdots \mathfrak{p}_r$$

which is a contradiction, since $\mathfrak{a}$ is the product of prime ideals. □

Lemma 18.2 (p.113 [?])
For ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}_K$, $\mathfrak{a} \mid \mathfrak{b} \iff \mathfrak{b} \subseteq \mathfrak{a}$.

Question. What does $\mathfrak{a} \mid \mathfrak{b}$ mean? It means there exists an ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{c} \cdot \mathfrak{a}$.

[21] This is very analogous to the proof of the existence of prime factorization in $\mathbb{Z}$. Noetherian-ness of $\mathcal{O}_K$ takes the place of well-ordereding. $\mathfrak{a}$ being maximal ideal that isn't the product of prime ideals is akin to selecting a to be the least element not a product of primes. a itself isn't prime so is a product, and so on...

[22] Inverses let us preserve containment of $\subsetneq$, because if we hit both sides with $\mathfrak{a}^{-1}$ we get nice things.

Proof. Since $\mathfrak{ca} \subseteq \mathfrak{a}$, we have that $\mathfrak{a} \mid \mathfrak{b}$ implies that $\mathfrak{b} \subseteq \mathfrak{a}$.

Now we prove the other direction. Suppose $\mathfrak{b} \subseteq \mathfrak{a}$, then

$$\mathfrak{b} = \mathfrak{a}(\mathfrak{a}^{-1}\mathfrak{b}),$$

where $\mathfrak{a}^{-1}\mathfrak{b}$ is integral. Letting $\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{c}$ shows that $\mathfrak{a} \mid \mathfrak{b}$. □

Theorem 18.3

Every nonzero ideal of $\mathcal{O}_K$ has a unique factorization as a product of prime ideals.

Proof. The lemma above tells us that $\mathfrak{p}$ is prime iff $\mathfrak{p} \mid \mathfrak{ab} \Rightarrow \mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$. Then proceed as follows as we had done so in integers.

Suppose

$$\begin{aligned}\mathfrak{a} &= \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r \\ &= \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_s\end{aligned}$$

for some prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r, \mathfrak{q}_1, \mathfrak{q}_2, \cdots, \mathfrak{q}_s$. Then $\mathfrak{p}_1$ divides $\mathfrak{q}_j$ for some $\mathfrak{j}$. Since $\mathfrak{q}_j$ is maximal, $\mathfrak{p}_1 = \mathfrak{q}_j$. We multiply by $\mathfrak{p}_1^{-1}$ repeat the process, concludes the proof. □

§19 April 21, 2022

Recall: last time we...

- Discussed fractional ideals (in $\mathcal{O}_K$).
- Introduced inverses to nonzero fractional ideals in $\mathcal{O}_K$/Dedekind domains.
- Proved $\mathcal{O}_K$ was a Dedekind domain
- Used the properties of $\mathcal{O}_K$ to show that every nonzero ideal of $\mathcal{O}_K$ factors uniquely as a product of prime ideals (and the same argument works for Dedekind domains).

§19.1 Ramification Theory

A major topic/theme in classical algebraic number theory is the factorization of ideals in $\mathcal{O}_K$ generated by primes in $\mathbb{Z}$.

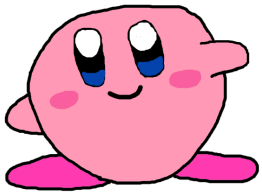

Figure 1: Kirby!

Question. Kirby, what primes ramify in $\mathbb{Q}(i)$?

Definition 19.1

Let $p \in \mathbb{Z}_+$ be a prime, and let K be a number field.

1) We say that p ramified in K (or $\mathcal{O}_K$) if, for

$$(p) := p \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r},$$

(for $\mathfrak{p}_i$'s pairwise distinct) we have that some $e_i \geq 2$.

2) We say that p is totally ramified if

$$(p) = \mathfrak{p}_1^n$$

where $n = [K : \mathbb{Q}]$ and $\mathfrak{p}_1$ is prime.

3) We say that p is intert if (p) is a prime ideal of $\mathcal{O}_K$.

4) We say that p is totally split if

$$(p) = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$$

(for $\mathfrak{p}_i$'s pairwise distinct), $n = [K : \mathbb{Q}]$.

Remark 19.2. These categories are not *all* the classifications of primes!

Example 19.3

$(2) = (1+i)^2$ in $\mathbb{Z}[i] = \mathcal{O}_K$ for $K = \mathbb{Q}(i)$, so 2 *ramifies* in K (and in fact is *totally ramified*).

Example 19.4

(3) in $\mathbb{Z}[i]$? It turns out that (3) is a prime ideal. So 3 is inert in $\mathbb{Q}(i)$.

Example 19.5

What about (5) in $\mathbb{Z}[i]$?

$$5 = (1+2i)(1-2i)$$

and $1+2i$, $1-2i$ are irreducible, but are not associates. So 5 is *totally split* in $\mathbb{Q}(i)$.

2 key structural questions are:

1) Which primes of $\mathcal{O}_K$ ramify?

2) How do individual rational primes factor in $\mathcal{O}_K$?

Theorem 19.6

p is ramified in K iff $p \mid \mathsf{Disc}(K)$.

Example 19.7

We can now answer the question posed to Kirby! In $\mathbb{Q}(i)$,

$$\mathsf{disc}(\mathbb{Q}(i)) = \begin{vmatrix} 1 & i \\ 1 & -i \end{vmatrix} = (-2i)^2 = -4$$

so 2 is the only prime that ramifies in $\mathbb{Q}(i)$.

We prove this in the monogenic case, i.e. when $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some $\theta \in \mathcal{O}_K$.

The moral is: study the factorization of f modulo p where $f = \mathsf{minpoly}_{\mathbb{Q}}(\theta)$.

Proof. Suppose K is monogenic, with $\mathcal{O}_K = \mathbb{Z}[\theta]$ and let $p \in \mathbb{Z}_+$ be prime. Let $f = \mathsf{minpoly}_{\mathbb{Q}}(\theta)$. Since $\mathsf{Disc}(K) = \Delta[1, \theta, \theta^2, \ldots, \theta^{n-1}] = \mathsf{disc}(f)$. We show that $p \mid \mathsf{disc}(f) \Leftrightarrow p$ ramifies in K.

Let $p \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}$ be the prime factorization of $p \cdot \mathcal{O}_K$. Then

$$\mathcal{O}_K/(p) \cong \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \mathcal{O}_K/\mathfrak{p}_2^{e_2} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_r^{e_r}$$

by Sunzi's Theorem, as $\mathfrak{p}_i + \mathfrak{p}_j = \mathcal{O}_K$, $\forall i \neq j$ (in HW7).

OTOH, we have that

$$\mathcal{O}_K/(p) = \mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong \mathbb{Z}[x]/(p, f(x)) \cong (\mathbb{Z}/p\mathbb{Z})/(\overline{f}(x))$$

We first have that $\mathbb{Z}[\theta] \cong \mathbb{Z}[x]/f(x)$ (since f is the minimum polynomial of θ), then we quotient again by p[23].

[23] Since we have $(R/(a))/(\overline{b}) \cong R/(a,b)$. For example, $(\mathbb{Z}/5\mathbb{Z})/(\overline{2}) \cong \mathbb{Z}/(2,5) \cong \mathbb{Z}/\mathbb{Z}$.

If $\overline{f}(x) = \overline{\pi}_1(x)^{f_1}\overline{\pi}_2(x)^{f_2}\cdots\overline{\pi}_s(x)^{f_s}$ is the factorization of $\overline{f}$ into produce of irreducibles, then

$$(\mathbb{Z}/p\mathbb{Z})[x]/(\overline{f}) \cong \mathbb{F}_p[x]/\overline{\pi}_1(x)^{f_1} \times \cdots \times \mathbb{F}_p[x]/\overline{\pi}_s(x)^{f_s}$$

(also by Sunzi's theorem.)

Our goal is to show that these line up... $s = r$ and exponents line up.

We isolate $\mathcal{O}_K/\mathfrak{p}_1^{e_1}$ and we have chain

$$\mathfrak{p}_1^{e_1} \subsetneq \mathfrak{p}_1^{e_1} \subsetneq \cdots \subsetneq \mathfrak{p}_1 \subsetneq \mathcal{O}_K$$

so $\mathfrak{p}_1/\mathfrak{p}_1^{e_1}$ is a maximal ideal of $\mathcal{O}_K/\mathfrak{p}_1^{e_1}$.

To find maximal ideals in $\mathcal{O}_K/(p)$, we take the maximal ideal in the first product $(\mathfrak{p}_1/\mathfrak{p}_1^{e_1})$ and product with the rest of the product. So there are exactly r maximal ideals, and on the other side we have exactly s maximal ideals. Thus $r = s$.

We do a similar thingy done in 1530 when we showed every finite Abelian group is the product of some cyclic groups:

$$\begin{aligned} G &\cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r} \\ &\cong \mathbb{Z}/q_1^{f_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/q_s^{f_s} \end{aligned}$$

where we reordered. We start with some ideal $\mathfrak{I}_1$

$$\mathfrak{I}_1 = I_1 \times \mathcal{O}_K/\mathfrak{p}_2^{e_2} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_r^{e_r}$$

where I_1 is maximal in $\mathcal{O}_K/\mathfrak{p}_1^{e_1}$, and we start forming chains to recover e_1, and we continue doing so by 'carving' into other factors. ("nilpotence argument" shows that after appropriate reordering, $e_i = f_i$, $\forall i$.)

We want to characterize when $e_i \geq 2$ (so we have ramification). This is when some $f_i \geq 2$, which is to say whether $\overline{f}$ mod p has a repeated root (is not separable). But this is equivalent to saying

$$\mathsf{disc}(f) \equiv 0 \pmod{p}$$

since taking discriminants commutes with reduction modulo p. So $p \mid \mathsf{disc}(f) = \mathsf{Disc}(K)$. $\square$