MATH 1560 Notes

Mattie Ji

Updated: August 25, 2022

Lecture 1 to 11 cover topics in Elementary Number Theory and are loosely based on Kenneth Ireland and Michael Rosen's *A Classical Introduction to Modern Number Theory* [IR11]. The last section of Lecture 11 and remaining lectures cover selected topics in Algebraic Number Theory and are loosely based on Chapter 1 to 6 of Stewart and Tall's *Algebraic Number Theory and Fermat's Last Theorem* [ST20].

Table of Content

1 Lecture 1 (January 27th) - Introduction to Number Theory

There are two maor branches in Number Theory - Algebraic and Analytic Number Theory.

1.1 What is Number Theory?

Definition 1.1. Number Theory is the study of the integers, along with their analogs in algebraic number fields. Primes are a key focus, both in terms of:

- 1) Distributional Properties - Analytic Number Theory
- 2) Building Blocks of Algebraic Numbers - Algebraic Number Theory

Example 1.2 (Problems in Analytic Number Theory)**.** There are many problems in Analytic Number Theory.

- Prime Number Theorem:

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

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

  This gives you a density approximation of $\pi(x)$ for large integer x.

- Twin Prime Conjecture:

  Twin primes are pair of primes (p, q) such that $q = p + 2$ (ex. $(3, 5)$). The Twin Prime Conjecture postulates that there are infinitely many pais of twin primes.

- Polignac's Conjecture:

  Let $2k$ be a even number, then there exists infinitely many pair of primes (p, q) where $q = p + 2k$. Yitang Zhang shrinked this number to $70,000,000$.

- The Goldbach Conjecture:

  Every even integer greater than 2 is the sum of two prime numbers.

Example 1.3 (Problems in Algebraic Number Theory)**.** There are many problems in Algebraic Number Theory.

- Factorization in (rings of Integers of) Number Fields:

  For example, 2 is a prime element of $\mathbb{Z}$, but 2 is not prime in $\mathbb{Z}[i]$ since $2 = (1 + i)(1 - i)$. Note that $1 + i = i(1 - i)$, so $(2) = (1 + i)^2$.

  One might ask how many ways are there to factor a given prime. It turns out that given a prime p, there's exactly 2 ways to factor them in $\mathbb{Z}[i]$

- Fermat's Last Theorem:

  There are no pairs of distinct integer (x, y, z) such that $x^n + y^n = z^n$, for $n \geq 3$. (SHE READ THE ENTIRE PROOF 2nd Year of Grad School????)

- ABC Conjecture:

  A "powerful number" is a positive integer whose prime factorization contain relatively few distinct primes (appropriately weighted) with exponent 1.

For example $2^{10} * 3^7$ is a powerful number, so is $2^{10} * 3^7 * 5$. 1 is also a powerful number.

Powerful Number has less prime factor whose power is 1, than the ones that have prime factor whose exponent is not 1.

If a, b are very powerful coprime numbers, can $a + b$ also be powerful?

For example, take $2^{10} + 3^{15} = 14,349,931 = 31 \cdot 462,901$, this is not a powerful prime. This lack of powerfulness is predicted by the ABC conjecture.

What about $3^{15} + 5$? ABC predicts that this sum is not very powerful.

2 Lecture 2 (February 1st)

2.1 Annoucement

A few notes:

- Homework 0 (biography) is going up tonight
- Lecture notes will (generally) be posted after each class

2.2 Unique Factorization

Definition 2.1 (Common Definitions)**.** We will establish some elementary notations first:

- We denote $a|b$ as "a divides b" and $a \nmid b$ as "a does not divide b".
- We say that a positive integer $p \geq 2$ is *prime* if its only positive divisors are 1 and p.
- $\mathbb{Z}_+$ denotes the set of positive integers, and let $\mathbb{N}$ be the natural numbers with 0!
- For a non-zero $n \in \mathbb{Z}$ and a prime p, there is a non-negative integer a such that $p^a|n$ but $p^{n+1}|n$, the number a is denoted as *the order of n at p* or $ord_p n$
- For $n = 0$, by convention we say that $ord_p 0 = \infty$
- Note that fairly trivially
$$ord_p n = 0 \iff p \nmid n$$

Lemma 2.2. Every non-zero integer can be written as a product of primes, except for -1. (Note that by convention the empty product is 1)

Proof. Suppose there exist some non-zero integer that can't be written as a product of primes, let N be the smallest integer greater than 2 that can't be written as a product of primes.

Clearly, N is not prime, or else $N = N$ is a valid product of primes.

Then we can write $N = a \cdot b$ where $1 < a, b < N$, but a and b can be written as product of primes, since N is the minimal number greater than 2 that can't be written as a product of primes. This is a contradiction. ■

Remark 2.3. Hence, for all non-negative integer n, we can write

$$n = (-1)^\epsilon \prod_{p \text{ pos prime}} p^{a(p)}$$

, where $\epsilon \in \{0, 1\}$ and $a(p)$ is a non-negative integer.

Theorem 2.4 (Unique Factorization)**.** For every non-zero integer n, there is a prime factorization

$$n = (-1)^\epsilon \prod_{p \text{ pos prime}} p^{a(p)}$$

where $\epsilon, a(p)$ are uniquely determined.

Moreover, $a(p) = ord_p n$

Before the proof, we recall a few things from Abstract Algebra

Lemma 2.5 (The Integers are an Euclidean Domain)**.** If $a, b \in \mathbb{Z}$ with $b > 0$, then there exist $q, r \in \mathbb{Z}$ st.

$$a = bq + r$$

, with $0 \leq r < b$

Proof. Consider the set

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

Note that S contains positive elements, (if a is positive, pick x = 0, if a is negative or zero, pick sufficiently negative value of x)

Let $r = a - qb$ be the least non-negative element of S.

Then we claim that the pair (q, r) here is the pair we are looking for. To do this, we only need to show that $0 \leq r < b$, suppose for the sake of contradiction that $r \geq b$, then

$$r = a - qb \geq b$$

But this means that

$$a - (q + 1)b \geq 0$$

So r is not the smallest integer possible satisfying the constraint, contradiction. ■

Corollary 2.6. $\mathbb{Z}$ is an Euclidean domain, with Euclidean function given by $x \mapsto |x|$.

Quick recall on what the Euclidean Domain is:

Definition 2.7 (Euclidean Domain)**.** Let R be an integral domain, then R is said to be a Euclidean Domain if there exist a *Euclidean function* $\lambda : R - \{0\} \to \mathbb{Z}_{\geq 0}$ such that

- if $a, b \in R$ and $b \neq 0$, then there exists $c, d \in R$ such that

$$a = cb + d, d = 0 \text{ or } \lambda(d) < \lambda(b)$$

Example 2.8. $\mathbb{Z}$ is a Euclidean domain with $\lambda = |\cdot|$
$k[x]$, where k is a field is an Euclidean Domain with $\lambda = deg$

Definition 2.9. If an ideal $I = (a)$ for some $a \in I$, then I is said to be a principal ideal.

R is said to be a principal ideal domain (PID) if every ideal in R is a principal ideal.

Proposition 2.10. If R is an Euclidean Domain, then R is a PID. (ie. For any ideal $I \subset R$, there exists some $a \in R$ such that $I = aR$

Proof. If I is the zero ideal, then $I = (0)$ and is thus principal.

Now suppose I is a non-zero ideal, then there exists some non-zero element $a \in I$, we can choose a such that $\lambda(a)$ is minimal.

Now consider all $b \in I$, since R is an Euclidean Domain, we have that

$$b = qa + r$$

, where $\lambda(r) < \lambda(a)$ or $r = 0$.

If r is non-zero, this would violate the minimality of $\lambda(a)$ and be a contradiction, thus $r = 0$.

SO $b = qa$. Thus, I is a principal ideal.

Thus, R is a PID. ■

Definition 2.11 (Irreducible vs Prime)**.** We say $p \in R$ is **irreducible** if $a|p \implies$ a is either a unit, or an associate of p. We say $p \in R$ is **prime** if p is not a unit, p is non-zero, and $p|ab$ implies that either $p|a$ or $p|b$

Remark 2.12. The zero ideal is a prime ideal. The prime elements generate prime ideals, but the zero element itself is not prime.

Definition 2.13 (Greatest Common Divisor)**.** Let R be an integral domain, then we $d \in R$ is said to be the gcd of $a, b \in R$ if

- i) d divides a and d divides b
- ii) If $d'|a$ and $d'|b$, then $d'|d$

We denote (a, b) as the gcd of a and b, and in fact in the integers,

$$dR = aR + bR$$

gcd's are also only unique up to units. For the integers, we will refer the gcd to only the positive gcd.

Aside for Ring Theory enthusiasts, GCD Domains are a class of rings more general than PIDs and UFDs.

There are two important properties of PIDs:

- 1) Nonunit irreducible elements are exactly the prime elements
- 2) GCDs always exist in PIDs

We are now ready to prove unique factorization in $\mathbb{Z}$, after the lemma.

Lemma 2.14. Suppose p is a prime, and $a, b \in \mathbb{Z}$, then $ord_p(ab) = ord_p(a) + ord_p(b)$

Proof. If one of a and b is 0, that case is trivial.

So WLOG, we can assume that $a, b \neq 0$. Let $\alpha = ord_p(a)$ and $\beta = ord_p(b)$, then

$$a = p^\alpha * c,\ p \nmid c$$
$$b = p^\beta * d,\ p \nmid d$$

So we have that

$$ab = p^{\alpha+\beta}(dc)$$

Note that $p \nmid dc$ because $p \nmid d$ and $p \nmid c$ (contrapositive of definition of prime), so $ord_p(ab) = \alpha + \beta$.

Note that we used the fact that the non-unit irreducible element is prime in a PID (so the definition of prime in $\mathbb{Z}$ aligns with that of prime in PID). ■

Theorem 2.15 (The Fundamental Theorem of Arithmetic)**.** $\mathbb{Z}$ is a UFD.

Proof. Recall that for a non-zero $n \in \mathbb{Z}$, we can write

$$n = (-1)^\epsilon \prod_{p \text{ pos prime}} p^{a(p)}$$

, where $\epsilon \in \{0, 1\}$ and $a(p) \geq 0$.

This is the existence part, now we will prove the uniqueness part.

Given a positive prime q, we can take ord_q of both sides of the expressions:

$$\begin{aligned} ord_q(n) &= \epsilon \cdot ord_q(-1) + \sum_p a(p) ord_q(p) \\ &= 0 + \sum_p a(p) ord_q(p) \\ &= a(q) ord_q(q) && ord_q(p) = 0 \text{ for all } p \neq q \\ &= a(q) \cdot 1 \\ &= a(q) \end{aligned}$$

Since the positive prime q is arbitrarily chosen, the factorization has to be unique. ■

3 Lecture 3 (February 3rd):

3.1 Arithmetic Functions:

Definition 3.1. An *arithmetic function* is a function $f : \mathbb{Z}_+ \to \mathbb{C}$ (typically they are integer-valued)

Example 3.2. Examples of Arithmeitc Functions:

- The euler ϕ function is an arithmetic function.
- $\tau(n) = \sum_{d|n} 1$ (by convention this is the positive divisors)
- $\sigma(n) = \sum_{d|n} d$ is the sum of divisors of n. Note that $\sigma(n) = 2n$ means n is perfect.

Definition 3.3. An arithmetic function f is multiplicative, if

$$f(mn) = f(m)f(n), \text{ when gcd(m, n) = 1}$$

An arithmetic function f is completely multiplicative, if

$$f(mn) = f(m)f(n), \ m, n \in \mathbb{Z}$$

Remark 3.4. If particular, with induction, if f is multiplicative, and $n_1, ..., n_k$ are positive pairwise coprime integers, then

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

In particular, when $n = p_1^{e_1}...p_k^{e_k}$,

$$f(n) = f(p_1^{e_1})...f(p_k^{e_k})$$

Definition 3.5. An arithmetic function is called a **summatory function** if it's a function f of the following form:

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

, where g is some arithmetic function.

Remark 3.6 (Food for Thought:)**.** How special are these summatory functions in the set of arithmetic functions? Good concept check at the end of next lecture.

Lemma 3.7 (Summatory Functions inherit Multiplicativity)**.** If g is a multiplicative function, and

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

, then f is also multiplicative.

Proof. For all m, n positive integers such that m and n are coprime, note that the divisors d of mn is exactly the product set of divisors a of m and divisors b of n, ie.

$$\{d : d|mn\} \iff \{(a, b) : a|m, b|n\}$$

We want to show that the two sets above are bijective.

Consider the map $(a, b) \mapsto ab$, suppose there's (c, d) such that $c \neq a, d \neq b$ but $ab = cd$, we know $gcd(a, b) = 1$, or else this would imply $gcd(m, n) > 1$, so we have that

$$ab = (p_1^{e_1}...p_r^{e_r})(q_1^{f_1}...q_s^{f_s})$$

Now notice that if there's a different product that equals ab, WLOG, we will say that d contains a factor of a, say p_i^k, but this means that $p_i^k | n$, but since $a|m$, we also know $p_i^k | m$, so $gcd(m, n) \geq p_i^k$ is a contradiction. So the map has to

be injective.

Moreover, for all $d \in \{d : d|n\}$, since $gcd(m,n) = 1$, we can take $a = gcd(d,m), b = gcd(d,n)$, then $d = ab$. Specifically, clearly, $a|d$ and $b|d$, since $gcd(a,b) = 1$, $ab|d$. Since $gcd(m,n) = 1$ and d divides mn, d is composed of divisors from m and n that are disjoint, so $gcd(m,d), gcd(n,d)$ partitions those divisors perfectly. so this is surjective.

$$\begin{aligned} f(mn) &= \sum_{d|mn} g(d) \\ &= \sum_{a|m}\sum_{b|n} g(ab) && \text{Bijection of Sets Above} \\ &= \sum_{a|m}\sum_{b|n} g(a)g(b) && (a,b) = 1 \\ &= (\sum_{a|m} g(a))(\sum_{b|n} g(b)) \\ &= f(m)f(n) \end{aligned}$$

■

Remark 3.8.

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

is the summatory function of the constant 1 function.

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

is the summatory function of the identity function.
It is not true that the summatory function of the completely multiplicative function is completely multiplicative, but this does mean that both σ, τ are multiplicative functions.
Let p be a prime, then

$$\tau(p^e) = e + 1$$

since the only divisors of p^e is $1, p, ..., p^e$.

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

So we obtain that, when $n = p_1^{e_1}...p_k^{e_k}$

$$\tau(n) = \prod_{i=1}^{k}(e_i + 1)$$

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

Remark 3.9. There are also higher order divisor functions

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

ie, $\sigma_0 = \tau, \sigma_1 = \sigma$.

This is still a multiplicative function since d^k is multiplicative.

3.2 Interlude: review of $\mathbb{Z}/n\mathbb{Z}$ and its units

Definition 3.10. If $a, b, m \in \mathbb{Z}$ with m non-zero, we say that a is congruent to b modulo m if $m|b-a$, we denote this as

$$a \equiv b \ (mod \ n)$$

Or as

$$a \equiv b(m)$$

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

Definition 3.11. The set of congruence classes mod m is denoted $\mathbb{Z}/m\mathbb{Z}$. If $\overline{a_1}, ..., \overline{a_n}$ form a complete set of congruence classes mod m, then

$$\{a_1, a_2, ..., a_m\}$$

is called the **complete set of residues mod m**.

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

$$\overline{a+b} = \overline{a} + \overline{b}$$

$$\overline{a \cdot b} = \overline{a} \cdot \overline{b}$$

Proposition 3.12. The set of units in $\mathbb{Z}/m\mathbb{Z}$ is exactly

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

Proof. Suppose $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$.

If $\overline{a}$ is invertible, then there exists $\overline{b} \in \mathbb{Z}/m\mathbb{Z}$ then

$$\overline{b}\overline{a} \equiv 1(m)$$

This happens if and only if there are integer b, n where

$$ba - mn = 1$$

This is equivalent to say

$$gcd(a, b) = 1$$

■

Theorem 3.13 (Bezout's Identity)**.** For integers a, b, then

$$gcd(a, b) \iff m, n \in \mathbb{Z} ma + nb = 1$$

3.3 The Euler ϕ Function

Definition 3.14. For all $n \in \mathbb{Z}_+$, $\phi(n)$ is defined to be the number of integers $1 \leq m \leq n$ coprime to m.

$$\phi(1) = 1$$

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

$$\phi(p^e) = p^e - p^{e-1}, e \geq 1$$

Theorem 3.15. ϕ is a multiplicative function.

Proof. If $(m, n) = 1$, then we wish to show $\phi(mn) = \phi(m)\phi(n)$.

By the Chinese Remainder Theorem, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Then their multiplicative groups are isomorphic, so

$$\phi(mn) = \phi(m)\phi(n)$$

■

Theorem 3.16 (Summatory Function of Euler ϕ Function)**.**

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

Proof. Proof 1 (Very Ingenious Proof):

Consider the n rational numbers,

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

and reduce those to lowest forms so that the numerator and denominator are coprime, then the question is

Given a positive divisor d of n, how many fractionals have d as their denominator, then there's exactly $\phi(d)$ of them.

Conversely, every denominator d that shows up is certainly a divisor of n, so we conclude that

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

Proof 2 (More General Proof):

Note that this is a multiplicative function since ϕ is multiplicative, so it suffices for us to prove this on prime powers.

Given p^k, then

$$\begin{aligned} \sum_{d|p^k} \phi(d) &= \sum_{i=1}^{k} p^k - p^{k-1} \\ &= p^k && \text{Telescope Sum} \end{aligned}$$

■

4 Lecture 4 (February 8)

4.1 Dirichlet Convolution

Definition 4.1 (Dirichlet Convolution)**.** Let f, g are arithmetic functions. Then the Dirichlet Product/Convolution of f and g is

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

Remark 4.2. Note that $(f*g)(n)$ is also an arithmetic function, and note that it is clearly commutative.

Proposition 4.3. The Dirichlet Convolution is associative.

Proof. Let f, g, h be arithmetic functions

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

■

Definition 4.4 (Multiplicative Identity of Dirichlet Convolution)**.** Let $I : \mathbb{Z}_+ \to \{0, 1\}$ be given by $I(n) = 1$ if $n = 1$, $I(n) = 0$, otherwise.

Then clearly for any arithmeitc function I,

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

The other way works similarly.

Lemma 4.5. If f is an arithmetic function with $f(1) \neq 0$, then there exists an arithmetic function g such that

$$f*g = I = g*f$$

Proof. By Commutativity, we only have to show one side.

We will define g recursively as

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

Then we can see that $(f*g)(1) = f(1) \cdot g(1) = 1$.

For all $n > 1$, we have that

$$\begin{aligned}\sum_{d|n} g(d)f(n/d) &= g(n)f(1) + \frac{-1}{f(1)} \sum_{d|n, d<n} g(d)f(n/d) \\ &= \frac{-f(1)}{f(1)} \sum_{d|n, d<n} g(d)f(n/d) + \sum_{d|n, d<n} g(d)f(n/d) \quad \text{Rewrite } g(n) \text{ with its reucrsive definition} \\ &= 0\end{aligned}$$

■

Remark 4.6. This means that the set of all arithmetic functions f where $f(1) \neq 0$ form an Abelian Group with the Dirichlet Convolution as its operation.

4.2 Mobius Function

Definition 4.7. Let $\mu : \mathbb{Z}_+ \to \{-1, 0, 1\}$ be given by

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

Note that we vacuously have that $\mu(1) = 1$.

Lemma 4.8. μ is a multiplicative function.

Proof. Let $m, n \in \mathbb{Z}_+$ with $(m, n) = 1$, then

$$m = p_1^{e_1}...p_k^{e_k}$$
$$n = q_1^{f_1}...q_l^{f_l}$$

If either m or n is not square-free, then clearly

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

Otherwise, suppose both m and n are square-free, then

$$m = p_1...p_k, n = q_1...q_l$$

, all distinct primes. Since $(m, n) = 1$, we also know that $(p_i, q_j) = 1$ for all choices. Then clearly

$$\mu(mn) = (-1)^{k+l} = \mu(m)\mu(n)$$

■

Lemma 4.9. Consider the summatory function of μ, then

$$f(n) = \sum_{d|n} \mu(d) = 0$$

for all $n \geq 2$

Proof. Since μ is multiplicative, then $f(n)$ is multiplicative. Now for any $n \geq 2$, so it suffices for us to check prime powers, indeed,

$$f(p^e) = \mu(1) + \mu(p) + ... + \mu(p^e) = \mu(1) + \mu(p) = 1 - 1 = 0$$

■

Definition 4.10. Let $i : \mathbb{Z}_+ \to \{1\}$ be the constant 1 function.

Lemma 4.11. i the multiplicative inverse of μ:

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

Proof. Clearly $(\mu * i)(1) = \mu(1) \cdot i(1) = 1$.

For $n > 1$, we have that

$$(i * \mu)(n) = \sum_{d|n} \mu(d) = 0$$

by the previous lemma. ■

Remark 4.12 (Summatory Functions as Convolutions)**.** We can turn a summatory function into a Dirichlet product in the sense that if $F(n) = \sum_{d|n} f(d)$, then $F = f * i$.

Remark 4.13. If f, g are multiplicative, then so is $f * g$. The proof is left as an exercise for the reader.

Theorem 4.14 (Mobius Inversion)**.** Let $F(n) = \sum_{d|n} f(d)$, then

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

Proof. We take advantage of the fact that much of this is simplified by the language of abstract algebra since

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

■

Corollary 4.15. If F is the summatory function of f and F is multiplicative, then so is f

Proof. Since Dirichlet Convolution preserves multiplicativity and both F and μ are multiplicative, $F * \mu = f$ is thus multiplicative. ■

Corollary 4.16. This is another way to show that ϕ is multiplicative

Proof. Since $F(n) = \sum_{d|n} \phi(d) = n$ is multiplicative, $\phi = F * \mu$ is multiplicative. ■

4.3 Applications of Mobius Inversion:

Definition 4.17. The n-th cyclotomic polynomial $\Phi_n(x)$ is the unique irreducible polynomial in $\mathbb{Z}[x]$ dividing $x^n - 1$ but does not divide $x^k - 1$ for $k < n$, then we have that

$$\Phi_n(x) = \prod_{1 \le k \le n, gcd(k,n)=1} (x - e^{\frac{2\pi ik}{n}})$$

So in other words, the n-th cyclotomic polynomial is the product of the linear factors with root being the n-th primitive roots of unity.

Proposition 4.18.

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

Proof. By Mobius Inversion, if $G(n) = \prod_{d|n} g(d)$, then

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

Thus, when $G(n) = x^n - 1$, we have that

$$g(n) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$$

, where $\mu(n/d) = 1$ only at $d = n$, so

$$g(n) = x^n - 1$$

Thus, since $G(n) = x^n - 1$, we have that

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

■

Alternative Proof

Proof. The set of roots of $x^n - 1$ form a cyclic group of order n, clearly each root of $\Phi_d(x)$ is also a root of $\Phi_n(x)$. Then intersection of roots of different order is empty, the union of all roots of each order dividing n is the entire set of roots. Thus, the two has to equal. ■

Definition 4.19 (Dynatomic Polynomials)**.** Dynatomic polynomials have as roots periodic points of a polynomial.

Let K be a field, and let $f \in k[x]$ be of deg $d \geq 2$, let $f^n = f \circ ... \circ f$, f composed itself n times.

We say $p \in \overline{K}$ is periodic under f if

$$f^n(p) = p$$

for some n.

Example 4.20. 0 is a period point of $f(x) = x^2 - 1$, since $f(0) = -1$, $f(f(0)) = f(-1) = 0$.

Definition 4.21. If n is the smallest integer such that $f^n(p) = p$, then p has *exact period* n.

Definition 4.22. The n-th dynatomic polynomial of f is

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

and hence

$$\prod_{d|n} \Phi_{f,n}(x) = f^n(x) - x$$

We hope that $\Phi_{f,n}(x)$ have roots that exactly the points of exact period n. This is false

Example 4.23. Let $f(x) = x^2 - 3/4$, then $f(x) - x = (x - 3/2)(x + 1/2)$ has roots $3/2, -1/2$.

Note that $f^2(x) - x = x^4 - 3/2x^2 - x = 3/16 = (x - 3/2)(x + 1/2)$, so we have that

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

But $x = -1/2$ is a fixed point, hence a contradiction.

Remark 4.24. For a degree 2 polynomial, generally it has 2 distinct points of exact period 2 and 2 more points distinct from the two prior that are fixed under f.

Here, the 2 former points have collided into 1 fixed point.

5 Lecture 5 (February 10)

5.1 Linear Congruence:

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 $(a, m)|b$.

The question is how does one find a solution?

Proposition 5.1. The following algorithm would work, given $ax \equiv b \ (mod \ m)$

- 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 then we have that
$$\frac{a'}{d'}x \equiv \frac{b'}{d'} mod(m')$$
- 3) Let $a''x \equiv b'' mod(m')$ be the result so far, we can replace b'' by $b'' + km'$ such that $(a'', b'' + km') > 1$ allows Step 2 to be repeated so that we can find
$$|a'''| < |a''|$$
This process has to terminate since the absolute value of a is decreasing in each step.

Example 5.2. Consider $10x \equiv 6 \ (mod \ 14)$.

Note that $(10, 14) = 2$, so Step 1 gives

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

Step 2 is redundant.

Then, consider the integer $3 + 7k$, and we want to fjnd one divisible by 5, so clearly $3 + 7 \cdot 1 = 10$ works, so

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

So we have that

$$x \equiv 2 \ mod \ 7$$

5.2 Simultaneous Congruence

Theorem 5.3 (Chinese Remainder Theorem - Classical Version)**.** Suppose that $m = m_1 m_2 ... m_t$ and that $(m_i, m_j) = 1$ for all $i \neq j$, let $b_1, ..., b_t$ be integers and consider the system of congruences

$$x \equiv b_1 mod(m_1)$$

$$\vdots$$

$$x \equiv b_t mod(m_t)$$

Then this system always has solutions, and any two solutions differ by a multiple of m.

Proof. ■

Remark 5.4 (Chinese Remainder Theorem - Modern Version)**.** Let $\psi : \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_k\mathbb{Z}$ be given by

$$\psi(n) = (n \ mod(m_1), ..., n \ mod(m_t)$$

Then the CRT tells us that ψ is surjective. Moreover, the kernel of ψ is clearly $m\mathbb{Z}$. Then by the first isomorphism theorem, we have that

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_k\mathbb{Z}$$

It follows that if $U(m)$ is the unit group of $\mathbb{Z}/m\mathbb{Z}$, then

$$U(m) \cong U(m_1) \times ... \times U(m_t)$$

5.3 Structure of Unit Groups

Theorem 5.5 (Lagrange's Theorem)**.** If G is a finite group, then for every subgroup H of G, $|H|$ divides $|G|$.

Corollary 5.6. If G is a finite group of order n and $a \in G$, then $a^n = e$, where e is the identity element.

Theorem 5.7 (Euler's Theorem)**.** For any $a \in \mathbb{Z}$ with $(a, m) = 1$, we have

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

Proof. Clearly in $\mathbb{Z}/m\mathbb{Z}$, for any $a \in \mathbb{Z}$ coprime to m, the order of a is $\phi(m)$, then by Lagrange's Theorem we have that

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

■

We present an alternative proof of Euler's Theorem:
(Skip for now)

5.4 Polynomial Training

We will be studying roots of polynomials over $\mathbb{Z}/m\mathbb{Z}$ for various m, especially polynomials of the form $x^d - a$ and the case where $m = p$ is prime. We may also touch on roots in $\overline{\mathbb{F}_p}$

Proposition 5.8. If $p \nmid d$, then the polynomial $x^d - a \in (\mathbb{Z}/p\mathbb{Z})$ $a \neq 0$ has exactly d roots in some extension of $\mathbb{Z}/p\mathbb{Z}$.

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

We will prove the proposition above by consider the following:

Proposition 5.9. A non-zero polynomial $f \in K[x]$ is separable if and only if $gcd(f, f') = 1$

Proof. Suppose that a polynomial $f \in K[x]$ is separable, now suppose they are not coprime, then there exists some gcd $g(x)$ that divides both. Moreover, let r be the root of $g(x)$, then then clearly

$$f(x) = (x - r)h(x)$$

, and $h(x)$ does not have root r since f is separable, so moreover,

$$f'(x) = (x - r)h'(x) + h(x)$$

Since $g(r) = 0$, $f'(x) = h(r) = 0$, but $h(x)$ does not have root r. Hence a contradiction.

Conversely suppose that $gcd(f, f') = 1$, then f being not separable means that it has a root r of multiplicity at least 2, then

$$f(x) = (x - r)^2 h(x)$$

and

$$f'(x) = 2(x - r)h(x) + (x - r)^2 h'(x)$$

clearly also has root r, so their gcd is not 1. Hence a contradiction. ■

Proof of Proposition 1

Proof. Let $K = \mathbb{Z}/m\mathbb{Z}$, then clearly when $p \nmid d$, we have that

$$f(x) = x^d - a, f'(x) = dx^{d-1} \neq 0$$

They don't share any common roots since $a \neq 0$, so they must be separable as they have gcd 1.

If $p|d$, then

$$f'(x) = dx^{d-1} = 0$$

So $gcd(f(x), f'(x)) = gcd(f(x), 0) = f(x)$, so it's not separable. ■

Now the second proposition we will use is (Prop. 4.1.2 from textbook):

Proposition 5.10. If p is a prime, and if $d|p-1$, then the polynomial $x^d - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$ has exactly d roots in $\mathbb{Z}/p\mathbb{Z}$.

Proof. We will use Fermat's Little Theorem which is Euler's Theorem in the case $m = p$ is a prime.

Indeed, using Fermat's little theorem, every non-zero element if $\mathbb{Z}/p\mathbb{Z}$ is a root to

$$x^{p-1} - 1 = 0$$

So $x^{p-1} - 1$ is separable. Since $d|p-1$, we have that $(x^d - 1)|(x^{p-1} - 1)$, so all roots of $x^d - 1$ are separable and there's d of them in $\mathbb{Z}/p\mathbb{Z}$. ■

Corollary 5.11. $G = (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic

Proof. For $d|p-1$, consider the number of elements of G of order d, which we will denote as $\psi(d)$, then Proposition 2 tells us that

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

Since the roots of $x^d - 1$ for all $d|n$ partitions the roots of $\mathbb{Z}/p\mathbb{Z}$.

We also note that this is the identity function.

Using the Mobius Inversion, we have that since $\psi * i = id$, $\psi = id * \mu$

$$\psi(d) = \sum_{c|d} \mu(c) \cdot d/c$$

We note that the right hand side is just $id * \mu$, and this is just ϕ since $id = \phi * i$ and μ and i are inverses, so we have that

$$\psi(d) = \phi(d)$$

, so we have that $\psi(d) = \phi(d)$ for all $d|p-1$.

In particular, if $p > 2$, then $\psi(p-1) = \phi(p-1) > 1$. So there exists an element of order $p-1$ in G. ■

6 Lecture 6 (February 15th)

Theorem 6.1. Suppose $p \in \mathbb{Z}_+$ is an odd prime, and let $e \geq 1$, then $U(p^c)$ is cyclic, where $U(n)$ denotes the multiplicative group of units modulo to n.

There are 3 steps that we would like to show:

- 1. Pick a primitive root $mod\ p$, call it g (proved last lecture)
- 2. Show that either g or $g+p$ is a primitive root mod p^2.
- 3. If you take any primitive root mod p^2, call it h, then h is also a primitive root mod p^e, for all $e \geq 2$.

Proof of Step 2

Proof. Let g be a primitive root module p, and let d be the order of $g\ mod(p^2)$.

Since $\phi(p^2) = p(p-1)$, that is the order of this multiplicative group, we have that $d|p(p-1)$ by Lagrange's Theorem.

We know by definition of d,

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

so

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

Since g is a primitive root of modulo p, so $(p-1)|d$, so altogehter, either $d = p-1$ or $d = p(p-1)$.

If $d = p(p-1)$, then we are done.

If $d = p-1$, Let $h = g+p$, since h is in the same modulo class as g, h is also a primitive root.

Now clearly $(g+p)^{p-1} \neq 1\ mod(p^2)$, since

$$g^{p-1} \equiv 1(p^2)$$

And using the binomial theorem

$$\begin{aligned} h^{p-1} &= g^{p-1} + (p-1)g^{p-2}p + ... + p^{p-1} \\ &\equiv 1 - pg^{p-2} \end{aligned}$$

Since $p \nmid g$, so pg^{p-2} is not 0.

So the order of $g+p$ has to be $p(p-1)$. ■

Proof of Step 3: A primitive root mod p^2 is a primitive root mod p^e, $e \geq 2$.

Proof. We will prove this with induction on e.

When $e = 1$, then we already proved this in Step 2.

Now suppose our inductive hypothesis is still true until $e = k$, then we wish to show that this is also true for $e = k+1$.

Let d be the order of a primitive root of h from p^e for $mod(p^{e+1})$. Then clearly $d|\phi(p^{e+1}) = p^e(p-1)$.

We also have that $p^{e-1}(p-1)|d$.

Thus, there are only two choices for d.

If $d = p^{e-1}(p-1)$, then we are done.

Otherwise, let $d = p^{e-1}(p-1)$, then we wish to show that

$$h^{p^{e-1}(p-1)} \neq 1 \ (mod\, p^{e+1})$$

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

$$h^{p^{e-2}(p-1)} \neq 1 \ (p^e) \ (*)$$

However, by Euler's Theorem

$$h^{p^{e-2}(p-1)} \equiv 1 \ (p^{e-1}) \ (**)$$

Conbining $(*)$ and $(**)$ gives us that

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

By the Binomial Theorem

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

We note that subsequent terms are all divisible by $p^{3(e-3)} = (p^(e-1))^3$, and hence by p^{e+1} since $e > 2$ as

$$3(e-1) \geq e+1, \forall e \geq 2$$

So we have that

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

It is crucial that p is odd, because as a result we have that

$$k^2 p^{2e-1}(p-1)/2 \text{ is divisible by } p^{e+1}$$

since $2e - 1 \geq e + 1$ for all $e \geq 2$.

Thus,

$$\begin{aligned} h^{p^{e-1}(p-1)} &\equiv 1 + kp^e \ mod(p^{e+1}) \\ &\neq 1 \ mod(p^{e+1}) \end{aligned}$$

Hence a contradiction, so h is a primitive root mod p^{e+1} ■

Remark 6.2. The number of generators for a unit group of modulo p^k for odd prime is just $\phi(\phi(p^k))$. Now, what exactly is $\phi(\phi(p^k))$, this would give us the intuition for the proof above (supposedly).

Theorem 6.3. $U(2^e)$ is cyclic if and only if $e = 1$ or $e = 2$.

Proof. Suppose $U(2^e)$ is cyclic, and assume for the sake of contradiction that $e > 2$.

It suffices to show that the group of units mod(8) is not cyclic, since for any group greater, we can always project it down to $U(8)$, then we see that $U(8)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Conversely, when $e = 1$, $e = 2$, we can verify this. ■

Corollary 6.4. $U(m)$ 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 if and only if $(|G_1|, |G_2|) = 1$.

We first note that $\phi(m)$ is even for all $m \geq 3$, so $U(m)$ is cyclic if and only if $m = p_1^{e_1}...p_k^{e_k}$ and $\phi(p_1)^{e_1}, ..., \phi(p_k)^{e_k}$ are coprime, but this can only happen in the 5 cases given above. ■

7 Lecture 7 (February 17th) - Special Integers:

7.1 Fermat and Mersenne primes

Example 7.1. Many small primes are of the form $2^m \pm 1$ for some natural number m, eg.

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

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

Lemma 7.2. If $2^m + 1$ is prime, then $m = 2^n$ for some $n \geq 0$

Proof. We will prove using the contrapositive. Suppose that m is not a power of 2, then $2^m + 1$ cannot be prime.

Since m is not a power of 2, we can write m as $m = 2^n \cdot q$, for some odd $q > 1$.

Consider the polynomial

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

Clearly $t = -1$ is a root of $f(t)$ as q is odd, so

$$f(t) = (t + 1)g(t)$$

, where $deg(f) = q > 1$.

Consider when $x^m + 1 = f(x^{2n})$, then

$$x^m + 1 = f(x^{2n}) = (x^{2n} + 1)(g(x^{2n}),\ m > 2^n$$

When $x = 2$, then we are done, where $2^{2^n} + 1 \mid 2^m + 1$ ■

Definition 7.3. Numbers of the form $2^{2^n} + 1$ are called *Fermat Numbers*. Fermat Numbers that are also prime are called *Fermat Primes*.

Example 7.4. The first few Fermat Numbers happen to be prime:

$$3, 5, 17, 257, 65537$$

Fermat conjectured that all Fermat Numbers are primes, in fact the 5 numbers shown here were the only numbers he was able to confirm is prime.

Euler managaed to compute $2^{2^5} + 1$ and showed that 641 divides said number.

So far no Fermat Numbers after the 5th Fermat number is prime.

Lemma 7.5. If $m > 1$, $a \geq 2$, and $a^m - 1$ is prime, then $a = 2$, and m has to be prime.

Proof. Suppose m is composite, so $m = n \cdot k$, $1 < n, k < m$. Then we have that

$$a^m - 1 = (a^k)^n - 1 = (a^k - 1)(a^{k(n-1)} + ... + 1)$$

Since a is at least 2, so we have a proper divisor.

Therefore, m has to be prime.

Now if $a > 2$, then $a^m - 1 = (a - 1)(a^{m-1} + ... + 1)$. This factorization is only trivial when $a = 2$. ■

Definition 7.6. 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*.

Remark 7.7. Mersenne was a contemporary of Fermat's. We currently have 51 Mersenne primes, and we are unclear that whether or not there's an infinite number of Mersenne primes.

The largest Mersenne prime known so far (also the largest known prime) is:

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

Definition 7.8. $n \in \mathbb{Z}_+$ is perfect if

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

Proposition 7.9. If $n = 2^{p-1}(2^p - 1)$ where $p \in \mathbb{Z}_+$, p is prime and $2^p - 1$ is prime, then n is perfect.

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

So if $n = 2^{p-1}(2^p - 1)$, then $\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1)$ as they are coprime.

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

Then $\sigma(2^p - 1) = 2^p$ as $2^p - 1$ is prime.

So we have that $\sigma(n) = 2n$, so we are done. ■

Proposition 7.10. If $n \in \mathbb{Z}_+$ is an even perfect number, then $n = 2^{p-1}(2^p - 1)$ where p and $2^p - 1$ are both prime.

Proof. The proof is trivial and is left as an exercise for the reader. ■

Theorem 7.11 (Euclid-Euler Theorem)**.** The even perfect numbers are in bijective correspondence to the Mersenne primes. Specifically, for any Mersenne prime $2^p - 1$, the map

$$2^p - 1 \mapsto 2^{p-1}(2^p - 1)$$

is the desired bijection.

7.2 Pseudoprimes and Carmichael Numbers

Theorem 7.12 (Wilson's Theorem)**.** If p is a prime, then

$$(p-1)! \equiv -1 \ (mod\ p)$$

Proposition 7.13. The converse of Wilson's Theorem is also true: if n is a positive integer such that $n \geq 2$ and

$$(n-1)! \equiv -1 \ (mod\ n) \ \ (*)$$

Then n is prime.

Remark 7.14. You can think of $(*)$ as a rudimentary primality test. It is not a great primality test, but it does give an explicit formula for primes

$$f(n) = \lfloor \frac{n!\ mod(n+1)}{n} \rfloor (n-1) + 2$$

We can also improve the test here.

Recall Fermat's Little Theorem: If $p \in \mathbb{Z}_+$ is prime and $a \in \mathbb{Z}$ is an integers, then

$$a^p \equiv a \ (mod\ p)$$

Thus take $n \in \mathbb{Z}_+$, if

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

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

Example,

$$2^n \not\equiv 2 \ (mod\ n) \implies n \text{ is composite}$$

Example 7.15. The converse of said test is unfortunately not true.

$$2^10 = 1024 \equiv 1 \ (mod \ 341)$$

So $2^{341} = 2^{1034} \cdot 22 \ mod \ 341$.

But $341 = 11 \cdot 31$ and is thus compositie.

We say that 341 is a pseudo-prime base 2.

Definition 7.16. We call n a **pseudo-prime** to the base a if n is composite and happens to satisfy

$$a^n \equiv a \ (mod \ n)$$

Remark 7.17. Sadly, it is not true that every composite n is a pseudo-prime base a for all $a \in \mathbb{Z}$. The smallest composite number that is a pseudo-prime base a for all $a \in \mathbb{Z}$ is 561.

Definition 7.18. A positive integer n is called a **Carmichael number** if n is composite, and

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

Proposition 7.19. If a composite 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 pseudo-prime to base a.

Proof. Suppose n is a pseudo-prime to the base $a_1, a_2, ..., a_r \in (\mathbb{Z}/n\mathbb{Z})^\times$, and suppose there exist a such that (a exists since n is not a Carmichael Number):

$$a^n \equiv a \ (mod \ n)$$

Then for all i,

$$(a \cdot a_i)^{n-1} = a^{n-1}a_i^{n-1} \equiv a^{n-1} \ mod(n) 1 \ mod(n)$$

Where in last inequality holds because if they do equal then $a^n \equiv \ a \ (mod(n))$prime, which gives a contradiction.

This means that n is not a pseudo-prime to the bases

$$a \cdot a_1, a \cdot a_2, ..., a \cdot a_r$$

■

8 Lecture 8 (March 1st)

8.1 Announcement:

Midterm is on March 17th! The plan is for it to be the evenings.

8.2 Power Residues

For this section, $pp.45-46$ of Ireland and Rosen are a good reference.

Definition 8.1. Suppose $m, n \in \mathbb{Z}_+$, $a \in \mathbb{Z}$ such that $(a, m) = 1$, then we say that a is a *nth power residue* modulo m if and only if

$$x^n \equiv a \, mod \, m \, (*)$$

is solvable.

Given such $(*)$, we are interested in two questions.

- 1. Does $(*)$ have a solution?
- 2. If yes, how many solutions are there?

In general this question is very hard to answer, but in some specific cases we do have some answers.

Proposition 8.2 (4.2.1)**.** If $m \in \mathbb{Z}_+$ such that $U(m)$ is cyclic, and $a \in \mathbb{Z}$ is coprime to m, 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 1 - Bezout's Theorem

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

$$a = g^b$$

, which is possible as g is a primitive root.

Suppose that x the hypotehtical solution is that $x = g^y$, then

$$x^n \equiv a \, (mod \, m) \iff g^{ny} \equiv g^b \, (mod \, m)$$

This holds if and only if (ie. unit group lagrange)

$$ny \equiv b \, (mod \, \phi(m))$$

It follows from Bezout's Theorem that this is solvable if and only if $d = (\phi(m), n) | b$.

If there is at least one solution, then there are exactly d solutions.

Now we wish to show that

$$d|b \iff a^{\phi(m)/d} \equiv 1 \, (mod \, m)$$

Suppose that d divides b, then $a^{\phi(m)/d} = g^{b\phi(m)/d}$. Since $d|b$, b/d is an integer, so we have that

$$a^{\phi(m)/d} = (g^{\phi(m)})^{b/d} \equiv 1 \, (mod \, m)$$

Conversely, suppose that

$$a^{\phi(m)/d} \equiv 1 \, (mod \, m) \implies g^{b\phi(m)/d} \equiv 1 \, (mod \, m)$$

So we have that $\phi(m) | b \cdot \phi(m)/d$, so b/d is an integer. ■

Lemma 8.3 (Fundamental Theorem of Finite Cyclic Groups)**.** Let G be a cyclic group of order n, and let H be a subgroup of G of order d. Then $x \in H$ if and only if x^d is the identity if and only if $ord(x)|d$.

Proof. Exercise for the reader. (It's really not that bad, trust me) ■

Theorem 8.4. Let G be a cyclic of order n, suppose k is a positive integer and $a \in G$. Then a is a k-th power in G ie. $a = b^k$ for some $b \in G$ if and only if $a^{n/(k,n)} = e$, the identity element of G, if and only if $x^k = a$ has (n, k) solutions in G.

Proof. Let H be the subgroup of G consisting of k-th powers in G, and let $g \in G$ be such that

$$G = \langle g \rangle$$

Then $H = \{g^{jk} | j \in \mathbb{N}\} = \langle g^k \rangle$.

Since $ord(g^k) = \frac{n}{(k,n)}$, we have that $\#H = \frac{n}{(k,n)}$.

Consider $\phi : G \to G, x \mapsto x^k$, we have that $im(\phi) = H$, erefore we have shown that element is in H if and only if it has to be a $d = \frac{n}{(k,n)}$-th power.

Note that this implies that ϕ is a (k, n)-to-1 mapping, so there are (k, n) number of solutions to a particular element. ■

Proof 2 - Cyclic Group Interpretation

Proof. Applying the theorem above immediately gives us the proposition above. ■

Theorem 8.5. Write $m = 2^e p_1^{e_1} ... p_r^{e_r}$, p_i pairwise distinct odd primes.

Then $x^n \equiv a \; mod \; m$, $(a, m) = 1$ is solvable if and only if the system

$$x^n \equiv a \; mod \; 2^e, x^n \equiv a \; mod \; p_1^{e_1}, ..., x^n \equiv a \; mod \; p_r^{e_r}$$

is solvable.

Use Chinese Remainder Theorem

Remark 8.6. We have that $U(p_i^{e_i}), U(2), u(4)$ are all cyclic, hence our prior discussion can be applied to those. Then we are left with the question of

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

Proposition 8.7 (4.2.2)**.** 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 always unique.

If n is even, a solution exists if and only if $a \equiv 1 \; (mod \; 4)$ and $a^{2^{(e-2)/d}} = 1 \; (mod \; 2^e)$ where $d = (n, 2^{e-2})$.

When a solution exists, there are exactly $2d$ solutions.

Proof. Exercise to come. ■

8.3 Quadratic Residues

Things are a lot nicer in Quadratic Residues!

Definition 8.8. Let $a \in \mathbb{Z}$, $m \in \mathbb{Z}_+$, $(a, m) = 1$. We say that a is a *quadratic residue* modulo m if the congruence

$$x^2 \equiv a \; (mod \; m) \; (*)$$

has a solution.

If $(*)$ does not have a solution, then a is referred to as a (quadratic) *non-residue*.

A couple of blackboxes here that are special cases of Proposition 4.2.3 and 4.2.4 in the textbook.

Proposition 8.9 (Quadratic Residue on Odd Primes)**.** Let $p \in \mathbb{Z}_+$ be an odd prime, and suppose that $a \in \mathbb{Z}$ that is not divisible by p, then

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

is solvable if and only if

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

is solvable for all $e \geq 1$.

Proposition 8.10 (Quadratic Residue on Powers of 2)**.** Suppose that $a \in \mathbb{Z}$ is odd. Then

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

is solvable if and only if

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

is solvable for all $e \geq 3$.

Proposition 8.11 (5.1.1)**.** Suppose $m = 2^e p_1^{e_1} ... p_r^{e_r}$ be the prime factorization of $m \in \mathbb{Z}_+$, and suppose $(a, m) = 1$.

Then,

$$x^2 \equiv a \; (mod \; m) \; (*)$$

is solvable if and only if three conditions are satisfied

- a) If $e = 2$, then $a \equiv 1 \; (mod \; 4)$
- b) If $e \geq 2$, then $a \equiv 1 \; (mod \; 8)$
- c) For each i, we have that
$$a^{(p_i - 1)/2} \equiv 1 \; (mod \; p_i)$$

Proof. Sunzi's Theorem tells us that $(*)$ is solvable if and only if $x^2 \equiv a(2^e)$, ..., $x^2 \equiv a(p_r^{e_r})$ are all solvable.

Consider $x^2 \equiv a \; mod \; (2^e)$,

1 is the only quadratic residue mod 4, and 1 is the only quadratic residue mod 8.

On the other hand, our blackbox gives that $x^2 \equiv 8$ is solvable if and only if $x^2 \equiv a \; mod(2^e)$ is solvable for all $e \geq 3$.

So we are done with (a) and (b).

For (c), consider $x^2 \equiv a \; (mod \; p_i^{e_i})$. Proposition 4.2.1 gives that $x^2 \equiv a \; mod \; p_i$ is solvable if and only if $a^{\phi(m)/d} \equiv 1 \; (mod \; m)$, since $\phi(m)/d = (p_i - 1)/2$, we have that

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

Then using the other black box, we know this is solvable if and only if solvable to an arbitrary power of p_i ■

Remark 8.12. Studying Quadratic Congruences amounts to studying them modulo primes.

8.4 The Legendre Symbol

Let p be an odd prime, and let $a \in \mathbb{Z}$.

Definition 8.13 (The Legendre Symbol)**.**

$$(\frac{a}{p}) = \begin{cases} 1, \text{ if a is a quadratic residue mod p} \\ 0, \text{ p divide a} \\ -1, \text{ otherwise (ie. dealing with quadratic non-residues)} \end{cases}$$

The symbol $(\frac{p}{q})$ is called the Legendre symbol.

Proposition 8.14 (5.1.2)**.** We have the parts:

- (a) $(\frac{a}{p}) = a^{(p-1)/2} \; mod \; p$ (Euler's Criterion)
- (b) $(\frac{ab}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p})$, so the Legendre Symbol is completely multiplicative
- (c) If $a \equiv b \; (mod \; p)$, then $(\frac{a}{p}) = (\frac{b}{p})$

9 Lecture 9 - March 3rd

9.1 Quadratic Residues Continued; Quadratic Reciprocity

Proof of Proposition 5.1.2 last lecture

Proof. Part (c) is clearly obvious.

For (a), WLOG a is not divisible by p, then by Fermat's Little Theorem

$$a^{p-1} \equiv 1 \; mod \; p$$

Since $p-1$ is even this is the same as saying

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

Since $\mathbb{Z}/p\mathbb{Z}$ is an integral domain, we have that

$$a^{(p-1)/2} \equiv \pm 1 \; (mod \; p)$$

We know from last lecture that

$$a^{(p-1)/2} \equiv 1 \; (mod \; p) \iff a \text{ is a quadratic residue mod p}$$

For (b), Part (a) tells us

$$(\frac{ab}{p}) \cong (ab)^{(p-1)/2} \equiv a^{(p-1)/2}b^{(p-1)/2} = (\frac{a}{p})(\frac{b}{p})$$

■

Corollary 9.1. There are some immediate corollaries to the proposition above:

- 1) There are exactly $\frac{p-1}{2}$ quadratic residues modulo p and $\frac{p-1}{2}$ quadratic non-residues modulo p. (Just realize them as roots of $x^{(p-1)/2}-1$
- 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. (We also note that this means the quadratic residues form a group)
- 3) If g is a primitive root modulo p, then
$$(\frac{g^i}{p}) = (-1)^i$$
This follows directly from the fact that a primitive root is not a quadratic residue and multiplicativity
- 4) $(\frac{-1}{p}) = (-1)^{(p-1)/2}$. This is called the "First Supplemental Law of Quadratic Reciprocity"

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

Definition 9.2. For p a positive odd prime, the set

$$S = \{-\frac{(p-1)}{2}, -\frac{(p-3)}{2}, ..., -1, 1, 2, ..., \frac{p-1}{2}\}$$

is called the *set of least residues mod p*. (We skipped 0).

Let $a \in \mathbb{Z}$ such that $p \nmid a$. Let μ be the number of negative least residues of the integers $a, 2a, ..., (\frac{p-1}{2})a$.

(eg. if $p=7$ and $a=4$, then $\frac{p-1}{2}=3$ and $1\cdot 4, 2\cdot 4, 3\cdot 4 \equiv -3, 1, -2 \; (mod \; 7)$. Thus $\mu = 2$ since there are 2 negatives.)

Lemma 9.3 (Gauss's Lemma)**.** Let $p \in \mathbb{Z}_+$ be an odd prime, and let $a \in \mathbb{Z}$ such that $p \nmid a$. Then

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

Proof. It is convenient for us to write

$$P = \{1, 2, ..., \frac{p-1}{2}\}, N = \{-1, -2, ..., \frac{-(p-1)}{2}\}$$

Then $\mu = |aP \cap N|$ - ie. how many elements of P are modulo equivalent to something in N.

If $x, y \in P$ with $x \neq y$, then $ax \neq \pm ay \; mod \; p$. For otherwise,

$$x = \pm y \; mod \; p$$

, which is impossible since x and y are distinct elements of P. Thus $aP = \{e_i \cdot i | i \in 1 : (p-1)/2\}$, for some $e_i = \pm 1$.

Now we mimic the elementary proof of Euler's Theorem

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

The factorials are units then we have that

$$a^{(p-1)/2} \equiv \prod_{i=1}^{(p-1)/2} e_i = (-1)^{\mu}$$

, since $\mu = |aP \cap N|$ Applying Euler's Criterion finishes the proof. ■

Proposition 9.4 (Second Supplemental Law of Quadratic Reciprocity (5.1.3))**.** For p a positive odd prime,

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

, we note that intuition comes from

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

We note that $\frac{(p^2-1)}{8} = \frac{p+1}{2} \cdot \frac{p-1}{4}$ means one of them is divisible by 2 and not by 4 and the other is divisble by 4.

It follows that

$$(\frac{2}{p}) = \begin{cases} 1, \text{ when } p = \pm 1 \; mod \; 8 \\ 01, \text{ when } p = \pm 3 \; mod \; 8 \end{cases}$$

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

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

First suppose that $p \equiv 1 \; mod \; 4$, then $\frac{p-1}{2}$ is even, so in fact

$$2P = \{2, 4, ..., \frac{p-1}{2}, \frac{p+3}{2}, ..., p-1\}$$

All elements starting at $\frac{p+3}{2}$ are in N, that's exactly $\frac{p-1}{4}$ in N. And the first $\frac{p-1}{4}$ elements are in P.

So we conclude that $\mu = \frac{p-1}{4}$, so Gauss's Lemma gives us that

$$(\frac{2}{p}) = (-1)^{(p-1)/4}$$

Since $p \equiv 1 \ mod \ 4$, then $(p+1)/2$ is odd, and so we have that

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

Now suppose $p \equiv 3 \ mod \ 4$, then we have that

$$2P = \{2, 4, ..., \frac{p-3}{2}, \frac{p+1}{2}, ..., p-1\}$$

, since $\frac{p-1}{2}$ is odd. The first $\frac{p-3}{4}$ elements are in P and the last $\frac{p+1}{4}$ elements are in N, so we have that

$$(\frac{2}{p}) = (-1)^{(p+1)/4}$$

Since $(p-1)/2$ is odd, this means that

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

■

Theorem 9.5 (The Law of Quadratic Reciprocity)**.** Let $p, q \in \mathbb{Z}_+$ be distinct odd primes. Then

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

In other words, $(\frac{p}{q}) = (\frac{q}{p})$ if and only if at least one of p, q is congruent to $1 \ mod \ 4$.

Example 9.6. Which odd primes $p \in \mathbb{Z}_+$ have 3 as a quadratic residue?

Suppose $p \equiv 1(4)$. Then,

$$(\frac{3}{p}) = (\frac{p}{3}) = \begin{cases} 1 \text{ if } p \equiv 1(3) \\ -1 \text{ if } p \equiv 1(4) \end{cases}$$

Thus $p \equiv 1(12)$ gives $(\frac{3}{p}) = 1$ and $p \equiv 5(12)$ (this corresonds to 1(4) and -1(3)) gives $(\frac{3}{p}) \equiv -1$. 5 and 12 came from the CRT.

Now suppose $p \equiv 3 \ mod \ 4$, then

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

Altogether, $p \equiv 11 \ mod \ 12$ gives $(\frac{3}{p}) = 1$, and $p \equiv 7 \ mod \ 12$ gives $(\frac{3}{p}) = -1$, 11 and 7 came from the CRT.

We conclude that $(\frac{3}{p}) = 1$ if and only if $p = \pm 1 \ (mod \ 12)$

10 Lecture March 8th

10.1 Proof of Quadratic Reciprocity

Example 10.1. Determine if 219 is a quadratic residue modulo 383 (which is infact a prime number).

Since 383 is prime, this is the same as asking

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

, we note that both 3 is $3 \ mod 4$ and 73 is $1 \ mod 4$, so

$$= -(\frac{383}{3})(\frac{383}{73}) = -(\frac{2}{3}) \cdot (\frac{18}{73}) = (\frac{18}{73}) = (\frac{2}{23})$$

By the second supplemental law of quadratic residues, we have that

$$(\frac{2}{23}) = 1$$

Remark 10.2. Note that we must factor the top argument before beginning to flip using Quadratic Reciprocity.

Now we will finally prove Quadratic Reciprocity. We present a proof using Gauss's Lemma.

Theorem 10.3. For $p, q \in \mathbb{Z}_+$, distinct odd primes,

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Proof. Let $P = \{1, 2, ..., \frac{p-1}{2}\}$, $N = -P - \{-1, -2, ..., -\frac{p-1}{2}\}$, $Q = \{1, 2, ..., \frac{q-1}{2}\}$.

Write $\overline{P}, \overline{N}$ for $P \ mod \ p$ and $N \ mod \ p$ respectively, so that Gauss's Lemma gives us that

$$(\frac{q}{p}) = (-1)^{\mu}$$

, where $\mu = |q\overline{P} \cap \overline{N}|$.

In other words, μ is exactly the number of $x \in P$ such that

$$qx \equiv n \ mod \ p$$

, for some $n \in N$, and hence this μ is the number of $x \in P$ such that for some $y \in \mathbb{Z}$, (n has to lie strictly between $-p/2$ and 0)

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

We now specify more precisely which y can possibly satisfy this condition for some $x \in P$.

Solving these two inequalities for y gives

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

On the other hand, since $x \leq \frac{p-1}{2}$, for all $x \in P$, this means gives

$$y < \frac{qx}{p} + \frac{1}{2} \leq \frac{q(p-1)}{2p} + \frac{1}{2}$$

We note that $\frac{p-1}{p} < 1$, so

$$y < \frac{q(p-1)}{2p} + \frac{1}{2} < \frac{q}{2} + \frac{1}{2} = \frac{q+1}{2}$$

Thus we have that ($0 < y$ is implicit)

$$0 < y < \frac{q-1}{2} \ (*)$$

Since y is an integer, we know that $y \in Q = \{1, 2, ..., \frac{q-1}{2}\}$.

Thus, we've shown that μ is the number of ordered pairs

$$(x, y) \in P \times Q, \ -\frac{p}{2} < qx - py < 0$$

Now we will switch the roles of p and q, then we also have that

$$(\frac{p}{q}) = (-1)^n$$

, where n is the number of pairs

$$(y, x) \in Q \times P, \ -\frac{q}{2} < py - qx < 0$$

, where we note the condition above is exactly the number of pairs

$$(x, y) \in P \times Q, 0 < qx - py < \frac{q}{2}$$

Then we see that

$$(\frac{p}{q}) \cdot (\frac{q}{p}) = (-1)^{\mu+n}$$

, so our question is, what is $\mu + n$.

We note that the two conditions for μ and n are mutually exclusive! So the number of $(x, y) \in P \times Q$ such that

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

is exactly $\mu + n$.

We note that it is impossible for $qx - py = 0$ since if $qx = py$ then that would imply x is at least q and y is at least p, but $Q < q$ and $P < p$, so our condition above simplifies to

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

, and the number of (x, y) satisfying this is still $P \times Q$.

Graphically, we are looking at the ordered pairs in a rectangular box $R = [1, p - 1/2] \times [1, q - 1/2]$ bounded by the two lines

$$qx - py = -p/2, qx - py = q/2$$

.

So we are counting the number of lattice points in R bounded by the two lines, we will indicate A, B as the complement of the shaded region in R.

If α is the number of integer points in A and β be the number of integers points in B, then we have that

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

As long as we show that the equation above agrees modulo 2, then we are good, so we want to show that $\alpha + \beta$ is 0 modulo 2.

We will do this by showing that $\alpha = \beta$.

Let ρ be the rotation given by

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

, we note that $(\frac{p+1}{4}, \frac{q+1}{4})$ is the center of this rotation as they are fixed, and we claim that $\rho(R) = R$ as in that the rotation maps R to itself, specifically $\rho(A) = B$, $\rho(B) = A$.

To do the last part, let $\rho(x, y) = (x', y')$, one need to check

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

We omit the step, and this implies that

$$\rho(A) = B, \rho(B) = A$$

Clearly ρ is a bijection and it preserves lattice points, so we have that $\alpha = \beta$.

Thus, we have that

$$\mu + n = \frac{(p-1)(q-1)}{4} - 2\alpha$$

So we have that

$$\mu + n \equiv \frac{(p-1)(q-1)}{4} \ (mod\ 2)$$

■

10.2 Jacobi Symbol

The Jacobi symbol generalizes the Legendre Symbol.

Definition 10.4. Let b be an odd positive integer, and let a be any integer. Write

$$b = p_1 p_2 ... p_m$$

, where $p_1, ..., p_n$ are primes (not necessarily distinct).

The symbol $(\frac{a}{b})$ defined by

$$(\frac{a}{b}) = (\frac{a}{p_1})...(\frac{a}{p_m})$$

is called the Jacobi Symbol. (The Legendre Symbol is a special case when b is prime)

Proposition 10.5 (Basic Properties of Jacobi Symbol)**.** A few basic properties

- $(\frac{a_1 a_2}{b}) = (\frac{a_1}{b})(\frac{a_2}{b})$ (Follows from Multiplicativity of the Legendre Symbol)
- $(\frac{a}{b_1 b_2} = (\frac{a}{b_1})(\frac{a}{b_2}))$ (Trivial from Definition)

So the Jacobi Symbol is totally multiplicative on the top and bottom.

Example 10.6. Big Warning:

$$(\frac{a}{b}) = 1 \not\iff \text{ a is quadratic residue modulo b}$$

For example $(2/15) = 1$, but 2 is not a quadratic residue modulo 15.

However,

$$(\frac{a}{b}) = -1 \implies \text{ a is a non-residue modulo b}$$

This follows from the fact that $(a/p_i) = -1$ for at least one of the prime factors of b.

Proposition 10.7 (5.2.2 of the Text)**.** Let $b \in \mathbb{Z}_+$ be odd, then

- a) $(\frac{-1}{b}) = (-1)^{(b-1)/2}$
- b) $(\frac{2}{b}) = (-1)^{(b^2-1)/8}$
- If $a, b \in \mathbb{Z}_+$ are odd, then

$$(\frac{a}{b}) \cdot (\frac{b}{a}) = (-1)^{\frac{(a-1)(b-1)}{4}}$$

11 Lecture March 10th

11.1 Recall:

Definition 11.1. Let $b \in \mathbb{Z}_+$ be odd, and let $a \in \mathbb{Z}$. Write $b = p_1 p_2 ... p_m$, where p_i are primes (not necessarily distinct). Then the symbol $(\frac{a}{b})$ is defined by

$$(\frac{a}{b}) = (\frac{a}{p_1})...(\frac{a}{p_m})$$

is called the Jacobi symbol.

Evidently this generalizes the Legendre Symbol.

Proposition 11.2 (Basic Properties:)**.** We have that the Jacobi symbol is completely multiplicative on top and bottom:

- i) $(\frac{a_1 a_2}{b}) = (\frac{a_1}{b})(\frac{a_2}{b})$
- ii) $(\frac{a}{b_1 b_2}) = (\frac{a}{b_1})(\frac{a}{b_2})$

We note that $(\frac{a}{b}) = -1 \implies a$ is not QR modulo b, but it equaling 1 does not necessarily imply a is a QR modulo b.

11.2 Main Lecture:

Lemma 11.3. Let $r, s \in \mathbb{Z}_+$ be odd, then

- (a) $\frac{rs-1}{2} = \frac{r-1}{2} + \frac{s-1}{2} \; mod \; 2$
- (b) $\frac{r^2 s^2 - 1}{8} = \frac{r^2-1}{8} + \frac{s^2-1}{8} \; mod \; 2$

Note that in (b), $r^2 - 1$ is divisble by 8 since $r^2 - 1 = (r-1)(r+1)$, one of them has to be 0 mod 4, the other is 2 mod 4.

Proof. Clearly $(r-1)(s-1)$ is divisble by 4, so

$$(r-1)(s-1) \equiv 0 \; mod \; 4$$

Hence $rs - 1 = (r-1)(s-1) + r + s - 2 = r + s - 2 \; mod \; 4$, so

$$rs - 1 \equiv (r-1) + (s-1) \; mod 4$$

Dividing by 2 on all sides by 4 gives us the desired claim for (a).

As for (b), the product $(r^2-1)(s^2-1) \equiv 0 \; mod \; 16$ since each is divisble by 4, so

$$r^2 s^2 - 1 = (r^2-1)(s^2-1) + r^2 + s^2 - 2 \; mod \; 16$$

So we have that

$$r^2 s^2 - 1 = (r^2-1) + (s^2-1) \; mod \; 16$$

Then just divide everything by 8 gives (b). ■

Corollary 11.4. Let $r_1, r_2, ..., r_m \in \mathbb{Z}_+$ be positive odd integers. Then,

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

This can be done just by using induction and the previous lemma, and we will use this corollary to prove our reciprocity law.

Theorem 11.5 (Reciprocity Laws for Legendre Symbols)**.** Let $b \in \mathbb{Z}_+$ be odd, then

- a) $(\frac{-1}{b}) = (-1)^{(b-1)/2}$
- b) $(\frac{2}{b}) = (-1)^{(b^2-1)/8}$
- If $a, b \in \mathbb{Z}_+$ are odd, then

$$(\frac{a}{b}) \cdot (\frac{b}{a}) = (-1)^{\frac{(a-1)(b-1)}{4}}$$

Proof. (a) and (b) follows from the corollary and the first and second supplemental law of quadratic reciprocity, just factor b out by its odd prime factors.

For (c), let $a = q_1...q_l$, let $b = p_1...p_m$, then

$$(\frac{a}{b}) \cdot (\frac{b}{a}) = \prod_i \prod_j (\frac{q_i}{p_j})(\frac{p_j}{q_i}) = (-1)^{\sum_i \sum_j (\frac{q_i-1}{2}) \cdot (\frac{p_i-1}{2})}$$

Then we see that applying the Fubini's Theorem and Corollary gives

$$\sum_i \sum_j (\frac{q_i-1}{2}) \cdot (\frac{p_i-1}{2}) \equiv (\sum_i \frac{q_i-1}{2})(\sum_j \frac{p_j-1}{2}) \equiv (\frac{a-1}{2})(\frac{b-1}{2})$$

So we conclude that

$$(\frac{a}{b}) \cdot (\frac{b}{a}) = (-1)^{\frac{(a-1)(b-1)}{4}}$$

■

Example 11.6 (Computing with the Jacobi Symbol)**.** Recall the earlier example $(\frac{219}{383})$, with the Jacobi Symbol, we can flip immediately, so

$$(\frac{219}{383}) = -(\frac{383}{219}) = -(\frac{164}{219}) = -(\frac{4}{219})(\frac{41}{219}) = -(\frac{41}{219}) = -(\frac{219}{41}) = -(\frac{14}{41})$$
$$= -(\frac{2}{41})(\frac{7}{41}) = -(\frac{7}{41}) = -(\frac{41}{7}) = -(\frac{-1}{7}) = -1(-1) = 1$$

11.3 Number Fields

Definition 11.7. A complex number α is called algebraic if it is algebraic over $\mathbb{Q}$, ie. it is the roots of a non-zero rational polynomial.

Proposition 11.8. We denote the set of algebraic numbers as $\overline{\mathbb{Q}}$, and this is infact a subfield of $\mathbb{C}$.

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

So supose $\alpha, \beta \in \overline{Q}$, then this characterization tells us that $\mathbb{Q}(\alpha)/\mathbb{Q}$ and $\mathbb{Q}(\beta)/\mathbb{Q}$ are finite, and $\mathbb{Q}(a, b)$ is no more than the product of the two extension degress here, so $\mathbb{Q}(a, b)/\mathbb{Q}$ is finite, so $a + b$, $a - b$, ab, ab^{-1} (if $b \neq 0$) are all algebraic. ■

Definition 11.9. 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 $K \subset \overline{\mathbb{Q}}$. By the definition of a finite extension, every number field has the form

$$K = \mathbb{Q}(a_1, ..., a_n), a_1, ..., a_n \in \overline{\mathbb{Q}}$$

However, the primitive element theorem actually tells us there exist some $\gamma \in \overline{Q}$ such that

$$K = \mathbb{Q}(\gamma)$$

Remark 11.10 (Sketch of Proof for Primitive Element Theorem)**.** Inductively, we note that it suffices to show that if

$$K = K_1(a, b) \implies K = K_1(\theta), \theta \in \overline{\mathbb{Q}}$$

Supose the minimal polynomials over $\mathbb{Q}$ of α and β respectively are (facotring over $\mathbb{C}$)

$$(t - a_1)...(t - a_n), a_1 = a$$

$$(t - b_1)...(t - b_m), b_1 = b$$

Irreducible polynomials in characteristic 0 are separable!!!! So we have that all the roots here are distinct.

Hence for each i and each $k \neq 1$, there exist at most $x \in K_1$ such that $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$.

There are only finitely many of these equations, since K_1 is infinite, we can choose some non-zero $c \in K_1$ such that

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

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

Define $\theta = \alpha + c\beta$, then we claim this θ is a primitive element, where $K_1(\alpha, \beta) = K_1(\theta)$

Proof is on page 39 of Stewart and TRall!

12 Lecture March 15th

12.1 Recall: Number Fields

Definition 12.1. A complex number α is called algebraic if it's algebraic over $\mathbb{Q}$.

Proposition 12.2. The set $\overline{\mathbb{Q}}$ form a subfield of the complex numbers.

Definition 12.3. A number field is a subfield k of $\mathbb{C}$ whose degree over $\mathbb{Q}$ is finite. Using the Primitive Element Theorem, k being a number field implies $k = \mathbb{Q}(\alpha)$ for some $\alpha \in \overline{\mathbb{Q}}$, they are actually equivalent definitions.

Remark 12.4. Crux of the proof of Primitive Element Theorem: Suppose $K = K_1(\alpha, \beta)$, then $K = K_1(\theta)$, and we can find θ as a function of α and β.

Write the minimal polynomial of α, β over k_1:

$$(t - a_1)...(t - a_n), a_i \in \overline{\mathbb{Q}}, a_1 = \alpha$$

$$(t - b_1)...(t - b_m), b_i \in \overline{\mathbb{Q}}, b_1 = \beta$$

Irreducible polynomials in characteristic zero are separable, so we have that $a_1, ..., a_n$ are distinct, and $b_1, ..., b_m$ are distinct.

Hence for each i and each $k \neq 1$, there exist at most one $x \in K$ such that

$$a_i + xb_k = a_1 + xb_1, ie. x = (a_i - \alpha)(b_1 - b_k)^{-1}$$

Since there are only finitely many of these equations, we can choose some non-zero $c \in k_1$ such that

$$a_i + cb_k \neq a_1 + cb_1, \forall 1 \leq i \leq n, 2 \leq k \leq m$$

Define $\theta = \alpha + c\beta$, then we claim that

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

This part is done in Ireland and Stewart.

Example 12.5 (Page 35)**.** The Primitive Element Theorem actually gives us a way to find the primitive element. For example, take $K = \mathbb{Q}(\sqrt{2}, 5^{1/3})$, and let $\alpha_1 = \sqrt{2}, \beta_1 = 5^{1/3}$.

We have that $\alpha_2 = -\sqrt{2}$, $\beta_2 = \zeta_3 5^{1/3}$, $\beta_3 = \zeta_3^3 5^{1/3}$, where $\zeta_3 = e^{2\pi i/3}$.

Note that we can take $c = 1$, and it has the property that

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1, 1 \leq i \leq 2, 2 \leq k \leq 3$$

SInce LHS is not real and RHS is always real.

SO we can take

$$\theta = \sqrt{2} + 5^{1/3}$$

So we have that

$$\mathbb{Q}(\sqrt{2}, 5^{1/3}) = \mathbb{Q}(\sqrt{2} + 5^{1/3})$$

12.2 Conjugates of algebraic numbers

The embeddings of a number field in $\mathbb{C}$ play a fundamental role in Number Theory.

Theorem 12.6 (Pg. 40)**.** Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. Then there exists exactly n distinct field embeddings of K into $\mathbb{C}$. (Label these $\sigma_1, ..., \sigma_n : K \to \mathbb{C}$).

Moreover, $\sigma_i(\theta)$ are the zeroes in $\mathbb{C}$ of the minimal polynomial of $\mathbb{Q}(\theta)$ over $\mathbb{Q}$.

Proof. Suppose $\sigma : K \to \mathbb{C}$ is an embedding, then σ has to fix $\mathbb{Q}$ (becuse it sends 1 to 1), so field automorphisms permutes the roots of the minimal polynomial, so $\sigma(\theta)$ is a root of the minimal polynomial over θ over $\mathbb{Q}$.

(We note that if two field isomorphism agrees on θ, they are the same isomorphism, so it is injective).

Now conversely, suppose I have two field automorphisms that sends θ to the same root, then we wish to show that they are the same field automorphism.

Indeed, from 1540 we have a unique field isomorphism (so injective)

$$\mathbb{Q}(\theta) \cong \mathbb{Q}(\theta_i), \theta \mapsto \theta_i$$

THis isomorphism comes from (1540 - Proposition 8.6 from Silverman)

$$\mathbb{Q}(\theta) \cong \frac{\mathbb{Q}[x]}{(f)}, \mathbb{Q}(\theta_i) \cong \frac{\mathbb{Q}[x]}{(f)}$$

So there's a biection between the roots of f and the embeddings of K into $\mathbb{C}$. ■

12.3 Discriminant of bases, Vandermount determinant

Definition 12.7. Let $K = \mathbb{Q}(\theta)$ be a number field of degree n, and let $\{\alpha_1, ..., \alpha_n\}$ be a basis of K as a vector space over $\mathbb{Q}$. Let $\sigma_i : K \to \mathbb{C}$, $1 \leq i \leq n$ be embeddings of K into $\mathbb{C}$.

Then, the **discriminant** of $\{\alpha_1, ..., \alpha_n\}$ is denoted as

$$\Delta[\alpha_1, ..., \alpha_n] = det(\sigma_i(\alpha_j))^2 = det \begin{bmatrix} \sigma_1(\alpha_1) & ... & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & ... & \sigma_n(\alpha_n) \end{bmatrix}$$

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

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

, where $det(C_{ik}) \neq 0$ since it's a map from basis to basis.

Proposition 12.8. The discriminant perserves linear transformation in the sense that, ie

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

Proof. Exercise! ■

Definition 12.9. A *Vandermount Matrix* is a matrix of the following form:

$$V = \begin{bmatrix} 1 & t_1 & ... & t_1^{n-1} \\ 1 & t_2 & ... & t_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & t_n & ... & t_n^{n-1} \end{bmatrix}$$

Proposition 12.10. Then the determinant of V is

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

Theorem 12.11 (Pg. 42)**.** The discriminant of any basis for $K = \mathbb{Q}(\theta)$ is rational and non-zero.

Proof. The most natural choice of basis is $1, \theta, ..., \theta^{n-1}$, it suffices for us to prove that this basis is rational and non-zero, since $(det(C_{ik})^2$ is a non-zero rational numbers.

Write $\theta = \theta_1, \theta_1, ..., \theta_n$ for the conjugates of θ_1 (ie. other roots of the minimal polynomial associated to θ).

Then we have that

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

Using a general observation, we note that we are calculating the determinant of a Vandermount Matrix, where in particular

$$(det(\theta_i^j))^2 = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2 = disc(minpoly_{\mathbb{Q}}(\theta))$$

We note that $disc(minpoly_{\mathbb{Q}}(\theta))$ is surjective on $\mathbb{Q}^\times$, so we are done. ■

13 Lecture March 22nd

13.1 Discriminants of bases, Vandermonde determinants

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

The discriminant of $\{\alpha_1, ..., \alpha_n\}$ is

$$\Delta[\alpha_1, ..., \alpha_n] = det(\begin{bmatrix} \sigma_1(\alpha_1) & ... & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & ... & \sigma_n(\alpha_n) \end{bmatrix})^2$$

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

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

, where $det(C_{ik}) \neq 0$.

From the homework, we will prove that

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

Definition 13.1. A square Vandermonde matrix is a matrix of the form

$$V = \begin{bmatrix} 1 & t_1 & ... & t_1^{n-1} \\ 1 & t_2 & ... & t_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & t_n & ... & t_n^{n-1} \end{bmatrix}$$

Proposition 13.2. The determinant of V is

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

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

On one hand we know that $det(V) = 0$ when $t_i = t_j$ for some $i \neq j$ since the rows won't be linearly independent, $det(V)$ (as a polynomial in $t_1, ..., t_n$) is disivible by $(t_j - t_i)$, $i < j$ since they are roots of the polynomial.

The above argument works if we use the Factor Theorem by treating this as a polynomial in terms of t_i and treating everything else as constants.

What is the degree of this polynomial??

Well, inductively we can show that the degree of this polynomial is the triangle numbers, so for $n \times n$ matrix V, it is the $n-1$-th triangle number

$$deg(det(V)) = \sum_{i=1}^{n-1} i = \frac{(n-1)n}{2}$$

The degree of D is also $\frac{(n-1)n}{2}$, since by combinatorics we have $\binom{n}{2} = \frac{(n-1)n}{2}$ choices for i and j.

Hence, $det(V)$ is a scalar multiple of D. Now both terms are monomial terms with either 1 or -1 as coefficients, so just pick one term in both and see if they have the same sign, which they do, so we conclude that they are the same polynomial. ■

Theorem 13.3 (pg. 42 of Stewart and Tall)**.** The discriminant of any $\mathbb{Q}$-basis for K is rational and non-zero.

Proof. By the fact proven from the homework, it suffices to proce this for the basis $\{1, \theta, .., \theta^{n-1}\}$.

Now we take $t_i = \theta_i = \sigma_i(\theta)$, to get that

$$\Delta[1, \theta, ..., \theta^{n-1}] = \prod_{i<j}(\theta_i - \theta_j)^2$$

$$= disc(minpoly_{\mathbb{Q}}(\theta)) \in \mathbb{Q}^*$$

, this product is fixed by all σ_i, so it's in the fixed field of all of them, which is $\mathbb{Q}$.

It is non-zero because $\theta_i \neq \theta_j \iff i \neq j$. ■

Example 13.4. Suppose $K = \mathbb{Q}(\sqrt{5})$, pic basis $\{1, \sqrt{5}\}$, therefore we have that

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

Another basis is $\{1, \frac{1+\sqrt{5}}{2}\}$, then

$$\Delta[1, \frac{1+\sqrt{5}}{2}] = det(\begin{bmatrix} 1 & (1+\sqrt{5})/2 \\ 1 & (1-\sqrt{5})/2 \end{bmatrix})^2 = 5$$

And we see that they differ by a square.

Suppose $K = \mathbb{Q}(2^{1/3})$, a basis is $B = \{1, 2^{1/3}, 2^{2/3}\}$, then

$$\Delta[B] = det(\begin{bmatrix} 1 & 2^{1/3} & 2^{2/3} \\ 1 & \omega 2^{1/3} & \omega^2 2^{2/3} \\ 1 & \omega^2 2^{1/3} & \omega^4 2^{2/3} \end{bmatrix})^2$$

13.2 Algebraic Integers

Definition 13.5. 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 $\overline{\mathbb{Z}}$, and clearly

$$\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}}$$

Example 13.6. Examples:

$\sqrt{2}$ is an algebraic integer, just take $x^2 - 2$.

$\frac{1+\sqrt{5}}{2}$ is an algebraic integer, take $x^2 - x - 1 = 0$.

Non-Examples:

$\frac{22}{7}$ is not an algebraic integer, mostly because the irreducible polynomial $7x - 22$ has to divide any polynomial whose root is $\frac{22}{7}$

Key Algebra Fact:

Proposition 13.7 (Gauss's Lemma)**.** If $f(x) \in \mathbb{Z}[x]$ is a monic polynomial with $f(x) = g(x)h(x)$, where $g(x), h(x)$ are monic polynomials in $\mathbb{Q}[x]$, then $g(x), h(x)$ are in fact in $\mathbb{Z}[x]$. (Gauss's Lemma)

Proposition 13.8 (Equivalent Definition of Algebraic Integers)**.** An algebraic number θ is an algebraic integer if and only if $minpoly_{\mathbb{Q}}(\theta)$ has integer coefficients!

14 Lecture March 24th

14.1 Algebraic Integers ctd.

Definition 14.1. A complex number x that satisfies $f(x) = 0$ for a non-constant monic polynomial $f(t) \in \mathbb{Z}[x]$ is called an *algebraic integer*.

Definition 14.2 (Equivalent Definition of Algebraic Integers)**.** An algebraic integer is an algebraic number whose minimal polynomial over $\mathbb{Q}$ has integer coefficients.

The set of algebraic integers is denoted by $\overline{\mathbb{Z}}$ and $\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}}$. In fact, $\overline{\mathbb{Z}}$ form a subring of $\overline{\mathbb{Q}}$.

Lemma 14.3 (pg. 44 S+T)**.** Let $\theta \in \mathbb{C}$, then θ is an algebraic integer if and only if the additive group generated by all powers of $1, \theta, \theta^2, ...$ is in fact finitely generated. (ie. $\mathbb{Z}[\theta]$ is finitely generated $\mathbb{Z}$-module).

Proof. In the forward direction, suppose $\theta \in \overline{\mathbb{Z}}$, then clearly there exist some non-constant polynomial $f(x)$ integer coefficients such that

$$f(\theta) = \theta^n + a_{n-1}\theta^{n-1} + ... + a_0 = 0$$

Then we claim that every power of θ lies in the additive group generated by $1, \theta, ..., \theta^{n-1}$, whic we will denote as Γ (pretty obvious using Euclidean Division).

Suppose inductively that $m \geq n$, and that $1, \theta, ..., \theta^m \in \Gamma$, then we can write

$$\theta^{m+1} = \theta^{m+1-n}\theta^n = \theta^{m+1-n}(-a_{n-1}\theta^{n-1} - ... - a_0) = -a_{n-1}\theta^m - (\text{lower degree terms})$$

, then apply the inductive htpothesis, we are done.

Conversely, suppose every power of θ lies in a finitely generated additive group G. Then the subgroup Γ of G generated by $1, \theta, \theta^2, ...$ (countably many) must also be finitely generated since $\mathbb{Z}$ is a Noetherian ring so any submodule of a finitely generated $\mathbb{Z}$-module is finitely generated.

Let $v_1, ..., v_n$ be generators of Γ (WLOG assume are non-zero), then each $v_i \in \mathbb{Z}[\theta]$, and we also have that for all i

$$\theta \cdot v_i \in \mathbb{Z}[\theta]$$

Hence, there exist integers b_{ij} such that

$$\theta v_i = \sum_{j=1}^{n} b_{ij} v_j$$

This gives usa system of linear equations:

$$(b_{11} - \theta)v_1 + b_{12}v_2 + ... + b_{1n}v_n = 0$$

$$b_{21}v_1 + (b_{22} - \theta)v_2 + ... + b_{2n}v_n = 0$$

$$\vdots$$

$$b_{n1}v_1 + b_{n2}v_2 + ... + (b_{nn} - \theta)v_n = 0$$

Then we can see that $v_1, ..., v_n$ is a solution to this system of linear equation. Let A be the coefficient matrix, since it has a non-trivial solution, so $Ax = 0$ for some non-zero vector x, so A is not invertible.

Thus $det(A) = 0$, we can write $A = B - \theta I$, and $det(B - xI)$ is a monic characteristic polynomial with integer coefficients and root $x = \theta$, so we have that θ is an algebraic integer. ■

Lemma 14.4 (Weaker Statement of Above)**.** $\theta \in \mathbb{C}$ is algebraic if and only if the additive subgroup generated by $1, \theta, \theta^2, ...$ is in fact generated by $1, \theta, \theta^2, ..., \theta^{n-1}$ for some n.

Theorem 14.5. $\overline{\mathbb{Z}}$ is a subring over $\overline{\mathbb{Q}}$

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

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

We observe that all powers of $\theta + \phi$ and $\theta\phi$ are integer linear combinations of the elements

$$\theta^r \phi^s \in \Gamma_\theta \Gamma_\phi$$

, where $\Gamma_\theta\Gamma_\phi$ is definied to be the additive group generated by $v_i w_j$, $1 \leq i \leq n, 1 \leq j \leq m$, where v_i and w_j are generators for Γ_θ and Γ_ϕ respectively.

Thus, $\Gamma_\theta\Gamma_\phi$ are finitely generated, then by our Lemma above, we have that $\theta + \phi$ and $\theta\phi$ are both algebraic integers. ■

Theorem 14.6 (p. 44 or 45)**.** Let $\theta \in \mathbb{C}$ satisfy a monic polynomial equation with coefficients in $\overline{\mathbb{Z}}$, then θ is indeed an algebraic integer.

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

14.2 Ring of integers of a number field

Definition 14.7. If K is a number field, then the set

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

is called the ring of integers of K. We note that $\mathcal{O}_k$ is the intersection of two subrings and is thus itself also a ring.

Remark 14.8. This is analogous to the relationship between integers and rationals. In fact, the field of fraction of $\mathcal{O}_k$ is K.

Lemma 14.9. Let $\alpha \in K$, then $c\alpha \in \mathcal{O}_k$ for some $c \in \mathbb{Z}$.

Proof. Suppose $\alpha \in K$, let $f(x) = minpoly_{\mathbb{Q}}(\alpha)$ and $deg(f) = n$.

Let $0 \neq c \in \mathbb{Z}$, let

$$g_c = c^n f(x/c)$$

Observe that for each α_i root of f, $c\alpha_i$ is a root of g_c.

We also note that g_c is monic, and we can choose c to be the least common multiple of all the denominators, then it in fact has integer coefficients. So g_c is a monic integer polynomial with root $c\alpha$. ■

Corollary 14.10. If K is a number field, then $K = \mathbb{Q}(\theta)$ for some algebraic integer θ. (as opposed to just some algebraic number)

Proof. Apply Lemma above and we can always choose our primitive element to be multipled by that c. ■

Remark 14.11 (WARNINGS! (46 - 47))**.** Although it is often that 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!

For example, suppose $K = \mathbb{Q}(\sqrt{5})$, then

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

In fact, $\mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \mathcal{O}_k$.

It in fact gets worse than this, $\mathcal{O}_k$ need not be of the form $\mathbb{Z}[\theta]$ fr some $\theta \in \overline{\mathbb{Z}}$. Dedekind first found a counterexample in 1871, with the example is

$$K = \mathbb{Q}(\theta), \theta \text{ a root of } x^3 - x^2 - 2x - 8$$

Number fields where $\mathcal{O}_k$ can be represented as $\mathbb{Z}$ adjoin some algebraic integer are called monogenic number fields.

15 Lecture April 5th

15.1 Integral bases for number fields

Before springbreak, recall that

- We introduced embeddings of a number field K into $\mathbb{C}$, which was directly related to the notion of conjugates.
- We also introduced discriminants of $\mathbb{Q}$-bases of number fields
- We introduced algebraic integers, which are algebraic numbers whose minimal polynomial over $\mathbb{Q}$ have integer coefficients
- The ring of integers of a number field K is by definition

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

- When $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$

Remark 15.1. The ring of integers of a number field K is a free $\mathbb{Z}$-module of rank n, where n is the degree of the number field K. The intuition is that K is a $\mathbb{Q}$-vector space of dimension n, so its contraction to the algebraic integers turns it into a free $\mathbb{Z}$-module of rank n.

Definition 15.2. Suppose $B = \{\alpha_1, ..., \alpha_n\}$ is a $\mathbb{Q}$-basis for K such that $\alpha_i \in \mathcal{O}_k$ for all i (we can pick them in $\mathcal{O}_k$ in the spirit of Gauss's Lemma). We say that B is an integral basis for $\mathcal{O}_k$ if every element of $\alpha = \mathcal{O}_k$ can be expressed uniquely as

$$\alpha = c_1\alpha_1 + ... + c_n\alpha_n, c_1, ..., c_n \in \mathbb{Z}$$

Note this is just the basis for a free $\mathbb{Z}$-module.

Theorem 15.3. Every number field has an integral basis.

Proof. Let K be a number field of degree n. We have noted that if $\{\alpha_1, ..., \alpha_n\}$ is a $\mathbb{Q}$-basis of K such that $\alpha_i \in \mathcal{O}_k$ for all i, then the absolute value discriminant of the basis is

$$|\Delta[\alpha_1, ..., \alpha_n]| \in \mathbb{Z}_+$$

This follows from computing the determinant of the Vandermonde matrix.

Let $\{\omega_1, ..., \omega_n\}$ be a $\mathbb{Q}$-basis with $\omega_i \in \mathcal{O}_k$, such that the absolute value of its discriminant is minimal among all the basis that are in $\mathcal{O}_k$.

We claim that then $\{\omega_1, ..., \omega_n\}$ is an integral basis for $\mathcal{O}_k$.

Indeed, suppose this is not true, then there exist some $\omega \in \mathcal{O}_k$ such that

$$\omega = a_1\omega_1 + ... + a_n\omega_n.a_1, ..., a_n \in \mathbb{Q}$$

, but at least one $a_i \notin \mathbb{Z}$, without loss we will say $i = 1$.

Then we can write

$$a_1 = a + r, a \in \mathbb{Z}, 0 < r < 1$$

Now consider $\Psi_1 = \omega - a\omega_1$, $\Psi_i = \omega_i$, for $2 \leq i \leq n$, and clearly $\psi_1, ..., \psi_n \in \mathcal{O}_k$.

Clearly, $\Psi_1, ..., \Psi_n$ also form a $\mathbb{Q}$-basis for K. Now consider the matrix M sending $\omega_i \mapsto \psi_i$ with respect to the ω_i-basis, then

$$M = \begin{pmatrix} a_1 - a & 0 & 0 & ... & 0 \\ a_2 & 1 & 0 & ... & 0 \\ a_3 & 0 & 1 & ... & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & 0 & ... & 1 \end{pmatrix}$$

Since M is a lower triangular matrix, $det(M)$ is just the product of all elements on its diagonal entry, so $det(M) = a_1 - a$. Hence we have that

$$\Delta[\Psi_1, ..., \Psi_n] = (det(M))^2 \Delta[\omega_1, ..., \omega_n]$$

But $a_1 - a < 1$, so this contradicts the minimality of the $\{\omega_1, ..., \omega_n\}$.

Thus, $\{\omega_1, ..., \omega_n\}$ is an integral basis for K. ■

Remark 15.4. The proof doesn't tell us if there's an integral basis whose absolute value of discriminant is not minimal, but if such basis does exist we note that $det(M) = \pm 1$ since the matrix from one integral basis to another is an integer matrix that is invertible, so the determinant would send the matrix to the unit group of $\mathbb{Z}$.

Thus, any integral basis has a discriminant achiebeing this minimal possible absolute value.

How do you know you're looking at an integral basis? If you are lucky, you can sometimes diagnose this from the discriminant.

Theorem 15.5 (Page 50 of Stewart and Tall)**.** Suppose $\{\alpha_1, ..., \alpha_n\}$, $\alpha_i \in \mathcal{O}_k$ is a $\mathbb{Q}$-basis of K, if $\Delta[\alpha_1, ..., \alpha_n]$ is square-free, then $\{\alpha_1, ..., \alpha_n\}$ is an integral basis.

Proof. Suppose $\{\beta_1, ..., \beta_n\}$ is an integral basis, then there exist $c_{ij} \in \mathbb{Z}$ such that

$$\alpha_i = \sum_j c_{ij}\beta_j, \forall i$$

Then $M = (c_{ij})$ is the change of basis matrix from the α_i basis to the β_i basis, so we have that

$$\Delta[\alpha_1, ..., \alpha_n] = (det(M))^2 \cdot \Delta[\beta_1, ..., \beta_n]$$

Now since $\Delta[\alpha_1, ..., \alpha_n]$ is square-free, and both $det(M)$ and $\Delta[\beta_1, ..., \beta_n]$ are integers, so it follows that $det(M) = \pm 1$.

Thus $\Delta[\alpha_1, ..., \alpha_n] = \Delta[\beta_1, ..., \beta_n]$, so $\{\alpha_1, ..., \alpha_n\}$ is itself also an integral basis. ■

Example 15.6. Suppose $K = \mathbb{Q}(\sqrt{5})$, then we previously observed that $\theta = \frac{1+\sqrt{5}}{2} \in \overline{\mathbb{Z}}$, hence $\theta \in \mathcal{O}_k$.

Then

$$\Delta[1, \frac{1+\sqrt{5}}{2}] = 5$$

Since 5 is square-free, this means that we also have an integral basis for K. We also note that $\mathcal{O}_k = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

Definition 15.7. Let K be a number field, the **discriminant** associated to any integral basis of $\mathcal{O}_k$ is called the **discriminant of K**. We refer to ths as $disc(K)$ or $\Delta(K)$.

Example 15.8. Examples of Discriminants

- $K = \mathbb{Q}(\sqrt{5})$ has $disc(K) = 5$
- $K = \mathbb{Q}(\sqrt{2})$, then we note $\mathcal{O}_k = \mathbb{Z}[\sqrt{2}]$, so

  $$disc(K) = \Delta[1, \sqrt{2}] = (-2\sqrt{2})^2 = 8$$

  We also note that $disc(K)$ is the same as the minimal polynomial of θ, which is $x^2 - 2$, with discriminant $b^2 - 4ac = 8$
- More interesting example, when $K = \mathbb{Q}(\theta)$ for θ a root of $x^3 - x^2 - 2x - 8$. An integral basis for $\mathcal{O}_k$ is

  $$\{1, \theta, \frac{\theta + \theta^2}{2}\}$$

  This is a number field that has NO power integral basis, and the discriminant is -503, which is prime.

Definition 15.9. Note that the following terms are synonymous

- $\mathcal{O}_k = \mathbb{Z}[\theta]$ for $\theta \in \overline{\mathbb{Z}} \cap \mathcal{O}_k$
- $\mathcal{O}_k$ (or K) is monogenic
- $\{1, \theta, ..., \theta^{n-1}\}$ form an integral basis for some $\theta \in \mathcal{O}_k$
- $\mathcal{O}_k$ (or K) has a power integral basis.

There are a couple number fields that we are interested in studying in more details

- **Quadratic Fields**
- **Cyclotomic Extensions**

15.2 Quadratic Field

Definition 15.10. A quadratic field is a number field K of degree 2 over $\mathbb{Q}$. Thus

$$K \text{ is quadratic } \implies K = \mathbb{Q}(\theta)$$

, where θ is a root of $x^2 + ax + b$, $a, b \in \mathbb{Z}$, so in other words

$$\theta = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

Let $a^2 - 4b = r^2 d$, where $r, d \in \mathbb{Z}$, d is square-free (so we have a square-free decomposition), then

$$\theta = \frac{-a \pm r\sqrt{d}}{2}$$

Proposition 15.11 (p.64 of ST)**.** The K is a quadratic fields if and only if

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

where d is a square-free integer.

Theorem 15.12 (p.64 of ST)**.** Let $d \in \mathbb{Z}$ be a square-free integer, and let $K = \mathbb{Q}(\sqrt{d})$, then $\mathcal{O}_k$ is equal to

- $\mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1 \ mod \ 4$
- $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \ mod \ 4$

16 Lecture April 7th

16.1 Quadratic Fields

Definition 16.1. A quadratic field is a number field K of degree 2 over $\mathbb{Q}$. Thus, $K = \mathbb{Q}(\theta)$ for θ a root of $x^2 + ax + b$ where $a, b \in \mathbb{Z}$, and thus $\theta = \frac{-a \pm \sqrt{a^2-4b}}{2}$.

Proposition 16.2. The Quadratic fields are of the form

$$\mathbb{Q}(\sqrt{d})$$

where $d \in \mathbb{Z}$ is square-free.

Theorem 16.3 (pg. 64 of ST)**.** Let $d \in \mathbb{Z}$ be a square-free integer, and let $K = \mathbb{Q}(\sqrt{d})$, then $\mathcal{O}_k$ is equal to

- $\mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1 \; mod \; 4$
- $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \; mod \; 4$

Proof. Every $\alpha \in \mathbb{Q}(\sqrt{d})$ is

$$\alpha = \frac{a + b\sqrt{d}}{c}, a, b, c \in \mathbb{Z}$$

We can assume without loss that $c > 0$ and $(a, b, c) = 1$.

Now $\alpha \in \mathcal{O}_k$ if and only if its minimal polynomial is an integer polynomial, so

$$(x - \frac{a + b\sqrt{d}}{c})(x - \frac{a - b\sqrt{d}}{c} \in \mathbb{Z}[x]$$

This holds if and only if

$$\frac{a^2 - b^2 d}{c^2} \in \mathbb{Z}, \frac{2a}{c} \in \mathbb{Z}$$

We claim that $(a, c) = 1$. Indeed, suppose $(a, c) \neq 1$, then $(a, c)|(a, b, c)$ by observing the experssion $\frac{a^2-b^2d}{c^2}$ and the fact that $(a, b, c) \neq 1$ lead to a contradiction.

Now since $\frac{2a}{c} \in \mathbb{Z}$, this only happens when c is either 2 or 1.

If $c = 1$, then $\alpha \in \mathcal{O}_k$ anyway.

Now if $c = 2$, the same argument shows us that $(b, c) = 1$, so b is odd and a is odd. Moreover, $\alpha \in \mathcal{O}_k$ with these assumptions iff

$$\frac{a^2 - b^2 d}{c^2} = \frac{a^2 - b^2 d}{4} \in \mathbb{Z}$$

THis happens if and only if

$$a^2 - b^2 d \equiv 0 \; mod \; 4$$

Since a, b are odd, their square is always 1 mod 4, so we have that

$$d \equiv 1 \; mod \; 4$$

Thus $c = 2$ and $\alpha \in \mathcal{O}_k$ implies that $d \equiv 1 \; mod \; 4$.

In summary, if $d \not\equiv 1 \; mod \; 4$, then $c = 1$, then α is of the form $a + b\sqrt{d}$, so $\mathcal{O}_k = \mathbb{Z}[\sqrt{d}]$.

If $d \equiv 1 \; mod \; 4$, then we can have $c = 2$ and a, b being odd. Hence we have that

$$\mathcal{O}_k = \mathbb{Z}[\frac{1 + \sqrt{d}}{2}]$$

■

Theorem 16.4 (pg. 65 of S+T)**.** We have that

- (a) If $a \not\equiv 1 \ mod \ 4$, $\{1, \sqrt{d}\}$ an integral basis. If $d \equiv 1 \ mod \ 45$, $\{1, \frac{1+\sqrt{d}}{2}\}$ is an integrable basis.
- (b) If $d \not\equiv \mod 4$, then
$$disc(K) = 4d$$
If $d \equiv 1 \ mod \ 4$, then
$$disc(K) = d$$

16.2 Cyclotomic Extensions

Definition 16.5. A cyclotomic field is a number field of the form

$$K = \mathbb{Q}(\zeta_n)$$

, where ζ_n is any primitive n-th root of unity, usually $\zeta_n = e^{2\pi i/n}$

Example 16.6. $K = \mathbb{Q}(i)$ is a cyclotomic extension since $\zeta_4 = i$.

$K = \mathbb{Q}(\sqrt{-3})$ is a cyclotomic extension since $K = \mathbb{Q}(\frac{1+\sqrt{-3}}{2}) = \mathbb{Q}(\zeta_3)$.

Proposition 16.7. Important facts about Cyclotomic Extensions:

- Any embedding of $\mathbb{Q}(\zeta_n) \to \mathbb{C}$ has image contained in $\mathbb{Q}(\zeta_n)$ (In other words, there extensions are Galois over $\mathbb{Q}$)
- We care about radical extensions, which are of the form
$$\mathbb{Q}(\sqrt[n]{a}), a \in \mathbb{Q}$$
These extensions are not generally Galois, but you could extend the extension to some Galois closure.

  In particular, we could "repair" the base field by adjoining a primitive n-th root of unity to turn this into a Kummer extension. Indeed, let $K = \mathbb{Q}(\zeta_n)$, then $L = K(\sqrt[n]{a})$, then L/K is Galois (the embeddings: $L \to \mathbb{C}$ fix K send L to itself)
- $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$
- The field automorphisms $\sigma : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$ form a cyclic group under composition, of order $\phi(n)$, you can describe this as a permutation on ζ_n.

Let $K = \mathbb{Q}(\zeta_n)$, then

- $\mathcal{O}_k = \mathbb{Z}[\zeta_n]$, the case for when $n = p$ is a prime is in Stewart and Tall
- When $n \geq 3$, $Disc(K) = (-1)^{\Phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}$
- For $n = p$ a prime, we habe that
$$Disc(\mathbb{Q}(\zeta_p)) = (-1)^{(p-1)/2} p^{p-2}$$
- In particular if $p \in \mathbb{Z}$ and $p \nmid n$, then $p \nmid Disc(\mathbb{Q}(\zeta_n))$.

Theorem 16.8 (Kronecker-Weber Theorem)**.** Every finite abelian extension of $\mathbb{Q}$ is contained in some cyclotomic extension.

16.3 Prime Factorization in Number Fields (5.1)

Recall the examples of non-UFDs given in MATH 1530, like $\mathbb{Z}[\sqrt{-5}]$, where $6 = 2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$, but 2 is not an associate of irreducibles $1+\sqrt{-5}$ or $1-\sqrt{-5}$.

In $\mathbb{Q}(\sqrt{15})$, we also have that $2 \cdot 5 = (5+\sqrt{15})(5-\sqrt{15})$ in $\mathbb{Z}[\sqrt{15}]$.

Notice:

$$5+\sqrt{15} = \sqrt{5}(\sqrt{5}+\sqrt{3})$$
$$5-\sqrt{5} = \sqrt{5}(\sqrt{5}-\sqrt{3})$$

Multipliying this then yields

$$25-15 = 10 = 5(\sqrt{5}+\sqrt{3})(\sqrt{5}-\sqrt{3})$$

So this factors in $a_1 = \sqrt{5}, a_2 = \sqrt{5}+\sqrt{3}, a_3 = \sqrt{5}-\sqrt{3}$ are being grouped in 2 ways:

$$(a_1^2)(a_2a_3) = (a_1a_2)(a_1a_3)$$

In other words, the problem of Non-UFD goes away by passing it through some extensions in $\mathcal{O}_L$ where $L = \mathbb{Q}(\sqrt{15},\sqrt{5}) = \mathbb{Q}(\sqrt{3},\sqrt{5})$.

In $\mathbb{Q}(\sqrt{30})$, we have that $2 \cdot 3 = (6+\sqrt{30})(6-\sqrt{30})$

In $\mathbb{Q}(\sqrt{-10})$, we have that $2 \cdot 7 = (2+\sqrt{10})(2-\sqrt{10})$

Theorem 16.9 (Principal Ideal Theorem)**.** Let K be a number field. Then there exist some finite extension L/K such that every non-zero $\alpha \in \mathcal{O}_K$ has a unique factorization into irreducibles in $\mathcal{O}_L$. (Note that $\mathcal{O}_L$ itself NEED not be a UFD. It is in fact not true that every number field K has a finite extension L/K such that $\mathcal{O}_L$ is a UFD)

17 Lecture April 12th

17.1 Ideals Fractional Ideals:

Definition 17.1. Let R be a commutative ring with unity. Recall that if I, J are ideals of R, then

$$I + J := \{a_i + b_j | a_i \in I, b_j \in J\}$$

is also an ideal, and

$$IJ := \{\sum_{i=1}^{n} a_i b_i | a_i \in I, b_i \in J\}$$

Remark 17.2. The naive definition of product of ideals does not work ie. if we define

$$IJ = \{a_i b_j | a_i \in I, b_j \in J\}$$

is not necessarily ideal. For example, in $\mathbb{Z}[x]$, take $I = (2, x), J = (3, x)$

Definition 17.3. Let K be a number field. An ideal of $\mathcal{O}_K$ is sometimes called an **integral ideal**. This is to contrast them with fractional ideals.

Definition 17.4. A **fractional ideal** of $\mathcal{O}_K$ is a set of the form

$$C^{-1}\mathfrak{b}$$

, where $\mathfrak{b}$ is an ideal of $\mathcal{O}_K$, and c is a non-zero element of $\mathcal{O}_k$

Example 17.5. The fractional ideals of $\mathbb{Z}$ are of the form $r\mathbb{Z}$ where $r \in \mathbb{Q}$. For instance,

$$\frac{2}{5}\mathbb{Z}$$

is a fractional ideal of $\mathbb{Z}$.

Remark 17.6. We note that if $\mathcal{O}_k$ is a PID, then the fractional ideals are really easy to describe, specifically:

$$C^{-1}(d) = C^{-1}d\mathcal{O}_k$$

Let $\alpha = C^{-1}d$, then this is just the ideal generated by α in $\mathcal{O}_k$. This need not hold outside of a UFD.

Definition 17.7 (Addition and Multiplication of Fractional Ideals)**.** If $\mathfrak{a}, \mathfrak{b}$ are fractional ideals, then

$$\mathfrak{ab} = \{\text{finite sum } \sum a_i b_j | a_i \in \mathfrak{a}, b_j \in \mathfrak{b}\}$$

The definition for $\mathfrak{a} + \mathfrak{b}$ is obvious. If

$$\mathfrak{a}_1 = c_1^{-1}\mathfrak{b}_1, \mathfrak{a}_2 = c_2^{-1}\mathfrak{b}_2$$

, where $\mathfrak{b}_1, \mathfrak{b}_2$ are integral ideals, then

$$\mathfrak{a}_1\mathfrak{a}_2 = (c_1c_2)^{-1}\mathfrak{b}_1\mathfrak{b}_2$$

, which is a fractional ideal.

The multiplication (of fractional ideals) is associative and commutative, with the unit ideal $\mathcal{O}_k$ as the multiplicative identity.

Thus, the set of non-zero fractional ideals form an abelian monoid under multiplication.

What about inverses?

Theorem 17.8 (pg. 109 of S+T)**.** The non-zero fractional ideals of $\mathcal{O}_k$ form a group under multiplication. (Note this usually doesn't hold unless we are in a Dedekind Domain)

Proof. For each integral ideal $\mathfrak{a} \subset \mathcal{O}_k$, define

$$\mathfrak{a}^{-1} = \{x \in K | x\mathfrak{a} \subset \mathcal{O}_k\}$$

Clearly $\mathcal{O}_k \subset \mathfrak{a}^{-1}$. If $\mathfrak{a}$ is non-zero, then for any $0 \neq c \in \mathfrak{a}$, we have that by definition

$$c\mathfrak{a}^{-1} \subset \mathcal{O}_k$$

Fixing such a c, we have that $c\mathfrak{a}^{-1} = \mathfrak{b}$ is in fact an ideal of $\mathcal{O}_k$.

This is because $c\mathfrak{a}^{-1}$ is an $\mathcal{O}_k$-submodule of $\mathcal{O}_k$, ie. an ideal of $\mathcal{O}_k$).

Thus, $\mathfrak{a}^{-1} = c^{-1}\mathfrak{b}$, so this is actually a fractional ideal.

By definition then, we have that

$$\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} \subset \mathcal{O}_k$$

Now we want to show that $\mathcal{O}_K \subset \mathfrak{a}\mathfrak{a}^{-1}$ (Blackboxed Momentarily pg. 110 - 112 of S + T, using the fact that $\mathcal{O}_K$ is a Dedekinf Domain) ■

Example 17.9. The product of an ideal with its inverse need not be the whole ring. For example take $R = \mathbb{C}[x, y]$ and consider its field of fraction K, then R is our integral domain here and K its field of fractions.

Now let $\mathfrak{a} = (x, y)$, what is $\mathfrak{a}^{-1}$, well since any element in $\mathfrak{a}^{-1}$ has to multiply to every element of $\mathfrak{a}$ into $\mathfrak{a}$, we have that $\mathfrak{a}^{-1} = R$, so

$$\mathfrak{a}\mathfrak{a}^{-1} \neq K$$

Remark 17.10. We can also extend the construction of inverses to fractional ideals using the exact same setup.

Assuming this, we have shown that

Theorem 17.11 (pg. 109 of S + T)**.** The non-zero fractional ideals of $\mathcal{O}_K$ form a group under multiplication.

Proof. We can deduce this quickly from the fact that integral ideals are invertible in $\mathcal{O}_K$.

Let $\mathfrak{a}$ be a non-zero fractional ideal of $\mathcal{O}_K$. Then we have that

$$\mathfrak{a} = c^{-1}\mathfrak{b}$$

$\mathfrak{b}$ is an integral ideal and $0 \neq c \in K$. Then define $a' = c\mathfrak{b}^{-1}$, where $\mathfrak{b}^{-1}$ is the inverse of the integral ideal $\mathfrak{b}$. We clearly then have that

$$\mathfrak{a}\mathfrak{a}' = \mathcal{O}_K$$

■

17.2 Dedekind Domain

Recall: A prime ideal a commutative ring R can be defined in a couple of different ways:

Proposition 17.12 (Equivalent Definition of Prime Ideals)**.** The following definitions of a prime ideal $\mathfrak{p}$ in a commutative ring R is:

- 1) If for any two ideals I, J of R such that $IJ \subset \mathfrak{p} \implies I \subset \mathfrak{p}$ or $J \subset \mathfrak{p}$
- 2) For any two elements $a, b \in R$ such that $ab \in \mathfrak{p} \implies a \in \mathfrak{p}$ or $b \in \mathfrak{p}$

To prove unique factorization of non-zero ideals, we first need to prove $\mathcal{O}_K$ is a Dedekind Domain.

Definition 17.13. A chain of ideals is a sequence of inclusions:

$$I_1 \subset I_2 \subset ...$$

and for such a chain to terminate means that there exist some N such that $I_n = I_N$ for all $n \geq N$.

Theorem 17.14 (pg. 109 - S + T)**.** The ring of integers $\mathcal{O}_K$:

- a) is an integral domain
- b) is Noetherian (every ascending chain of ideals terminates, or equivalently every ideal is finitely generated)
- c) The ring of integers is integrally closed in its field of fractions, meaing if $\alpha \in Frac(\mathcal{O}_K) = K$ satisfies a monic polynomial equation with coefficients in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$.
- d) Every non-zero prime ideal of $\mathcal{O}_K$ is maximal.

We also note that a ring satisfying $(a) - (d)$ is known as a Dedekind Domain.

18 Lecture April 14th

Recall that last time we

- Defined fractional ideals
- Defined the inverse of an integral ideal (and that the same definition holds for fractional ideal - with the exception of the zero ideal, which is fractional but not invertible)
- Briefly stated the definition of a Dedekind Domain

Theorem 18.1 (pg. 109 - S + T)**.** The ring of integers $\mathcal{O}_K$:

- a) is an integral domain
- b) is Noetherian (every ascending chain of ideals terminates, or equivalently every ideal is finitely generated)
- c) The ring of integers is integrally closed in its field of fractions, meaning if $\alpha \in Frac(\mathcal{O}_K) = K$ satisfies a monic polynomial equation with coefficients in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$.
- d) Every non-zero prime ideal of $\mathcal{O}_K$ is maximal.

We also note that a ring satisfying $(a) - (d)$ is known as a Dedekind Domain.

Proof. (a) is obvious, (c) was noted in a previous lecture.

For (b), we know that if $[K : \mathbb{Q}] = n$, then $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n (ie. $\mathcal{O}_K$ is a free abelian group of a rank n).

If $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, then $(\mathfrak{a}, +)$ is free abelian of rank less than or equal to n (See. Theorem 1.16 of S + T) So in other words, $(\mathfrak{a}, +)$ is finitely generated as an $\mathcal{O}_K$ module (since $\mathbb{Z} \subset \mathcal{O}_K$, so every ideal of $\mathcal{O}_K$ is finitely generated with respect to $\mathcal{O}_K$.

For (d), let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. Let $0 \neq \alpha \in \mathfrak{p}$. Then consider $N := N_{K/\mathbb{Q}}(\alpha) = \alpha_1 ... \alpha_n$, where $\alpha_1, ..., \alpha_n$ are conjugates of α and define $\alpha_1 = \alpha$.

We note that $N(\alpha) \in \mathbb{Q}$ since its fixed by all the filed embeddings. Moreover, $\alpha_2 ... \alpha_n = \frac{N(\alpha)}{\alpha} \in K$. In fact, $\alpha_2 \alpha_3 ... \alpha_n \in \mathcal{O}_K$.

Thus, we have that $N(\alpha) \in \mathfrak{p}$ since $\mathfrak{p}$ is an ideal.

Thus $N(\alpha) \cdot \mathcal{O}_K \subset \mathfrak{p}$, which means that

$$\mathcal{O}_K/\mathfrak{p} \text{ is a quotient of } \mathcal{O}_K/N\mathcal{O}_K$$

Now, $\mathcal{O}_K/N\mathcal{O}_K$ is a finitely generated abelian group where every element has finite order (add it N times, goes to 0), so in particular $\mathcal{O}_K/N\mathcal{O}_K$ is a finite group.

Hence we have that $\mathcal{O}_K/\mathfrak{p}$ is finite group. Since $\mathfrak{p}$ is prime, $\mathcal{O}_K/\mathfrak{p}$ is an integral domain. But we know that any finite integral domain is in fact a field, so this means that $\mathfrak{p}$ is actually a maximal ideal. ■

Proposition 18.2 (pg. 112 S + T - Existence Claim)**.** Every non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$ is a product of prime ideals.

Proof. Suppose not, then let $\mathfrak{a}$ be a maximal element of the set of ideals of $\mathfrak{a}$ that is NOT a product of prime ideals. Why does this exist?

Recall Zorn's Lemma: In a poset where every chain has an upperbound that's also in the poset, there's at least 1 maximal element in said poset.

The Noetherian property of $\mathcal{O}_K$ tells us every chain has an upperbound in that poset (some finite termination), so Zorn's Lemma gives us this maximal element.

Certainly $\mathfrak{a}$ itself is not a prime ideal, but applying Zorn's Lemma to the poset of proper ideals containing $\mathfrak{a}$ to conclude that $\mathfrak{a} \subset \mathfrak{p}$ for some maximal ideal $\mathfrak{p}$, which is prime.

We have that $\mathcal{O}_K \subsetneq \mathfrak{p}^{-1} \subset \mathfrak{a}^{-1}$ since inverses of integral ideals is inclusion reversing and $\mathfrak{a} \subset \mathfrak{p} \subset \mathcal{O}_K$. (We note it respects proper containment since you can also take an inverse back)

It follows that

$$\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K \ (*)$$

By the maximality of $\mathfrak{a}$, we know that $\mathfrak{a}\mathfrak{p}^{-1}$ is a product of prime ideals, but this means that

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2 ... \mathfrak{p}_r$$

, where $\mathfrak{p}_2, ..., \mathfrak{p}_r$ are prime, but then we have that

$$\mathfrak{a} = \mathfrak{p}\mathfrak{p}_2 ... \mathfrak{p}_r$$

is a product of prime ideals, hence a contradiction. ■

Lemma 18.3 (pg. 113 S+T)**.** For ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}_K$ (or more generally a Dedekind Domain), we have that

$$\mathfrak{a}|\mathfrak{b} \iff \mathfrak{a} \supseteq \mathfrak{b}$$

(Note we say $\mathfrak{a}|\mathfrak{b}$ if there exist an ideal C such that $\mathfrak{b} = C\mathfrak{a}$)

Proof. Suppose $\mathfrak{a}|\mathfrak{b}$, clearly $\mathfrak{b} = C\mathfrak{a} \subseteq \mathfrak{a}$. Conversely, suppose that $\mathfrak{b} \subseteq \mathfrak{a}$. Now let $\mathfrak{b} = \mathfrak{a}(\mathfrak{a}^{-1}\mathfrak{b})$, where $\mathfrak{a}^{-1}\mathfrak{b}$ is integral since $\mathfrak{a}^{-1}\mathfrak{b} \subset \mathfrak{a}^{-1}\mathfrak{a} = \mathcal{O}_K$. ■

Theorem 18.4 (pg. 112)**.** Every nonzero ideal of $\mathcal{O}_K$ has a unique factorization as product of prime ideals.

Proof. The lemma above tells us that $\mathfrak{p}$ is prime if and only if $\mathfrak{p}|\mathfrak{a}\mathfrak{b} \implies \mathfrak{p}|\mathfrak{a}$ or $\mathfrak{p}|\mathfrak{b}$ (specifcally if helps the forward direction).

Suppose $\mathfrak{a} = \mathfrak{p}_1 ... \mathfrak{p}_r = \mathfrak{q}_1 ... \mathfrak{q}_s$, as product of prime ideals (not necessarily distinct).

Then $\mathfrak{p}_1$ divides one of $\mathfrak{q}_j$ for some j, so since $\mathfrak{q}_j$ is maximal in $\mathcal{O}_K$, we have that $\mathfrak{p}_1 = \mathfrak{q}_j$.

Now we can go down the list from $1, ..., r$ because we can get rid of the previous $\mathfrak{p}_i$ using $\mathfrak{p}_i^{-1}$, and repeating the process tells us that this factorization is unique. ■

19 Lecture April 21st

19.1 Last Time:

- Discussed Fractional Ideals
- Introduced inverses to non-zero fractional ideals in $\mathcal{O}_K$ and more generally Dedekind Domains
- Proved $\mathcal{O}_K$ was a Dedekind Domain
- Provided an analog for prime factorization in $\mathcal{O}_K$, that every non-zero ideal of $\mathcal{O}_K$ factors uniquely as a product of primne ideals. (And analogously to all Dedekind Domains)

19.2 This Lecture:

A major topic/theme in classical algebraic number theory is the factorzation of ideals in $\mathcal{O}_K$ that are generated by primes in $\mathbb{Z}$.

Definition 19.1. Let $p \in \mathbb{Z}_+$ be a positive prime number, and let K be a number field,

- 1) We say p **ramifies** in K (or $\mathcal{O}_K$) if for
$$(p) := p\mathcal{O}_K = p_1^{e_1} p_2^{e_2} ... p_r^{e_r}$$
, where $p_1, ..., p_r$ are pairwise distinct prime ideals, and there's some $e_i \geq 2$
- 2) We say that p is **totally ramified** if
$$(p) := p_1^n$$
, where $n = [K : \mathbb{Q}]$, and p_1 is a prime ideal
- 3) We say that p is **inert** if (p) is a prime ideal of $\mathcal{O}_K$, ie.
$$(p) = p_1$$
- 4) We say that p is **totally split** if $(p) = p_1 p_2 ... p_n$, p_i pairwise distinct, $n = [K : \mathbb{Q}]$

Note that this is not an exhaustive list of prime factorizations in $\mathcal{O}_K$, but note that in a Quadratic Extension, this is indeed an exhaustive list.

Example 19.2. Here are some examples of prime factorization:

- 2 is totally ramified (and thus ramified) in $\mathbb{Z}[i]$ (ring of integers of $\mathbb{Q}(i)$), n particular
$$(2) = (1+i)(1-i) = (1+i)^2$$
- 3 is inert in $\mathbb{Z}[i]$ since (3) is a prime ideal in $\mathbb{Z}[i]$
- In $\mathbb{Z}[i]$, we can write $5 = (1+2i)(1-2i)$, which are both prime in $\mathbb{Z}[i]$. However, $1+2i, 1-2i$ aren't associates, because the only units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$, and none of them make the cut.

  Thus, 5 is totally split in $\mathbb{Z}[i]$.

There are two structural questions we want to answer:

- 1) Which primes of $\mathcal{O}_K$ ramify?
- 2) How do individual rational primes (primes in $\mathbb{Z}$) factor in $\mathcal{O}_K$

Theorem 19.3. p is ramified in K if and only if $p | Disc(K)$

Proof. We will prove this in the monogenic case, ie. when $\mathcal{O}_K$ is of the form $\mathbb{Z}[\theta]$ for some $\theta \in \mathcal{O}_K$, but note that this holds for any general number field.

The main ideal of the proof is to study the facotrization of f modulo p where $f = minpoly_{\mathbb{Q}}(\theta)$.

Suppose K is monogenic, with $\mathcal{O}_K = \mathbb{Z}[\theta]$, and let $p \in \mathbb{Z}_+$ be prime and let $f = minpoly_{\mathbb{Q}}(\theta)$.

Since $Disc(K) = \Delta[1, \theta, ..., \theta^{n-1}] = disc(f)$, we only need to show that

$$p|disc(f) \iff p \text{ ramifies in } K$$

Let $p\mathcal{O}_K = p_1^{e_1}...p_r^{e_r}$ be the prime factorzation of $p\mathcal{O}_K$, then we note that

$$\mathcal{O}_K/(p) \cong \mathcal{O}_K/p_1^{e_1} \times ... \times \mathcal{O}_\mathcal{K}/p_r^{e_r}$$

, by the Chinese Remainder Theorem. We note this is because $p_i + p_j\mathcal{O}_K$ for all $i \neq j$.

On the other hand, we note that

$$\mathcal{O}_\parallel/(p) = \frac{\mathbb{Z}[\theta]}{p\mathbb{Z}[\theta]} \cong \frac{\mathbb{Z}[x]}{(p, f(x))}$$

This isomorphism comes from the fact that firstly:

$$\mathbb{Z}[\theta] \cong \frac{\mathbb{Z}[x]}{(f(x))}$$

Second, in general if $\frac{\frac{R}{(a)}}{(b)} \cong \frac{R}{(a,b)}$, Thus, we have that

$$\mathcal{O}_\parallel/(p) = \frac{\mathbb{Z}[\theta]}{p\mathbb{Z}[\theta]} \cong \frac{\mathbb{Z}[x]}{(p, f(x))} \cong \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{(\overline{f}(x))}$$

If $\overline{f}(x) = \overline{\pi}_1(x)^{f_1}\overline{\pi}_2(x)^{f_2}...\overline{\pi}_s(x)^{f_s}$, then

$$(\mathbb{Z}/p\mathbb{Z})[x]/(\overline{f}) \cong \frac{\mathbb{F}_p[x]}{\overline{\pi}_1^{f_1}} \times ... \times \frac{\mathbb{F}_p[x]}{\overline{\pi}_s^{f_s}}$$

(We note we can use the CRT again because $\mathbb{F}_p[x]$ is an Euclidean Domain so gcd of two irreducible polynomial here is the constant 1 polynomial).

We note that for $\mathfrak{p}_1$ for $\mathcal{O}_K/(p)$, we have a chain of ideals

$$p_1^{e_1} \subsetneq p_1^{e_1-1} \subsetneq ... \subsetneq p_1 \subsetneq \mathcal{O}_K$$

So in other words, $\frac{p_1}{p_1^{e_1}}$ is a (in fact unique) maximal ideal of $\mathcal{O}_K/(p_1^{e_1})$.

Now we claim that if $R \cong R_1 \times R_2$ and $I \subset R_1$ is maximal in R_1, then $I \times R_2$ is maximal in R. So we know that $\mathcal{O}_K/(p)$ has a total of r maximal ideals from one side (due to uniqueness), and the other side shows us it has a total of s maximal ideals, so we have that $r = s$.

Start with the ideal $J_1 = I_1 \times \frac{\mathcal{O}_K}{p_2^{e_2}} \times ... \times \frac{\mathcal{O}_K}{p_r^{e_r}}$ where I_1 is maximal in $\mathcal{O}_K/p_1^{e_1}$, and then we descend from I_1 down all the way to the zero ideal for each J_k (we note this terminates because $\frac{\mathcal{O}_K}{(p)}$ is a finite ring) - this is kind of the crux of the "nilpotent argument" that shows that after appropriate reordering, we have that $e_i = f_i$ for all i as well.

Hence we see that some $e_i \geq 2$ if and only if $\overline{f} mod p$ has a repeated root $f_i \geq 2$, so $\overline{f}$ is not separable. But this is equivalent to saying that $disc(f) \cong 0 \ mod \ p$, so $p|disc(f)$ ■

20 Lecture April 26th

20.1 Recall:

Last time, we

- introduced definitions of ramified primes, totally split primes, inert primes, and totally ramified primes
- We proved that given a number field K and rational prime p, $p|Disc(K) \iff p$ ramifies in K (we assumed K to be monogenic but it holds it general)
- The main idea of $\mathcal{O}_K = \mathbb{Z}[\theta]$ is that we can understand $\mathcal{O}_K$ well via $minpoly_{\mathbb{Q}}(\theta)$. and that

$$(p) = p_1^{e_1}...p_r^{e_r}$$

The main idea of this proof is also used in proving what's known as the Dedekind-Kummer Theorem (part of why she wanted to become a mathematician).

20.2 Dedekind-Kummer Theorem:

Theorem 20.1 (Dedekind-Kummer)**.** Let $K = \mathbb{Q}(\theta)$ with $\theta \in \mathcal{O}_K$. Let f be the minimal polynomial of θ over $\mathbb{Q}$, and let $p \in \mathbb{Z}$ be a prime rational integer.

Suppose that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. If $\overline{f}(x) = \overline{\pi_1}(x)^{e_1}...\overline{\pi_r}(x)^{e_r}$ be the factorization of $f(x)$ into irreducibles modulo p.

Then,

$$p\mathcal{O}_K = p_1^{e_1}...p_r^{e_r}$$

is the prime factorization of $p\mathcal{O}_K$, where in fact

$$p_i = (p, \pi_i(\theta))$$

for any lift $\pi_i \in \mathbb{Z}[x]$ of $\overline{\pi}_i$.

Note that, we say that $\pi(x)$ is a lift of $\overline{\pi}(x)$ if

$$\pi(x) \ mod \ p = \overline{\pi}(x)$$

Example 20.2. Here are some applications of the Dedekind Kummer Theorem.

- 1) Let $K = \mathbb{Q}(\zeta_5)$, then we have that $\mathcal{O}_K = \mathbb{Z}[\zeta_5]$, so we can apply $D - K$ theorem to the minimal polynomial of ζ_5, which is just $f(x) = x^4 + x^3 + x^2 + 1$.

  Let's try factoring $2\mathcal{O}_K$, then in $f \ mod \ 2$, we claim that $\overline{f}(x)$ is irreducible modulo 2.

  Indeed, if not, then f has either a linear or a quadratic factor modulo 2, but it doesn't have any roots, so no linear factors mod 2.

  As for quadratic factors, suppose it exist, then we have some α such that $deg_{\mathbb{F}_2}(\alpha) = 2$ is a root of f. Hence we have that $\mathbb{F}_2(\alpha) \cong \mathbb{F}_4$, so $\alpha^4 = \alpha$, so α is a root of

  $$x^3 + x^2 + 2x + 1 = x^3 + x^2 + 1 \ (mod \ 2)$$

  So $minpol_{\mathbb{F}_2}(\alpha)|x^3 + x^2 + 1$, but $x^3 + x^2 + 1$ is irreducible in $\mathbb{F}_2$.

  Thus, $\overline{f}(x)$ is irreducible in modulo 2, so in other words, using the D-K Theorem,

  $$2\mathcal{O}_K = (2, 0) = (2)$$

  So we have that (2) is inert since it's a prime ideal in $\mathcal{O}_K$.

- 2) Let's factor $5\mathcal{O}_K$ in $K = \mathbb{Q}(\zeta_5)$, then

$$f(x) \equiv x^4 - 4x^3 + 6x^2 - 4x + 1 \; mod \; 5 \equiv (x-1)^4 \; mod \; 5$$

  So we have that

$$5\mathcal{O}_K = (5, \zeta_5 - 1)^4$$

  , so 5 is totally ramified in $\mathcal{O}_K$.

- 3) Consider $11\mathcal{O}_K$ in $K = \mathbb{Q}(\zeta_5)$, then

$$f(x) \equiv (x-4)(x-9)(x-5)(x-3) \; mod \; 11$$

  So we have that

$$11\mathcal{O}_K = (11, \zeta_5 - 4)(11, \zeta_5 - 9)(11, \zeta_5 - 5)(11, \zeta_5 - 3)$$

  So 11 is totally split in $\mathcal{O}_K$.

- 4) More generally, for $K = \mathbb{Q}(\zeta_n)$ where $n \geq 3$ is prime, p splits completely if and only if $p \equiv 1 \; mod \; n$.

Now we will proceed to prove the Dedekind Kummer Theorem.

Proof. Consider the homomorphism:

$$\phi : \frac{\mathbb{Z}[\theta]}{p\mathbb{Z}[\theta]} \to \frac{\mathcal{O}_K}{p\mathcal{O}_K}$$

By sending (this is well-defined)

$$x + p\mathbb{Z}[\theta] \mapsto x + p\mathcal{O}_K \quad (*)$$

Let $m = [\mathcal{O}_K : \mathbb{Z}[\theta]]$, then by our hypothesis $p \nmid m$.

We claim that ϕ is in fact surjective, indeed, let $x \in \mathbb{O}_K$, then applying Lagrange's Theorem to the quotient group $\mathcal{O}_K/\mathbb{Z}[\theta]$ tells us that

$$y := mx \in \mathbb{Z}[\theta]$$

As adding it m times modulo $\mathbb{Z}[\theta]$ gets it into $\mathbb{Z}[\theta]$.

Let m' be such that $m'm \equiv 1 \; mod \; p\mathbb{Z}[\theta]$, so this implies that $m'm \equiv 1 \; mod \; p\mathcal{O}_K$.

Then we have that

$$\phi(m'y + p\mathbb{Z}[\theta]) = m'mx + p\mathcal{O}_K = x + p\mathcal{O}_K$$

So we have shown that ϕ is indeed surjective. Now recall that

$$\phi : \frac{\mathbb{Z}[\theta]}{p\mathbb{Z}[\theta]} \to \frac{\mathcal{O}_K}{p\mathcal{O}_K}$$

Let $\{\alpha_1, ..., \alpha_n\}$ be an integral basis of $\mathcal{O}_K$ and let $\{1, \theta, ..., \theta^{n-1}\}$ be a basis of $\mathbb{Z}[\theta]$, then clearly $\frac{\mathbb{Z}[\theta]}{p\mathbb{Z}[\theta]}$ has order p^n, and the same with the range.

So ϕ is a function between two rings of the same cardinality, and since ϕ is surjective, ϕ is in fact an isomorphism.

Hence, we have that

$$\frac{\mathbb{Z}[\theta]}{p\mathbb{Z}[\theta]} \cong \frac{\mathcal{O}_K}{p\mathcal{O}_K}$$

Last time we said that

$$\frac{\mathbb{Z}[\theta]}{p\mathbb{Z}[\theta]} \cong \frac{\mathbb{F}_p[x]}{(\overline{f})} \cong \frac{\mathbb{F}_p[x]}{(\overline{\pi}_1^{e_1}(x))} \times ... \times \frac{\mathbb{F}_p[x]}{(\overline{\pi}_r^{e_r}(x))}$$

, where we have that

$$\overline{f} = \overline{\pi_1}^{e_1} ... \overline{\pi_r}^{e_r}$$

is the prime factorzation of $\overline{p}$.

We also have that on the other hand,

$$\mathcal{O}_{\|}/(p) \cong \frac{\mathcal{O}_{\|}}{(p_1^{e_1})} \times ... \times \frac{\mathcal{O}_{\|}}{(p_r^{e_r})}$$

Now since we have shown that (without using Monogenicity)

$$\frac{\mathbb{Z}[\theta]}{p\mathbb{Z}[\theta]} \cong \frac{\mathcal{O}_K}{p\mathcal{O}_K}$$

The same argument as last time implies that the π_i's correspondent to the p_i's and the exponents align after appropriate reordering.

We will finish the proof on the expression next time! ■

21 Lecture April 28th

21.1 Recall:

Last time,

- Birefly revisited the proof that $p|Disc(K) \iff p$ ramifies in K in the monogenic case, but note this holds in general
- Stated Dedekind-Kummer Theorem and proved (albeit somewhat rapidly) the "shape" portion of the theorem, ie.

$$p\mathcal{O}_K = p_1^{e_1}...p_r^{e_r}$$
$$minpoly_{\mathbb{Q}}(x) \equiv \pi_1^{e_1}(x)...\pi_r^{e_r}(x) \ mod \ p$$

- But we haven't proved what exactly $p_1, ..., p_r$ are. That, $p_i = (p, \pi_i(\theta))$

21.2 Finishing the Proof:

Theorem 21.1. Let $K = \mathbb{Q}(\theta), \theta \in \mathcal{O}_K$. Let $f := minpoly_{\mathbb{Q}}(\theta)$, $p \in \mathbb{Z}$ be prime.

Suppose that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. If $\overline{f}(x) = \overline{\pi_1}(x)^{e_1}...\overline{\pi_r}(x)^{e_r} \ mod \ p$ is prime factorization of f modulo p, then

$$p\mathcal{O}_K = p_1^{e_1}...p_r^{e_r}$$

, (**We proved up to here**) where $p_i = (p, \pi_i(\theta))$ for any lift of $\pi_i(x) \in \mathbb{Z}[x]$ of $\overline{\pi_i}(x)$.

Proof. So far we defined a homomorphism

$$\phi : \frac{\mathbb{Z}[\theta]}{p\mathbb{Z}[\theta]} \to \frac{\mathcal{O}_K}{p\mathcal{O}_K}$$
$$x + p\mathbb{Z}[\theta] \mapsto x + p\mathcal{O}_K$$

We argued that since $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$, ϕ becomes an isomorphism remarkably.

Hence, we have that

$$\frac{\mathcal{O}_K}{p\mathcal{O}_K} \cong \frac{\mathbb{Z}[\theta]}{p\mathbb{Z}[\theta]} \cong \frac{\mathbb{Z}[x]}{(p, f(x))} \cong \frac{\mathbb{F}_p[x]}{(\overline{f}(x))}$$
$$\frac{\mathcal{O}_K}{p\mathcal{O}_K} \cong \frac{\mathcal{O}_K}{p_1^{e_1}} \times ... \times \frac{\mathcal{O}_K}{p_r^{e_r}}$$
$$\frac{\mathbb{F}_p[x]}{(\overline{f}(x))} \cong \frac{\mathbb{F}_p[x]}{\overline{\pi_1}^{f_1}} \times ... \times \frac{\mathbb{F}_p[x]}{\overline{\pi_s}^{f_s}}$$

"Comparing the nilpotent orders" or an argument with chains of ideals shows that $r = s$ and $e_i = f_i$ after some reordering, hence

$$\mathcal{O}_K/p_i \cong \mathbb{F}_p[x]/(\overline{\pi}_i(x))$$

Since p_i is a prime ideal and non-zero ideals are maximal, $\mathcal{O}_K/p_i$ is remarkably a finite field. Moreover, since $(p) \subset p_i$, we also have that the finite field has characteristic p.

Thus, $\mathcal{O}_K/p_i$ is a finite extension of $\mathbb{F}_p$, call the degree of extension f_i (abuse of notation, not the same as before).

Since $\overline{\pi_i}(x)$ is an irreducible polynomial in $\mathbb{F}_p[x]$, we have that

$$f_i = deg\overline{\pi_i}(x)$$

This f_i is called **the inertial degree of** p_i **over** p, so we have that

$$|\mathcal{O}_K/p_i| = p^{f_i} = p^{deg(\overline{\pi_i})}$$

The ideal $(\overline{\pi}_i(x))/(\overline{f}) \subset \frac{\mathbb{F}_p[x]}{(\overline{f})}$ correspond via the chain of isomorphisms prior to the ideal $p_i/p\mathcal{O}_K$. The 3rd isomorphism theorem then says that $(p, \pi_i(\theta))$ (for any life π_i) is the only possible lift of $p_i/p\mathcal{O}_K$ to $\mathcal{O}_K$. ■

Remark 21.2 (Dedekind's Revenge)**.** What if $p|[\mathcal{O}_K : \mathbb{Z}[\theta]]$?

If $K = \mathbb{Q}(\sqrt{-3})$, then $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}] = \mathbb{Z}[\omega]$.

Let $\theta = \sqrt{-3}$, so that $[\mathcal{O}_K : \mathbb{Z}[\theta]] = 2$ (We can argue that the $disc(x^2+3) = -12$ while $disc(K) = disc(x^2+x+1) = -3$, then

$$[\mathcal{O}_K : \mathbb{Z}[\theta]] = \sqrt{(-12/-3)} = 2$$

Get $(x^2+3) = x^2 - 1 = (x-1)^2 \ mod\ 2$, then incorrectly applying the DK-Theorem gives us that 2 ramifies in $\mathcal{O}_K$.

OTOH, using DK correctly gives us $x^2 + x + 1 \ mod\ 2$ has no roots in $mod\ 2$ and is thus irreducible over $\mathbb{F}_2$, thus the correct conclusion is that (2) is actually inert in $K = \mathbb{Q}(\sqrt{-3})$.

21.3 Ramification degrees, inert degrees, primes upstairs and downstairs

Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. We showed that $\mathcal{O}_K/\mathfrak{p}$ is a fintie field with charactersitic p, where $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ (contraction of maximal ideal to $\mathbb{Z}$ is still a maximal ideal).

Thus, $\mathcal{O}_K/\mathfrak{p}$ is a finite extension of $\mathbb{Z}/p\mathbb{Z}$ with degree f. f is called the **inertial degree**.

We can think of $\mathcal{O}_K/\mathfrak{p}$ as a $\mathbb{F}_p$-vector-space - it's a quotient of $\mathbb{Z}/p\mathbb{Z}$-vector-space $\mathcal{O}_K/(p)$ (since $(p) \subset \mathfrak{p}$).

But we have said that

$$|\mathcal{O}_K/(p)| = p^n, n = [K : \mathbb{Q}]$$

Thus, we observe that $f \leq n$ using some linear algebra,

If $p\mathcal{O}_K = \mathfrak{p}^e p_2^{e_2} ... p_r^{e_r}$, then e is called the **ramification index / ramification degree** of $\mathfrak{p}$ over p.

We write $e(\mathfrak{p}|p)$ as the ramification index, and $f(\mathfrak{p}|p)$ as the inertial degree.

We say that $\mathfrak{p}$ **lies above** p in K, and that p lies below $\mathfrak{p}$ in $\mathbb{Q}$.

Colloquially $\mathfrak{p}$ is a "prime upstairs" and p is a "prime downstairs".

21.4 Fundamental Identity

Theorem 21.3 (Fundamental Identity)**.** Let $p \in \mathbb{Z}$ be prime, and suppose $[K : \mathbb{Q}] = n$ and $p\mathcal{O}_K = p_1^{e_1} ... p_g^{e_g}$ is the prime factorization of $p\mathcal{O}_K$, where $f_i = f(p_i|p)$.

Then, the sum

$$\sum_{i=1}^{g} e_i f_i = n$$

Remark 21.4. When p is totally ramified, $e_1 = n$, $f_1 = 1$.

When p is inert, $[\mathcal{O}_K/p : \mathbb{F}_p] = n$.

When K is Galois, the e_i for $1 \leq i \leq g$ are all the same, and similarly for f_i's (Look back at $\mathbb{Q}(\zeta_5)$ examples)

Proof. In the monogenic case, the proof is remarkably simplified, this is because the f_i's are remarabkly easy to find.

We had that

$$\mathcal{O}_K/p_i \cong \mathbb{F}_p[x]/\overline{\pi_i}(x)$$
$$\mathcal{O}_K/(p) \cong ... \cong \mathbb{F}_p/(\overline{f})$$

, where $deg(\overline{f}) = n$ and $|\mathbb{F}_p[x]/(\overline{\pi_i}^{e_i})| = p^{e_i deg(\pi_i)} = p^{e_i f_i}$.

And we can multiply the $p^{e_i f_i}$ back to p^n, so $\sum_i e_i f_i = n$ ■

22 Last Lecture: Minkowski, Lagrange, and Waring Walk into a Bar

22.1 1. Four Squares Theorem and Waring's Problem

Theorem 22.1 (Lagrange, 1770)**.** Every non-negative integer can be written as a sum of four square integers.

Remark 22.2. In the same year Waring asseted, in his book, that for every integer $k \geq 2$, there is a $g(k)$ such that every non-negative integers can be written as the sum of at most $g(k)$ k-th powers.

So the Four Square Theorem is the same as saying $g(2) = 4$.

Waring then claimed that $g(3) = 9$ and $g(4) = 19$. Note that 23 and 239 each requires 9 cubes, and 79 required 19 fourth powers.

The assertion was proven by Hilbert in 1909.

$g(3) = 9$ was proven by Wiefreich-Kamper in 1909, and $g(4) = 19$ was proved in 1986 by Balasubramanian, Dress, and Deshuvilles.

Remark 22.3. Another interesting question to ask is what is the "Asymptotic version" of $g(k)$ is, which we denote as $G(k)$.

We know that

$$4 \leq G(3) \leq 7$$
$$G(4) = 16$$

So in general, the mileage differs on these.

22.2 2. Lattices and Minkowski's Theorem

Definition 22.4. Let $e_1, ..., e_n$ be a set of basis vectors for $\mathbb{R}^n$. Then the additive subgroup of $(\mathbb{R}^n, +)$ generated by $e_1, ..., e_n$ is called a **lattice**.

Example 22.5. $\mathbb{Z}^n$ is the most obvious lattice in $\mathbb{R}^n$, generated by the standard basis.

$\alpha\mathbb{Z}^n$ for $0 \neq \alpha \in \mathbb{R}$ is also an obvious choice.

Also things, like $\frac{1}{2}\mathbb{Z} \times \mathbb{Z} \subset \mathbb{R}^2$ is also a lattice.

Definition 22.6. If L is a lattice generated by $e_1, ..., e_n$ in $\mathbb{R}^n$, then the **fundamental domain** of L is the set

$$\{\sum_{i=1}^{n} a_i e_i | a_i \in \mathbb{R}, 0 \leq a_i < 1\}$$

Definition 22.7. A set $X \subset \mathbb{R}^n$ is convex if for all $x, y \in X$,

$$\lambda(x) + (1 - \lambda)y \in X, \lambda \in [0, 1]$$

X is **symmetric** if $x \in X \implies -x \in X$.

Theorem 22.8 (Minkowski, pg. 140 of S + T)**.** Let L be an (n-dimensional) lattice in $\mathbb{R}^n$ with foundamental domain T, and let X be a bounded, symmetric, convex subset of $\mathbb{R}^n$. If

$$vol(X) > 2^n vol(T)$$

Then X contains a non-zero point of L.

(We note that a symmetric and convex set necessarily centers around the origin).

Remark 22.9. If T is the fundamental domain of standard basis in $\mathbb{R}^2$, ie. $L = \mathbb{Z}^2$, then clearly $vol(T) = 1$ our statement says

$$vol(X) > 4$$

The intuition is that the four squares around the xy-axis has area 4, so X has to contain a lattice point.

Lemma 22.10. Let $f : \mathbb{R}^n \to \mathbb{R}^n$ be a linear transformation, let X be symmetric and convex, then $f(X)$ is also symmetric and convex.

Theorem 22.11. Every non-negative integer can be written as a sum of four square integers.

Proof. We will first prove the statement for prime numbers, then we will extend this to all positive integers.

Clearly $2 = (1)^2 + (1)^2 + 0^2 + 0^2$ is a sum of four squares. Now we want to prove this for an odd prime.

We **claim that** $r^2 + s^2 + 1 \equiv 0 \mod p$ has a solution where $(r, s) \in \mathbb{Z}^2$, indeed this is because every element of $\mathbb{Z}/p\mathbb{Z}$ can be written as the sum of two squares, the main idea is to do this $p \mod 4$ and use Quadratic Residues, the details are left as exercise.

Select such an r, s. Now consider the lattice $\Lambda \subset \mathbb{Z}^4$ given by

$$\Lambda = A\mathbb{Z}^4$$

, where $A = \begin{pmatrix} p & 0 & r & s \\ 0 & p & s & -r \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

If $\vec{t} = (t_1, t_2, t_3, t_4) \in \mathbb{Z}^4$ and $\vec{x} = (x_1, x_2, x_3, x_4)$ where $\vec{x} = A\vec{t}$. Then I claim that

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \mod p$$

Indeed, we have that

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= (pt_1 + rt_3 + st_4)^2 + (pt_2 + st_3 - rt_4)^2 + (t_3)^2 + (t_4)^2 \mod p \\ &\equiv (rt_3 + st_4)^2 + (st_3 - rt_4)^2 + t_3^2 + t_4^2 \mod p \\ &\equiv (1 + r^2 + s^2)(t_3^2 + t_4^2) \mod p && \text{Try to Compare Coefficients} \\ &\equiv 0 \mod p && \text{Since } 1 + r^2 + s^3 \equiv 0 \mod p \end{aligned}$$

The idea now is that we will construct a ball around the origin that's small enough so that Minkowski's Theorem tell us that their sum has to be the prime p.

Recall that a 4-dimensional ball of radius R has volume

$$V(R) = \frac{\pi^2 R^4}{2}$$

Now we will choose R such that

$$(i)\ 16p^2 < V(R) \implies 2p <\approx 1.11R^2$$
$$(ii)\ R^2 < 2p$$

Thus we want R such that

$$R^2 < 2p <\approx 1.11R^2$$

So taking $R^2 = 1.9p$ works. Let X be the ball centered at the origin in $\mathbb{R}^4$ of radius $R = \sqrt{1.9p}$. Let T be the fundamental domain of $\Lambda = A\mathbb{Z}^4$.

Then

$$vol(T) = det(A) = p^2$$

Since from (i), we have that

$$V(R) > 16p^2 = 2^4 vol(T)$$

So we can apply Minkowski's Theorem, X contains some non-zero lattice point of Λ say $(x_1, x_2, x_3, x_4) \neq (0, 0, 0, 0)$.

Furthermore, we know that $x_1^2 + x_2^2 + x_3^2 + x_4^2 = np$ for some $n \in \mathbb{N}$. Howeverm subce $R^2 < 2p$, the square of norm of the vector is less than $2p$, so we have to have the case that

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$$

Now for the case of natural numbers, we claim that for any two positive integers a, b that can be written as a sum of 4 squares, ab is also a sum of 4 squares. Indeed, this follows from property of Quarternions.

More explicitly,

$$(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2)$$
$$= (aA - bB - cC - dD)^2 + (aB + bA + cD - dC)^2 + (aC - bD + cA + dB)^2 + (aD + bC - cB + dA)^2$$

■

23 Appendix

This section contains some important theorems that were covered in Problem Sets of the course but were not covered during lecture.

23.1 Dedekind Domains are 2-generated Ideal Domains

In this section, we will show that every integral ideal of Dedekind Domain $\mathcal{O}_K$ can be generated by 2 elements it contains.

Lemma 23.1. Suppose $\mathfrak{a}, \mathfrak{b}$ are comaximal, then $\mathfrak{a}^n$ and $\mathfrak{b}$ are also comaximal in $\mathcal{O}_K$ for all integers $n \geq 1$

Proof. Let's induct on n, clearly when $n = 1$, this is trivial.

Now suppose our inductive hypothesis is true until $n = k$, meaning that $\mathfrak{a}^k + \mathfrak{b} = (1)$. Then we wish to show that $\mathfrak{a}^{k+1} + \mathfrak{b} = (1)$.

Indeed, it suffices for us to show that $1 \in \mathfrak{a}^{k+1} + \mathfrak{b}$, since the other direction is trivial. Since $\mathfrak{a} + \mathfrak{b} = 1$, there exist some element $a \in \mathfrak{a}, b \in \mathfrak{b}$ such that $a + b = 1$.

Since $\mathfrak{a}^k + \mathfrak{b} = (1)$, this means that there exist some element $x \in \mathfrak{a}^k, y \in \mathfrak{b}$ such that $x + y = 1$, now

$$1 = (a + b)(x + y) = ax + bx + by + ay = ax + (bx + by + ay)$$

Since $a \in \mathfrak{a}, x \in \mathfrak{a}^k$, clearly $ax \in \mathfrak{a}^{k+1}$. Since $b \in \mathfrak{b}, y \in \mathfrak{b}$, we have that $bx + by + ay \in \mathfrak{b}$, thus 1 is the sum of an element from $\mathfrak{a}^{k+1}$ and $\mathfrak{b}$, so $1 \in \mathfrak{a}^{k+1} + \mathfrak{b}$. ■

Corollary 23.2. Suppose $\mathfrak{a}, \mathfrak{b}$ are comaximal, then $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are also comaximal for any integers $n, m \geq 1$

Proof. Apply Lemma 23.1 for the first time shows us that $\mathfrak{a}^m$ and $\mathfrak{b}$ are comaximal. Applying Lemma 23.1 the second time shows us that $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are comaximal. ■

Corollary 23.3. Suppose $\mathfrak{p}_1, ..., \mathfrak{p}_n$ are pairwise comaximal, then $\mathfrak{p}_1^{e_1}, ..., \mathfrak{p}_n^{e_n}$ are pairwise comaximal for any integer $e_1, ..., e_n \geq 1$

Proof. Apply Corollary 23.2 on each pair. ■

Lemma 23.4. Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{e}$ be pairwise comaximal ideals, then $\mathfrak{ab}$ and $\mathfrak{e}$ are comaximal.

Proof. Again, it suffcies for us to show that $1 \in \mathfrak{ab} + \mathfrak{e}$. Indeed, since $1 \in \mathfrak{a} + \mathfrak{e}$, $1 \in \mathfrak{b} + \mathfrak{e}$, we have that there exist $a \in \mathfrak{a}, b \in \mathfrak{b}, e_1, e_2 \in \mathfrak{e}$ such that

$$a + e_1 = 1, b + e_2 = 1$$

Now we have that

$$1 = (a + e_1)(b + e_2) = ab + (ae_2 + be_1 + e_1e_2)$$

Then clearly $ab \in \mathfrak{ab}$ and $ae_2 + be_1 + e_1e_2 \in \mathfrak{e}$, so $1 \in \mathfrak{ab} + \mathfrak{e}$. ■

Theorem 23.5. Let I be an integral ideal of $\mathcal{O}_K$, then I is either principal or generated by 2 elements.

Proof. If I is the zero ideal, then $I = (0)$ is already principal.

If $I = \mathcal{O}_K$ the entire ring, then $I = (1)$ is also principal.

Now if I is a non-zero non-unit ideal, then we can choose some $a \in I$ where $a \neq 0$.

Since we proved that unique factorization of ideals exist in $\mathcal{O}_K$, we can write

$$I = \mathfrak{p}_1^{e_1} ... \mathfrak{p}_r^{e_r}$$

as I's unique factorization of prime ideals $\mathfrak{p}_1, ..., \mathfrak{p}_r$.

Now since $a \in I$, we have that (a), the principal ideal generated by a, is also a subset of I. So $(a) \subset I$. Moreover, we proved in lecture that $(\mathfrak{a}) \subset I$ if and only if $I|(a)$, so in other words, the unique prime factorization of (a) would be

$$(a) = \mathfrak{p}_1^{f_1}...\mathfrak{p}_r^{f_r}\mathfrak{q}_1^{g_1}...\mathfrak{q}_s^{g_s}, f_1 \geq e_1, ..., f_r \geq e_r$$

Now, we claim that there exist some element $b \in I$ such that its unique prime factorization is

$$(b) = \mathfrak{p}_1^{e_1}...\mathfrak{p}_r^{e_r}\mathfrak{a}_1^{h_1}...\mathfrak{a}_t^{h_t}$$

, where each $\mathfrak{a}_i$ is distinct from any of $\mathfrak{q}_1, ..., \mathfrak{q}_s$.

Indeed, we claim it suffices for us to find an element $b \in I$ such that $b \notin \mathfrak{p}_1^{e_1+1}$, ... $b \notin \mathfrak{p}_r^{e_r+1}$ and $b \notin \mathfrak{q}_1$, ..., $b \notin \mathfrak{q}_s$.

This is because since $b \in I$, we have that $I|(b)$, so b has prime factors $\mathfrak{p}_1^{e_1}...\mathfrak{p}_r^{e_r}$, but this any of those $\mathfrak{p}_i$ has more than e_i in their exponent, this should imply that $b \in \mathfrak{p}_i^{e_i+1}$ and hence a contradiction. Thus, the order of each $\mathfrak{p}_i$ for (b) is e_i.

Moreover, if (b)'s unique factorization shares any common factor with at least one of $\mathfrak{q}_1, ..., \mathfrak{q}_s$, say $\mathfrak{q}_j$, then it automatically means that $b \in \mathfrak{q}_j$, so we again have a contradiction. Thus, the order of each $\mathfrak{q}_j$ in (b) is 0.

Now we want to prove we can find this said b. Indeed, clearly for each $\mathfrak{p}_i$, $\mathfrak{p}_i^{e_i+1} \neq \mathfrak{p}_i^{e_i}$ (or else factorization won't be unique), so we pick some element $b_i \in \mathfrak{p}_i^{e_i} - \mathfrak{p}_i^{e_i+1}$. Now let $b_{r+1}, ..., b_{r+s}$ all be 1 respectively Let $\mathfrak{b}_1 = \mathfrak{p}_1^{e_1+1}, ..., \mathfrak{b}_r = \mathfrak{p}_r^{e_r+1}, \mathfrak{b}_{r+1} = \mathfrak{q}_1, ..., \mathfrak{b}_{r+s} = \mathfrak{q}_s$, then for each $\mathfrak{b}_i$, Lemma 23.4 tells us that $\mathfrak{b}_i$ and $\prod_{j \neq i} \mathfrak{b}_j$ are comaximal, so there exist some $x_i \in \prod_{j \neq i} \mathfrak{b}_j$ and $y_i \in \mathfrak{b}_i$ such that $x_i + y_i = 1$.

Now let

$$b = \sum_{i=1}^{r+s} b_i x_i$$

We claim that this is the b we are looking for. Indeed, clearly each $b_i x_i \in \prod_{i=1}^{r+s} \mathfrak{b}_i$, and since I divides $\prod_{i=1}^{r+s} \mathfrak{b}_i$, we have that it is a subset of I, so $b \in I$.

Now, we wish to show that b is not in any of the $\mathfrak{b}_i$. Indeed, it suffices for us to show that b does not vanish when quotienting it under $\mathfrak{b}_i$, indeed, for any arbitrary $\mathfrak{b}_k$

$$\begin{aligned} b &\equiv \sum_{i=1}^{r+s} b_i x_i \mod \mathfrak{b}_k \\ &\equiv b_k x_k \mod \mathfrak{b}_k && \text{Every other } x_i \text{ is contained in } \mathfrak{b}_k \\ &\equiv b_k(1 - y_k) \mod \mathfrak{b}_k && \text{Recall } x_k + y_k = 1, y_k \in \mathfrak{b}_k \\ &\equiv b_k \mod \mathfrak{b}_k \end{aligned}$$

Now if $k \in [1, r]$, then we established earlier that we picked b_k so that $b_k \in \mathfrak{p}_k^{e_k} - \mathfrak{p}_k^{e_k+1}$, so $b_k \notin \mathfrak{b}_k$. If $k \in [r+1, r+s]$, then $b_k = 1$ is clearly not in $\mathfrak{b}_k$ since it's not the unit ideal.

Thus, we have found our desired b (Note we basically just gave a constructive use of the CRT)

Now we claim that $I = (a, b)$. Indeed, we first note that the following two product of prime ideals are comaximal

$$(i)\mathfrak{p}_1^{f_1-e_1}...\mathfrak{p}_r^{f_r-e_r}\mathfrak{q}_1^{g_1}...\mathfrak{q}_s^{g_s}$$

$$(ii)\mathfrak{a}_1^{h_1}...\mathfrak{a}_t^{h_t}$$

Indeed, from Corollary 24.3 and the fact that $\mathfrak{p}_1, ...\mathfrak{p}_r, \mathfrak{q}_1, ..., \mathfrak{q}_s, \mathfrak{a}_1, ..., \mathfrak{a}_t$ are pairwise distinct prime ideals and thus pairwise comaximal, so we have that the list

$$\mathfrak{p}_1^{f_1-e_1}, ..., \mathfrak{p}_r^{f_r-e_r}, \mathfrak{q}_1^{g_1}, ..., \mathfrak{q}_s^{g_s}, \mathfrak{a}_1^{h_1}, ..., \mathfrak{a}_t^{h_t}$$

is pairwise comaximal. Then repeated applications of Lemma 23.4 shows us that (i) and (ii) are comaximal ideals.

Thus, we have that

$$\mathfrak{p}_1^{f_1-e_1}...\mathfrak{p}_r^{f_r-e_r}\mathfrak{q}_1^{g_1}...\mathfrak{q}_s^{g_s} + \mathfrak{a}_1^{h_1}...\mathfrak{a}_t^{h_t} = (1)$$

Now multiplying both sides by $I = \mathfrak{p}_1^{e_1}...\mathfrak{p}_r^{e_r}$ and recall that we showed that ideal products are distributive over addition, we have that

$$\mathfrak{p}_1^{e_1}...\mathfrak{p}_r^{e_r}(\mathfrak{p}_1^{f_1-e_1}...\mathfrak{p}_r^{f_r-e_r}\mathfrak{q}_1^{g_1}...\mathfrak{q}_s^{g_s} + \mathfrak{a}_1^{h_1}...\mathfrak{a}_t^{h_t}) = \mathfrak{p}_1^{f_1}...\mathfrak{p}_r^{f_r}\mathfrak{q}_1^{g_1}...\mathfrak{q}_s^{g_s} + \mathfrak{p}_1^{e_1}...\mathfrak{p}_r^{e_r}\mathfrak{a}_1^{h_1}...\mathfrak{a}_t^{h_t}$$

$$= (a) + (b)$$

$$\mathfrak{p}_1^{e_1}...\mathfrak{p}_r^{e_r}(\mathfrak{p}_1^{f_1-e_1}...\mathfrak{p}_r^{f_r-e_r}\mathfrak{q}_1^{g_1}...\mathfrak{q}_s^{g_s} + \mathfrak{a}_1^{h_1}...\mathfrak{a}_t^{h_t}) = \mathfrak{p}_1^{e_1}...\mathfrak{p}_r^{e_r}(1) = \mathfrak{p}_1^{e_1}...\mathfrak{p}_r^{e_r} = I$$

Thus, we have that

$$I = (a) + (b) = (a, b)$$

Thus, I is a 2-generated ideal. ■

23.2 Infinitude of Primes in $\mathcal{O}_K$

In this section, we will show that $\mathcal{O}_K$ has infinity many prime ideals. We accomplish this by mimicking Euclid's Infinitude of Prime argument onto $\mathcal{O}_K$.

Theorem 23.6. $\mathcal{O}_K$ has infinitely many prime ideals.

Proof. First we will show that $\mathcal{O}_K$ has at least 1 non-zero prime ideal. Indeed, this just comes from the fact that the maximal ideal, which is prime, of $\mathcal{O}_K$ is not the zero ideal. This is because $\mathcal{O}_K$ contains some non-zero non-unit elements (for example 2 is not a unit in $\mathcal{O}_K$ since its inverse $1/2$ is not an algebraic integer), and that from Zorn's Lemma, every non-unit element in a ring is contained in some maximal ideal.

It now suffices for us to show that $\mathcal{O}_K$ has infinitely many non-zero prime ideals. Indeed, suppose for the sake of contradiction that $\mathcal{O}_K$ only has finitely many non-zero prime ideals, say $\mathfrak{p}_1, ..., \mathfrak{p}_n$.

Now we claim that for each of these $\mathfrak{p}_i$, we can find some non-zero rational integer $a_i \in \mathfrak{p}_i$. Indeed, take any non-zero algebraic integer $r_i \in \mathfrak{p}_i$, then r_i is the root of a minimal integer polynomial $f(x) \in \mathbb{Z}[x]$, we can split $f(x)$ into $f(x) = g(x) + c$ where $g(0) = 0$ and c is the constant term of $f(x)$. c has to be non-zero or else $f(x)$ wouldn't be minimal.

Then we note that

$$g(r_i) = -c$$

But since $g(x)$ is an integer polynomial, $g(r_i)$ is just the integral sum of powers of r_i, which is closed in the ideal $\mathfrak{p}_i$, so $-c \in \mathfrak{p}_i$ is a non-zero integer.

Moreover, since additive inverse is closed in an ideal, we can take $a_i \in \mathfrak{p}_i$ to be positive.

Now, consider the term $[\prod_{j=1}^n a_j] + 1 \in \mathcal{O}_K$. It is certainly not contained in any of the $\mathfrak{p}_i$ because $a_i \in \mathfrak{p}_i$, so in particular it is not projected to zero when modding $\mathcal{O}_K$ by $\mathfrak{p}_i$:

$$[\prod_{j=1}^{n} a_j] + 1 \equiv 1 \mod \mathfrak{p}_i$$

However, we recall that we have proved in a previous homework that $[\prod_{j=1}^{n} a_j] + 1$ is a unit in $\mathcal{O}_K$ if and only if $N_{K/\mathbb{Q}}([\prod_{j=1}^{n} a_j]+1) = \pm 1$, but $[\prod_{j=1}^{n} a_j]+1$ is an integer and is greater than 1 since we chose a_i's to all be positive, so

$$N_{K/\mathbb{Q}}([\prod_{j=1}^{n} a_j] + 1) = ([\prod_{j=1}^{n} a_j] + 1)^{[K:\mathbb{Q}]} > 1$$

Thus,$[\prod_{j=1}^{n} a_j] + 1$ is not a unit in $\mathcal{O}_K$. But then Zorn's Lemma tells us that every non-unit element is contained in some maximal ideal, which is prime. But this means that $[\prod_{j=1}^{n} a_j] + 1$ is contained in one of the $\mathfrak{p}_1, ..., \mathfrak{p}_n$, so we have a contradiction.

Thus, we conclude that $\mathcal{O}_K$ has infinitely many prime ideals. ■

References

[IR11] Kenneth F. Ireland and Michael I. Rosen. *A classical introduction to modern number theory*. Springer, 2011.

[ST20] Ian Stewart and David Orme Tall. *Algebraic Number Theory and Fermat's last theorem*. CRC Press, Taylor amp; Francis Group, 2020.