Contents

Chapter 1

Unique Factorization

1.1 Unique Factorization in $\mathbb{Z}$

It will be more convenient to work with $\mathbb{Z}$ rather than restricting ourselves to the positive integers. The notion of divisibility carries over with no difficulty to $\mathbb{Z}$. If p is a positive prime, $-p$ will also be a prime. We shall not consider 1 or -1 as primes even though they fit the definition. This is simply a useful convention. They are called the units of $\mathbb{Z}$.

There are a number of simple properties of division that we shall simply list.

1. $a \mid a, a \neq 0$.
2. If $a \mid b$ and $b \mid a$, then $a = \pm b$.
3. If $a \mid b$ and $b \mid c$, then $a \mid c$.
4. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

Lemma 1 Every nonzero integer can be written as a product of primes.

Theorem 1.1.1 For every nonzero integer n there is a prime factorization

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

with the exponents uniquely determined by n. In fact, we have $a(p) = \operatorname{ord}_p n$.

The proof if this theorem if is not as easy as it may seem. We shall postpone the proof until we have established a few preliminary results.

Lemma 2 If $a, b \in \mathbb{Z}$ and $b \geq 0$, there exist $q, r \in \mathbb{Z}$ such that $a = qb + r$ with $0 \leq r < b$.

Definition 1.1.1 If $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, we define $(a_1, a_2, \ldots, a_n)$ to be the set of all integers of the form $a_1x_1 + a_2x_2 + \cdots + a_nx_n$ with $x_1, x_2, \ldots, x_n \in \mathbb{Z}$.

Remark 1.1.1 Let $A = (a_1, a_2, \ldots, a_n)$. Notice that the sum and difference of two elements in A are again in A. Also, if $a \in A$ and $r \in \mathbb{Z}$, then $ra \in A$, i.e., A is an ideal in the ring $\mathbb{Z}$

Lemma 3 If $a, b \in \mathbb{Z}$, then there is a $d \in \mathbb{Z}$ such that $(a, b) = (d)$

Definition 1.1.2 Let $a, b \in \mathbb{Z}$. An integer d is called a greatest common divisor of a and b if d is a divisor of both a and b and if every other common divisor of a and b divides d.

Remark 1.1.2 The gcd of two numbers, if it exists, is determined up to sign.

Lemma 4 Let $a, b \in \mathbb{Z}$. If $(a, b) = (d)$ then d is a greatest common divisor of a and b.

Definition 1.1.3 We say that two integers a and b are relatively prime if the only common divisors are ± 1, the units.

It's fairly standard to use the notation (a, b) for the greatest common divisor of a and b. With this convention we can say that a and b are relatively prime if $(a, b) = 1$.

Proposition 1.1.2 Suppose that $a \mid bc$ and that $(a, b) = 1$. Then $a \mid c$.

Corollary 1.1.3 If p is a prime and $p \mid bc$, then either $p \mid b$ or $p \mid c$.

Corollary 1.1.4 Suppose that p is a prime and that $a, b \in \mathbb{Z}$. Then $\mathrm{ord}_p ab = \mathrm{ord}_p a + \mathrm{ord}_p b$.

1.2 Unique Factorizaion in a Principal Ideal Domain

For this section, we mostly refer to Section 1.5 and supply some details.

1.3 Unique Factorization in $k[x]$

In this section we consier the ring $k[x]$ of polynomials with coefficients in a field k. If $f, g \in k[x]$, we say that f divides g if there is an $h \in k[x]$ such that $g = fh$.

If $\deg f$ denotes the degree of f, we have $\deg fg = \deg f + \deg g$ (why? Because a field k is necessarily an integral domain). nonzeros constants are the units of $k[x]$. A nonconstant polynomial p is said to be irreducible if $q \mid p \implies q$ is either a constant or a constant times p.

Lemma 5 Every nonconstant polynomial is the product of irreducible polynomials.

Proof. Simply by induction. ■

Definition 1.3.1 A polynomial f is called monic if its leading coefficient is 1.

Definition 1.3.2 Let p be a monic irreducibe polynomial. We define $\mathrm{ord}_p f$ to be the integer a defined by the property that $p^a \mid f$ but that $p^{a+1} \nmid f$.

Remark 1.3.1 $\mathrm{ord}_p f = 0$ iff $p \nmid f$.

Theorem 1.3.1 Let $f \in k[x]$. Then we can write

$$f = c \prod_p p^{a(p)},$$

where the product is over all monic irreducible polynomials and c is a constant. The constant c and the exponents $a(p)$ are uniquely determined by f; in fact, $a(p) = \mathrm{ord}_p f$.

The existence of such a product follows immediately from Lemma 5. The uniqueness part is more difficult and will be postponed.

Lemma 6 Let $f, g \in k[x]$. If $g \neq 0$, there exist polynomials $h, r \in k[x]$ such that $f = hg + r$, where either $r = 0$ or $r \neq 0$ and $\deg r \leq \deg g$.

Proof. If $g \mid f$, we are done. If $g \nmid f$, let $r = f - hg$ be the polynomial of least degree among all polynomials of the form $f - lg$ with $l \in k[x]$. We claim that $\deg r < \deg g$. If not, let the leading term of r be ax^d and that g be bx^m. Then $r - \frac{a}{b}x^{d-m}g(x) = f - (h + \frac{a}{b}x^{d-m})g$ has smaller degree than r and is of the given form. This is a contradiction. ■

Lemma 7 Given $f, g \in k[x]$ there is a $d \in k[x]$ such that $(f, g) = (d)$.

Proof. See Theorem 1.6.1. ■

Definition 1.3.3 Let $f, g \in k[x]$. Then $d \in k[x]$ is said to be a greatest common divisor of f and g if d divides f and g and every common divisor of f and g divides d.

Remark 1.3.2 Notice that the greatest common divisor of two polynomials is determined up to multiplication by a constant. If we require it to be monic, it is uniquely determined and we may speak of the greatest common divisor.

Lemma 8 Let $f, g \in k[x]$ By lemma 7 there is a $d \in k[x]$ such that $(f, g) = (d)$. d is the greatest common divisor of f and g.

Proof. Since $f \in (d)$ and $g \in (d)$ we have $d \mid f$ and $d \mid g$. Suppose that $h \mid f$ and that $h \mid g$. Then h divides every elements in $(f, g) = (d)$. In particular $h \mid d$, we are done. ■

Definition 1.3.4 Two polynomial f and g are said to be relatively prime if the only common divisor of f and g are constants. In other words, $(f, g) = (1)$.

Proposition 1.3.2 If f and g are relatively prime and $f \mid gh$, then $f \mid h$.

Corollary 1.3.3 If p is an irreducible polynomial and $p \mid fg$, then $p \mid g$ or $p \mid g$.

Corollary 1.3.4 If p is a monic irreducible polynomial and $f, g \in k[x]$, we have

$$\operatorname{ord}_p fg = \operatorname{ord}_p f + \operatorname{ord}_p g.$$

Using these tools, we can prove the uniqueness of factorizaion.

1.4 Class Notes 17-01-10

For us, ring means commutative ring with identity.

Definition 1.4.1 A *ring* is a set with two binary operations $(+, \cdot)$ satisfying

1. $(R, +)$ is an *abelian group*, which means
   - $+$ is commutative and associative.
   - $\exists\, 0_R, a = a + 0_R = 0_R + a$ for all $a \in R$.
   - Given $a \in R$, $\exists a' \in R$ such that $a + a' = 0_R$.
2. $\cdot$ is commutative and associative.
   $\exists\, 1_R$ such that $a \cdot 1_R = 1_R \cdot a = a$ for all $a \in R$.
3. $\cdot$ is distributive over addition, which means
   - $a \cdot (b + c) = a \cdot b + a \cdot c$
   - $(a + b) \cdot c = a \cdot c + b \cdot c$

Exercise 1.4.1

1. Show that $a + b = a + c \Rightarrow b = c$.(Cancellation)

Proof.

$$\begin{aligned} a+b=a+c &\Leftrightarrow a'+(a+b)=a'+(a+c) \\ &\Leftrightarrow (a'+a)+b=(a'+a)+c \\ &\Leftrightarrow 0_R+b=0_R+c \\ &\Leftrightarrow b=c \end{aligned}$$

■

2. Show a' is unique. We denote this a' by $-a$.

   Proof. if the statement doesn't hold, then there exist a', a'' such that $a + a' = 0_R = a + a''$. We then apply cancellation and get $a' = a''$. ■

3. Show 0_R is unique.

   Proof. Say there are two zero element 0_R and $0'_R$, then we have

   $$0_R = 0_R + 0'_R = 0'_R$$

   ■

4. Show 1_R is unique.

   Proof. Say there are two unit element 1_R and $1'_R$, then we have

   $$1_R = 1_R \cdot 1'_R = 1'_R$$

   ■

5. Show $a \cdot 0_R = 0_R \cdot a = 0_R$

   Proof. We know that $a \cdot 0_R + a = a \cdot (0_R + 1_R) = a \cdot 1_R = a = 0_R + a$, apply cancellation then we are done. ■

6. Show that $(-1_R) \cdot a = -a$.

   Proof. Since $a \cdot 0_R = 0_R$, we have $a \cdot (1_R + (-1_R)) = 0_R$ or $a + (-1_R) \cdot a = 0_R$. Then $-a = (-1_R) \cdot a$, for a' is unique. ■

7. The zero ring is the ring with 1 element. Show R is zero ring $\Leftrightarrow 1_R = 0_R$.

   Proof.
   " $\Rightarrow$ " : Trivial.
   " $\Leftarrow$ " : Since we have $a \cdot 1_R = 1_R \cdot a = a$ for all $a \in R$ and $1_R = 0_R$, we have $0_R = a \cdot 0_R = a$ for all $a \in R$. ■

8. Does cancellation hold for $\cdot$?
   Sol. No. Consider $a \cdot b = a \cdot c$ and $a \neq 0_R$, then $a \cdot (b - c) = 0_R$. So if R is an *integral domain*, then we can apply cancellation of non-zero element.

Definition 1.4.2 R is said to be an *integral domain* if

$$a \cdot b = 0 \quad \Longleftrightarrow \quad a = 0 \ \text{ or } \ b = 0.$$

Definition 1.4.3 R is said to be a field if every non-zero element in R has a multiplication inverse.

Exercise 1.4.2

1. If R is an integral domain, then we can apply cancellation of non-zero element.
2. Show that every field is an integral domain.

   Proof. If $a \cdot b = 0$ and $a \neq 0_R$, let a' be the multiplication inverse of a, then $b = 1_R \cdot b = a' \cdot a \cdot b = a' \cdot 0_R = 0$. ∎

3. Check that a^{-1} is unique.

   Proof. If a^{-1} and a' are both multiplication inverse of a, then $a \cdot a^{-1} = a \cdot a' = 1_R$. Apply cancellation of non-zero element, we have $a' = a^{-1}$. ∎

Remark 1.4.1 Though every field is an integral domain, not every integral domain is a field. For example, $\mathbb{Z}$ is an integral domain but not a field.

Ways to make new rings:

Let R be an integral domain, how to construct a new ring?
Let $K = \{(a, b), a, b \in R, b \neq 0\}$. We also define an equivalent relation $(a, b) \sim (c, d)$ if $ad = bc$.

- Check this is an equivalent class.
  - $(a, b) = (a, b)$
  - if $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then $(a, b) \sim (e, f)$
- We define
  - $(a, b) + (c, d) = (ad + bc.bd)$
  - $(a, b) \cdot (c, d) = (ac, bd)$

  Check these two operation pass to equivalent class.
- $0_K = [(0, 1_R)]$, $1_K = [(1_R, 1_R)]$

Definition 1.4.4 If R, S are two rings, a homomorphism $\phi : R \to S$ is a map such that

1. $\phi(1_R) = 1_S$.
2. $\phi(a + b) = \phi(a) + \phi(b)$.
3. $\phi(ab) = \phi(a)\phi(b)$.

An isomorphism is a homomorphism that is both injective and surjective.

$\phi : R \to S$, $a \mapsto [(a, 1_R)]$ is an injective homomophism. For example, we have $\mathbb{Z} \subset \mathbb{Q}$.

Remark 1.4.2 If R is a field, then the homomorphism is isomorphism, i.e., ϕ is also surjective. Because for any $[(a, b)] \in K$, we have $\phi(ab^{-1}) = [(ab^{-1}, 1)] = [(a, b)]$.

Ways to kill elements:

Definition 1.4.5 An ideal I in R is a non-empty subset such that

1. I is closed under addition.
2. I is closed under multiplication by arbitrary elt in R.

Note that $(I, +) \subset (R, +)$ is an abelian subgroup.

Example 1

- (0) is an ideal.
- R itself is an ideal.
- if $a \in R$, the $R \cdot a$ is an ideal, denoted by $(a)_R$.
- $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

Quotient Ring: Let $I \subset R$ be an ideal. $R/I =$ coset of I in $R = \{a + I, a \in R\}$, we define

1. $(a + I) \oplus (b + I) = (a + b) + I$.
2. $(a + I) \odot (b + I) = ab + I$.

with zero elt $(0 + I)$ and identity elt $(1 + I)$.

1.5 Class Notes 17-01-12

Definition 1.5.1 A non-zero element in $\mathbb{R}$ is called a unit if $\exists\, v \in \mathbb{R}$ such that $uv = 1_{\mathbb{R}}$.

Definition 1.5.2 Two element $a, b \in \mathbb{R}$ are said to be associative if $\exists\, u \in \mathbb{R}$, u is a unit, such that $a = bu$, denoted by $a \sim b$.

Definition 1.5.3 A non-zero element π in $\mathbb{R}$ is said to be irreducible if π is not a unit and if $a \mid \pi \Rightarrow a$ is a unit or a is associative of π.

Definition 1.5.4 A non-zero element in $\mathbb{R}$ is said to be prime if π is not a unit and $\pi \mid ab \Rightarrow \pi \mid a$ or $\pi \mid b$, $\forall a, b \in \mathbb{R}$.

Proposition 1.5.1 If π is a prime, then π is irreducible.

Proof. Let π be a prime, suppose $a \mid \pi$, then $\pi = ab$ for some $b \in \mathbb{R}$. Thus $\pi \mid ab$ and by definition, $\pi \mid a$ or $\pi \mid b$.

- If $\pi \mid a$, then $a \sim \pi$.
- If $\pi \mid b$, then $a \sim 1$.

■

Remark 1.5.1 A irreducible is not necessary to be a prime.
Let $R = \mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$. We have

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

We write $\pi = (1 + \sqrt{-5})$ and claim that $2, 3, \pi, \overline{\pi}$ are irreducibles but none of them are associative of each other.
We define the norm function $N : R \to \mathbb{Z}$, where $N(\alpha) = \alpha\overline{\alpha}$, i.e., if $\alpha = a + bi$, then $N(\alpha) = a^2 + 5b^2$. We notice that

- If $\alpha > 0$, then $N(\alpha) > 0$.
- $N(\alpha\beta) = N(\alpha)N(\beta)$.

<u>Check: 2 is irreducible:</u>
<u>Find unit:</u>
$N(uv) = N(1) = 1 = N(u)N(v) \Rightarrow N(u) = N(v) = 1$. But $a^2 + 5b^2 = 1 \Rightarrow a = \pm 1, b = 0$.
Suppose $2 = \alpha\beta$, then $4 = N(2) = N(\alpha\beta) = N(\alpha)N(\beta)$.

1. If $N(\alpha) = 1, N(\beta) = 4$
   Then α is a unit $\Rightarrow$ 2 is irreducible.
2. If $N(\alpha) = 2, N(\beta) = 2$
   Then $a^2 + 5b^2 = 2$ has no solution.

Definition 1.5.5 An UFD (Unique Factorization Domain) is an integral domain R in which every non-zero element(up to unit) factors uniquely into a product of irreducibles.

Proposition 1.5.2 Let R be a domain in which factorization (of irreducibles) exists. Then R *is a UFD* $\Leftrightarrow$ *every irreducible in* R *is prime.*

Proof.
" $\Leftarrow$ " : Let a be an element of R and $a \neq 0$. If $a = \pi_1\pi_2\cdots\pi_n = \sigma_1\sigma_2\cdots\sigma_m$ are two factorizations. Since π_1 is prime, $\pi_1 \mid \sigma_i$ for some i. By rearranging, we may assume $\pi_1 \mid \sigma_1$, Thus $\pi_1 \sim \sigma_1$. Repeating this process, we can conclude that the two factorizations are the same.

********Not Complete********

■

Remark 1.5.2 There are clearly rings such that no factorization exists. For example, consider the ring $\mathbb{Z}[2^{1/2}, 2^{1/4}, 2^{1/8}, \dots] \subset \mathbb{R}$. It's the smallest subring of $\mathbb{R}$ that contains $2^{1/2}, 2^{1/4}, \dots$.

Definition 1.5.6 A ring R is said to be noetherian if it satisfies any of the following equivalent conditions:

1. Any ascending chain of ideals in R terminates.
   Namely, $I_1 \subset I_2 \subset I_3 \subset \cdots \Rightarrow I_n = I_{n+1} = \cdots$ for some n.
2. Any ideal I in R is finite generated.
   Namely, $I = (a_1, \dots, a_n)$ for some n.

Proof.
"1. ⇒2. ": Let I be an ideal, if $I \neq 0$, pick $a_1 \in I, a_1 \neq 0$, clearly $(a_1) \subset I$. If $(a_1) = I$, we are done, If not, $\exists a_2 \in I \backslash (a_1) \Rightarrow (a_1, a_2) \subset I$, this chain terminates.
"1. ⇐2. ": Suppose $I_1 \subset I_2 \subset \dots$ be an ascending ideal. Let $I = \cup I_n$, we claim that I is an ideal. Let $a, b \in I$, then there exists n such that $a, b \in I_n$. Therefore $a + b \in I_n$, and $a + b \in I$. Let $a \in I$, then $a \in I_n$ for some n. Therefore $ra \in I_n \implies ra \in I$. Thus I is an ideal. But $I = (a_1, \dots, a_m)$, so there exists n, such that $a_1, \dots, a_m \in I_n$. Thus $I = I_n$ and $I_n = I_{n+1} = \cdots$. ■

Exercise 1.5.1 Suppose R is a Noetherian domain, show R admits factorizations.

Proof. If b is not irreducible, then $b = ac$ or $(b) \subset (a)$

********Not Complete********

■

Definition 1.5.7 A PID (Principle Ideal Domain) is a domain in which every ideal is generated by a single element.

Theorem 1.5.3 Every PID is a UFD.

Proof. Let R be a PID, then it's noetherian. So factorizations exist. So it suffices to show that every irreducible is a prime. Let π be a irreducible in R. Suppose $\pi \mid ab$ and a is not divided by π. We look at $I = (a, \pi)$, there exists $c \in R$, such that $I = (c)$. Thus we have $c \mid \pi, c \mid a$. So $c \sim 1$ or $c \sim \pi$. Since c is not associative of π, c is associative of 1. But then

$$1 = ax + \pi y$$

for some $x, y \in R$. So $b = abx + \pi by$ or $\pi \mid b$. ■

1.6 Class Notes 17-01-17

■ **Example 2** $\mathbb{Z}$ is a PID.

Remark 1.6.1 Any ideal $I \subset \mathbb{Z}$ is of the form of $n\mathbb{Z}$.

Proof. $\forall I \subset \mathbb{Z}$, if $I = (0)$, we are done. If I is not zero ideal, let n be the smallest positive element in I. We claim: $I = n\mathbb{Z}$. Let $b \in I$, then $b = nq + r$, where $0 \leq r < n$. But $r = b - nq \implies r \in I \implies r = 0$. Therefore $b = nq$. ■

If K is a field, let $R = k[x]$ = polynomial in variable x over the field K. What are the units in R? For arbitrary $f(x), g(x) \in K[x]$, if $f(x)g(x) = 1$, we claim that $f(x), g(x)$ must be constant polynomial. For if we write $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots$, $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots$. Then $f(x)g(x) = a_n b_m x^{m+n} + \cdots$. Since $a_n \neq 0, b_m \neq 0$ and K *is an integral domain*, we have $a_n b_m \neq 0$. Therefore

$$\deg f(x)g(x) = \deg f(x) + \deg g(x).$$

We then apply this conclusion to $f(x)g(x) = 1$ and get $\deg f(x) \deg g(x) = \deg 1 = 0$, thus $f(x), g(x)$ must be constant.

Remark 1.6.2 Whether a polynomial is irreducible depends on the field. For example, if $x^2 + 1 \in \mathbb{R}[x]$, then it's irreducible (why?). But if $x^2 + 1 \in \mathbb{C}[x]$, then it's reducible (why?).

Division Algorithm: Let $f(x), g(x) \in K[x], g(x) \neq 0$, then there exists $q(x), r(x) \in K[x]$, such that

$$f(x) = g(x)q(x) + r(x),$$

where $r(x) = 0$ or $0 \leq \deg r(x) < \deg g(x)$.
Using this fact, we have the following theorem.

Theorem 1.6.1 $K[x]$ is a PID.

Proof. For all ideal $I \in K[x]$, if $I = (0)$, we are done. If $I \neq (0)$, let $g(x) \in I$ be the polynomial of least degree, let $f(x) \in I$, then

$$f(x) = g(x)q(x) + r$$

with $r = 0$ or $0 \leq \deg r(x) < \deg g(x)$ by division algorithm. But then $r(x) = 0$, for otherwise $r(x)$ will be a polynomial whose degree is less than $g(x)$. Therefore $f(x) = g(x)q(x)$, $f(x) \in (g(x))$. ■

Definition 1.6.1 A domain R is said to be an Euclidean domain if there exists a function $\lambda : \mathbb{R} \setminus \{0\} \to \mathbb{Z}^{\geq 0}$, such that given $a, b \in R, b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $0 \leq \lambda(r) < \lambda(b)$.

■ **Example 3** $R = \mathbb{Z}[i]$ is an Euclidean domain.

Proof. Let $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$ (if $\alpha = a + bi$). Let $\alpha, \beta \in R$, $\beta \neq 0$, we have

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i = r + si.(r, s \in \mathbb{Q})$$

Let $m + ni \in \mathbb{Z}[i]$ be the closest element to $r + si$. We denote $r' = r - m, s' = s - n$, then $\frac{\alpha}{\beta} = r + si = m + ni + r' + s'i$, or

$$\alpha = \beta(m + ni) + \beta(r' + s'i),$$

where $(m + ni) \in \mathbb{Z}[i]$ and $\beta(r' + s'i) \in \mathbb{Z}[i]$, we remain to show that $N(\beta(r' + s'i)) < N(\beta)$. This is the case because

$$\begin{aligned} N(\beta(r' + s'i)) &= N(\beta)N(r' + s'i) \\ &\leq N(\beta)(\frac{1}{4} + \frac{1}{4}) \\ &< N(\beta) \end{aligned}$$

We are done. ■

The Natural question is what are the units in $\mathbb{Z}[i]$? Does a prime in $\mathbb{Z}$ still a prime in $Z[i]$? To answer the first question, we assume u is a unit in $\mathbb{Z}[i]$. Then by definition there exists some v such that $uv = 1$. But then $1 = N(1) = N(uv) = N(u)N(v) \implies N(u) = 1$. Thus the only possible values of u is $\pm 1, \pm i$. We also check they are actually units. Now, to answer the second question, we try some small cases. We look at $5, 7, 11$ and 13.

■ **Example 4** If $5 = ab$, $a, b \in \mathbb{Z}[i]$, then $25 = N(5) = N(ab) = N(a)N(b) \implies N(a) = 5$. So a can only be $\pm 1 \pm 2i$ or $\pm 2 \pm i$. We try by hand and find $5 = (2+i)(2-i)$ is a factorization, so 5 is not a prime.

■ **Example 5** If $7 = ab$, $a, b \in \mathbb{Z}[i]$, then $49 = N(5) = N(ab) = N(a)N(b) \implies N(a) = 7$. We try by hand and find no factorization, so 7 is a prime.

Use the same method, we find $5, 13$ are not prime while $7, 11$ are prime.

Remark 1.6.3 Obervation:

1. If $p \equiv 1 \pmod 4$, then $p = \pi\overline{\pi}$, where π is a irreducible.
2. If $p \equiv 3 \pmod 4$, then p remains prime.
3. If $p = 2$, $2 = (1+i)(1-i) = (-i)(1+i)^2$ (ramification).

Remark 1.6.4 Let $R = \mathbb{Z}[\omega]$, where ω is a primitive cube root of 1, then R is a Euclidean domain.

Chapter 2

Congruence

2.1 Class Notes 17-01-19

Definition 2.1.1 We write $a \equiv b \pmod{p}$, if $p \mid (a - b)$.

Remark 2.1.1 To solve $ax \equiv b \pmod{m}$ in $\mathbb{Z}$ is the same to solve $[a]x = [b]$ in $\mathbb{Z}/m\mathbb{Z}$.

We now try to solve the equation $a \equiv b \pmod{m}$.

Proposition 2.1.1 A necessary and sufficient condition for this equation to have solutions is $d \mid b$, where $d = (a, m)$ is the gcd of a and m.

<u>Think About:</u> $ax \equiv 1 \pmod{m}$ has solutions is equivalent to $(a, m) = 1$.

Proof.
" $\Rightarrow$": If we have some solution x_0 such that $ax_0 \equiv 1 \pmod{m}$. Then $ax_0 = 1 + mt$ so that $(a, m) = 1$.
" $\Leftarrow$": If $(a, m) = 1$, then there exists x_0, t such that $1 = ax_0 - mt$, so $ax_0 \equiv 1 \pmod{m}$. ■

Remark 2.1.2 In $\mathbb{Z}/m\mathbb{Z}$, $[a]x \equiv [1]$ implies that $[a]$ is a unit.

Definition 2.1.2 $\phi(m) = \#$ of units in $\mathbb{Z}/m\mathbb{Z}$.

We give a few example:

m	1	2	3	4	5
$\phi(m)$	1	1	2	2	4

Now we give the formal proof of our proposition.

Proof. Suppose x_0 is a solution, then there exist t such that

$$ax_0 = b + mt,$$

Since $(a, m) \mid a$, $(a, m) \mid m$, we have $(a, m) \mid b$. Conversely, suppose $(a, m) \mid b$, we may write b as $b = (a, m)b'$. Similarly, $a = (a, m)a'$ and $m = (a, m)m'$ with $(a', m') = 1$. Denote $d := (a, m)$, then $da'x \equiv db' \pmod{dm'}$, $a'x \equiv b' \pmod{m'}$. Since $(a', m') = 1$, $a'x \equiv b' \pmod{m'}$ has solutions. ■

Remark 2.1.3 According to the proof, we will have $d = (a, m)$ solutions.

Now we want to introduce *Chinese Remainder Theorem in* $\mathbb{Z}$. We want to solve a system of congruence equations. Namely, we are looking at the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

where m_i are pairwise coprime.

Theorem 2.1.2 (Chinese Remainder Theorem).
The system always admits solutions.

We notice that if x_0 is a solution to the system, so does $x = km_1m_2\cdots m_n + x_0$, $k \in \mathbb{Z}$. So the system will have infinitely many solutions. The sketch of the proof is as followed.
Suppose we can solve the system

$$\begin{aligned} x_i &\equiv 1 \pmod{m_i} \\ x_i &\equiv 0 \pmod{m_j} \quad \forall j \neq i \end{aligned}$$

then $x = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ is a solution for the original system. But why does the system even have a solution?
Consider the following system as an example,

$$\begin{aligned} x &\equiv 1 \pmod{m_1} \\ x &\equiv 0 \pmod{m_2} \\ &\vdots \\ x &\equiv 0 \pmod{m_n} \end{aligned}$$

We know that since m_i are coprime, $(m_1, m_2m_3\cdots m_n) = 1$.

$$\begin{aligned} &\Rightarrow \exists\, c, d_1, \text{ s.t. } cm_1 + d_1m_2m_3\cdots m_n = 1 \\ &\Rightarrow x = d_1m_2m_3\cdots m_n \text{ is a solution} \end{aligned}$$

Remark 2.1.4 If there are two solutions for the system, say x and y, then

$$x - y \equiv 0 \pmod{m_1m_2\cdots m_n} \implies x \equiv y \pmod{m_1m_2\cdots m_n}.$$

Namely, the solution is unique up to a multiple of $m_1m_2\cdots m_n$.

In order to generalize CRT, we need some background.
Suppose R, S are two rings, then $R \times S := \{(r, s), r \in R, s \in S\}$. We also define sum and product on $R \times S$, namely,

$$\begin{aligned} (a, b) + (c, d) &= (a + c, b + d), \\ (a, b) \cdot (c, d) &= (ac, bd). \end{aligned}$$

We can check that $R \times S$ is actually a ring. The projection maps are ring homomorphisms, i.e., there exist projection maps E_S, E_R,

$$\begin{aligned} E_S &: R \times S \to S \\ E_R &: R \times S \to R \end{aligned}$$

But there doesn't exist any homomorphism from S or R to $R \times S$.
We know that for a ring homomorphism $\phi : R \to S$, $\ker \phi = \{x \in R, \phi(x) = 0\}$ is an ideal. For ring homomorphism $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, it's kernal is exactly the ideal $m\mathbb{Z}$. So in fact, what CRT in $\mathbb{Z}$ says is that the ring homomorphism

$$f : \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z},$$

or

$$a \mapsto ([a]_{m_1}, \dots, [a]_{m_n})$$

is surjective.

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, "f"] & S \\ R/I \arrow[ur, dashed, "\tilde{\phi}"'] & \end{tikzcd}$$

For a ring homomorphism $\phi : R \to S$, $I = \ker \phi$,

- ϕ is injective if and only if $\ker \phi = \{0\}$.
- There exists a unique ring homomorphism $\tilde{\phi} : R/I \to S$, or $\tilde{\phi} : [a] \mapsto \phi(a)$ such that the diagram commutes. $\tilde{\phi}$ is also well defined, for if $[a] = [b]$, then we have

$$\begin{aligned} [a] = [b] &\Rightarrow (a - b) \in I \\ &\Rightarrow \phi(a - b) = 0 \\ &\Rightarrow \phi(a) = \phi(b). \end{aligned}$$

Now, let $R = \mathbb{Z}$, $S = \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$. Let $m = m_1 m_2 \cdots m_n$, then $\ker \phi = \mathbb{Z}/m\mathbb{Z}$, we have the following diagram.

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\phi"] \arrow[d, "f"] & \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z} \\ \mathbb{Z}/m\mathbb{Z} \arrow[ur, "\tilde{\phi}"'] & \end{tikzcd}$$

Notice that $\tilde{\phi}$ is an isomorphism.
We have the natural question that what are the units in R and S? Let $U(R)$ denote the set of units of the ring R, then $U(R \times S) = U(R) \times U(S)$. We thus have a branch of corollaries.

Corollary 2.1.3 $U(\mathbb{Z}/m\mathbb{Z}) \cong U(\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times U(\mathbb{Z}/m_n\mathbb{Z})$.

Corollary 2.1.4 $\phi(m) = \phi(m_1)\phi(m_2)\cdots\phi(m_n)$.

Corollary 2.1.5 If $m = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}$, then

$$\begin{aligned} \phi(m) &= \phi(p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}) \\ &= \phi(p_1^{\gamma_1})\phi(p_2^{\gamma_2})\cdots\phi(p_s^{\gamma_s}), \end{aligned}$$

with $\phi(p_i^{\gamma_i}) = p_i^{\gamma_i} - p_i^{\gamma_i - 1}$.

Corollary 2.1.6

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

The proof is simply use the fact that the statement is true for primes, and every element of $\mathbb{Z}$can be factorized as a product of primes.

Proof. We claim that if the statement is true for $m, n\,((m, n) = 1)$, then it's true for mn.

$$\begin{aligned}\sum_{d|mn} \phi(d) &= \sum_{d_1|m, d_2|n} \phi(d_1 d_2) \\ &= \sum_{d_1|m} \sum_{d_2|n} \phi(d_1)\phi(d_2) \\ &= (\sum_{d_1|m} \phi(d_1))(\sum_{d_2|n} \phi(d_2)) \\ &= m \cdot n.\end{aligned}$$

■

2.2 Class Notes 17-01-24

Suppose $I, J \subset R$ are two ideals, how to make new ideals with I, J? Evidently, $I \cap J$ and $I + J$ are ideals. Also,

$$I \cdot J := \{\sum a_i b_i, a_i \in I, b_i \in J\} \subset I \cap J$$

is an ideal.

■ **Example 6** Let $I = m\mathbb{Z}$,$J = n\mathbb{Z}$. then we have

$I + J$	$I \cap J$	$I \cdot J$
$((m, n))$	$([m, n])$	$mn\mathbb{Z}$

.

Definition 2.2.1 We say two ideals I, J are coprime if $I + J = (1)$.

Remark 2.2.1 If I, J are coprime, then $I \cap J = I \cdot J$.

Proof. For some $x \in I \cap J$, since I, J are coprime, there exists some $a \in I, b \in J$ such that $a + b = 1$. But then $a \cdot x + x \cdot b = x \in I \cdot J$. So $I \cap J \subset I \cdot J$. The other direction is obvious. ■

Theorem 2.2.1 (Generalized Chinese Remainder Theorem). Let $I_1, I_2, \ldots, I_n$ be pairwise coprime ideals in R, then the map

$$\phi : R \to R/I_1 \times \ldots \times R/I_n$$

1) is surjective
2) has $\ker \phi = I_1 I_2 \ldots I_n = I_1 \cap I_2 \cap \ldots \cap I_n$

Lemma 9 We first look at $n = 2$ case. If I, J are coprime ideals in R, then the map

$$\phi : R \to R/I \times R/J$$

1) is surjective.
2) has $\ker \phi = I \cap J = IJ$.

Proof. It's enough to solve the system of congrence

$$x \equiv 1 \pmod I$$
$$x \equiv 0 \pmod J$$

and

$$
\begin{aligned}
y &\equiv 0 \pmod{I} \\
y &\equiv 1 \pmod{J}
\end{aligned}
$$

Since I, J are coprime, there exists $c \in I, d \in J$ such that $c + d = 1$. c, d is the solution to our two systems. ■

Lemma 10 I_1 is coprime to $I_2 I_3 \cdots I_n$.

Proof. There exist

$$
\begin{aligned}
a_2 + b_2 &= 1 \\
a_3 + b_3 &= 1 \\
&\dots \\
a_n + b_n &= 1,
\end{aligned}
$$

$a_i \in I_1$, $b_j \in I_j$.
Then

$$
\begin{aligned}
b_2 b_3 \dots b_n &= (1 - a_2) \dots (1 - a_n) \\
&= 1 + a,
\end{aligned}
$$

where $a \in I_1$.
By $n = 2$ case

$$
\begin{tikzcd}
R \arrow[r] \arrow[d] & R/I_1 \times R/(I_2 \times I_3 \times \cdots \times I_n) \\
R/I_1 \times R/I_2 \times \cdots \times R/I_n \arrow[ur]
\end{tikzcd}
$$

■

Let us denote $U(R)$ by $R^\times$. Note that $\phi(n) = \|(\mathbb{Z}/n\mathbb{Z})^\times\|$. We now want to look at the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$. We first develop some background in abstract algebra.

Theorem 2.2.2 (Lagrange Theorem). Let G be a finite group, $H \subset G$ is a subgroup, then the order of H divides the order of G, i.e.,

$$|H| \mid |G|$$

Proof. Take two cosets in H, Ha and Hb. They are equal or disjoint. So

$$|G| = |H| \cdot \# \text{ of cosets}$$

■

Definition 2.2.2 If $a \in G$, then $o(a) =$ smallest positive integer d such that

$$a^d = 1$$

is called the order of the element a.

Corollary 2.2.3 $\forall a \in G$, we have $o(a) \mid |G|$.

Proof. $\langle a \rangle := \{1, a, \dots, a^{d-1}\}$ is the subgroup generated by a. Then $\langle a \rangle \subset G \Rightarrow d \mid |G|$. ■

Corollary 2.2.4 $a^{|G|} = 1$.

Corollary 2.2.5 If $n \geq 1$, $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. $(a, n) = 1 \Rightarrow a \to [a]$ is a unit in $\mathbb{Z}/n\mathbb{Z}$, i.e., $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times, |(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$. $\Rightarrow [a]^{\phi(n)} = 1$ in $(\mathbb{Z}/n\mathbb{Z})^\times$, i.e., $a^{\phi(n)} \equiv 1 \pmod{n}$. ∎

Exercise 2.2.1 Find the last 3 digits of 3^{1203}.

Proof. $\phi(1000) = \phi(2^3 5^3) = (8-4)(125-25) = 400$. So $3^{400} \equiv 1 \pmod{1000}$. The last three digits are then 027. ∎

We now look at the structure of $(\mathbb{Z}/p\mathbb{Z})^\times$, where p is a prime.

Theorem 2.2.6 $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

We do some checking, let $p = 5, 7, 11, 13$. For $p = 11$, we find that $2, 3, 7, 9$ are $\mathbb{Z}/11\mathbb{Z}$'s generator.

Lemma 11 Let $a \in G$ be an element of order d, then the order of a^m is $\frac{d}{(d,m)}$.

Proof. Let $(d, m) = b$, we then have $d = bd', m = bm'$, where $(d', m') = 1$. We claim that $o(a^m) = d'$. For $(a^m)^{d'} \cong a^{bm'd'} \cong a^{dm'} \cong (a^d)^{m'} \cong 1$. Suppose $(a^m)^l = 1 \Rightarrow a^{ml} = 1 \Rightarrow d \mid ml \Rightarrow bd' \mid bm'l \Rightarrow d' \mid m'l \Rightarrow d' \mid l$. ∎

Corollary 2.2.7 If G is cyclic of order d, then the number of generators of G is $\phi(d)$.

Chapter 3

The Structure of $U(\mathbb{Z}/n\mathbb{Z})$

3.1 Class Notes 17-01-26

Theorem 3.1.1 $(\mathbb{Z}/p\mathbb{Z})$ is a field.

Proof. If $[a] \neq 0 \Rightarrow (p, a) = 1 \Rightarrow \exists x, y \ s.t. \ px + ay = 1 \Rightarrow [a][y] = [1]$. ■

Theorem 3.1.2 Let K be a field, let G be a finite subgroup of K, then G is cyclic.

Lemma 12 Let $f(x) \in K[x]$ be any non-zero polynomial. Then the number of roots of f in K is elss or equal to $\deg f$

Proof. If $f(x)$ has no root, we are done. If $f(x)$ has some roots, say α is a root, then

$$f(x) = (x - \alpha)g(x) + r(x), \quad r(x) = 00$$

So $f(x) = (x - \alpha)g(x)$. By induction the lemma holds. ■

We can then prove the theorem.

Proof. Let K be a field. Let $G \subset K^{\times}$ be a finite subgroup of order n. $G \subset \{\text{roots of} x^n - 1\} \Rightarrow G = \{\text{roots of} x^n - 1\}$. Any element in G has order dividing by n for every divisor d of n. Let $\Sigma_d = \{a \in G, o(a) = d\}$, then

$$G = \sqcup_{d|n} \Sigma_d, \quad n = |G| = \sum_{d|n} |\Sigma_d|.$$

We claim: $|\Sigma_d| = 0$ or $\phi(d)$.
If $\Sigma_d = \emptyset \Rightarrow |\Sigma_d| = 0$. Suppose $\Sigma_d \neq \emptyset \Rightarrow \exists a \in G, \text{s.t.} o(a) = d$. Let $H = \langle a \rangle = \{1, a, \dots, a^{d-1}\} \subset G$. i.e.,

$$\begin{aligned} \Sigma_d &= \text{set of elements with order } d \\ &= \text{all elements of } H \end{aligned}$$

. $\Rightarrow |\Sigma_d| = \phi(d)$. Then

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

$\Rightarrow |\Sigma_d| = \phi(d), \forall d \mid n$. In particular $|\Sigma_n| = \phi(n) \Rightarrow G$ is cyclic. ■

We then want to discuss the structure of $(\mathbb{Z}/p^{\gamma}\mathbb{Z})^{\times}$

Theorem 3.1.3 If p is an odd prime, then $(\mathbb{Z}/p^\gamma\mathbb{Z})^\times$ is cyclic.

Proof. Since $\mathbb{Z}/p^\gamma\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is surjective, $(\mathbb{Z}/p^\gamma\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ is surjective. Let us denote $G := (\mathbb{Z}/p^\gamma\mathbb{Z})^\times$, $H := (\mathbb{Z}/p\mathbb{Z})^\times$, and let K be the kernal of $G \to H$, i.e.,

$$K = \{[x] \in G, x \equiv 1 \pmod p\}.$$

Note we have $|G| = p^{\gamma-1}(p-1), |H| = p-1$. So we have $|K| = \dfrac{|G|}{|H|} = p^{\gamma-1}$. We will show K is cyclic by explicitly constructing a system. We consider the cyclic group generated by $1 + ap$, where $a \equiv 0 \pmod p$. We know that

$$(1+ap)^{p^{\gamma-1}} \equiv 1 \pmod{p^\gamma},$$

want however

$$(1+ap)^{p^{\gamma-2}} \not\equiv 1 \pmod{p^\gamma}.$$

Lemma 13 Let p be any prime, $a, b \in \mathbb{Z}, \gamma \geq 1$. If $a \equiv b \pmod{p^\gamma}$, then $a^p \equiv b^p \pmod{p^{\gamma+1}}$.

Proof. First notice that for $1 \leq i \leq p-1$, $\binom{p}{i}$ is divided by p, then

$$\begin{aligned} a = b + p^\gamma t \;&\Rightarrow\; a^p = (b+p^\gamma t)^p \\ &\Rightarrow\; a^p = b^p + \sum_{i=1}^{p-1} \binom{p}{i} b^i (p^\gamma t)^{p-1} + (p^\gamma t)^p. \\ &\Rightarrow\; a^p \equiv b^p \pmod{p^{\gamma+1}} \end{aligned}$$

■

We then prove the following lemma,

Lemma 14 $(1+ap)^{p^{\gamma-2}} \equiv 1 + ap^{\gamma-1} \pmod{p^\gamma}$

Proof. We induction on γ.
When $\gamma = 1$, the statement is trivially true. Assume the statement is true for γ, check for $\gamma+1$. We know

$$(1+ap)^{p^{\gamma-2}} \equiv 1 + ap^{\gamma-1} \pmod{p^\gamma},$$

and we want to show

$$(1+ap)^{p^{\gamma-1}} \equiv 1 + ap^\gamma \pmod{p^{\gamma+1}}$$

By lemma 13,

$$\begin{aligned} (1+ap)^{p^{\gamma-1}} &\equiv (1+ap^{\gamma-1})^p \pmod{p^{\gamma+1}} \\ &= 1 + p \cdot ap^{\gamma-1} + \sum_{i=2}^{p-1} \binom{p}{i} (ap^{\gamma-1})^i + a^p p^{p(\gamma-1)} \\ &\equiv 1 + ap^\gamma \pmod{p^{\gamma+1}} \end{aligned}$$

So the statement holds for $\gamma + 1$. ■

■

Chapter 4

Quadratic Reciprocity

4.1 Class Notes 17-01-31

Last class we have prove that if $n = p$ os a prime, then $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, and if n is odd, $n = p^r$, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

********Not Complete********

Let p is an odd prime, $(a, p) = 1$, is a a square modulo p? We try $a = -1$ for $p = 5, 13, \ldots$. We have the following proposition.

Proposition 4.1.1 -1 is a square modulo $p \iff p \equiv 1 \pmod 4$.

Definition 4.1.1 We introduce the legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square modulo } p \\ -1 & \text{otherwise} \end{cases}$$

We have the following proposition.

Proposition 4.1.2

1. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b \pmod p$
2. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

The proof of Proposition 4.1.2.3 is as followed.

Proof. Let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$, then $\langle g \rangle = \{1, g, g^2, \ldots, g^{p-1}\}$. $1, g^2, g^4, \ldots, g^{p-1}$ are already square. But $g, g^3, g^5, \ldots, g^{p-2}$ are not square (why?). If $g = h^2$ is a square, it will not generate the group! ∎

The proof of Proposition 4.1.2.2 is as followed.

Proof. if $a = b^2$, then $a^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \pmod p$. If $a \neq b^2$, say $a = g$, then $g^{\frac{p-1}{2}} \not\equiv 1 \pmod p$ since g is a primitive root. So $g^{\frac{p-1}{2}} \equiv -1 \pmod p$, i.e., $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. ∎

Theorem 4.1.3

- Suppose p, q are odd prime, then

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

or

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

Namely, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if either $p, q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ otherwise.

- $$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8 \\ -1 & \text{if } p \equiv 3, 5 \pmod 8 \end{cases} = (-1)^{\frac{p^2-1}{8}}.$$

Exercise 4.1.1 Is 101 a square modulo 107?

Proof. Yes, because we have

$$\begin{aligned}\left(\frac{101}{107}\right) = \left(\frac{107}{101}\right) = \left(\frac{6}{101}\right) &= \left(\frac{2}{101}\right)\left(\frac{3}{101}\right) \\ &= (-1)\left(\frac{101}{3}\right) \\ &= (-1)\left(\frac{2}{3}\right) = (-1)(-1) = 1\end{aligned}$$

■

Exercise 4.1.2 Is 79 a square of 97?

Proof. Yes, because we have

$$\begin{aligned}\left(\frac{79}{97}\right) = \left(\frac{97}{79}\right) &= \left(\frac{18}{79}\right) \\ &= \left(\frac{2}{79}\right) = 1\end{aligned}$$

■

4.2 Class Notes 17-02-02

Lemma 15 **(Gauss's Lemma).** If $(a, p) = 1$. Consider the residue system

$$\left\{-\frac{p-1}{2}, \ldots, -1, +1, +2, \ldots, +\frac{p-1}{2}\right\}.$$

Let $\mu = \#$ of negative classes that $a \cdot 1, a \cdot 2, \ldots, a \cdot \frac{p-1}{2}$ fall into. Then

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

Let $a \cdot i \equiv \pm m_i \pmod p$, we claim that if $i \neq j$, then $m_i \neq m_j$.

Proof. if $m_i = m_j$, then $a_i \equiv \pm a_j \pmod p$, so $i \equiv \pm j \pmod p$. We know that

$$\left\{m_1, m_2, \ldots, m_{\frac{p-1}{2}}\right\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$$

Let $\mu = \#$ of negative signs. Then $a^{\frac{p-1}{2}} \prod i \equiv (-1)^{\mu} \prod m_i \pmod p$ ■

Lemma 16 (Eisenstein's Lemma).
Let $\Sigma = \{2, 4, \ldots, p-1\}$, for $j \in \Sigma$, consider $[\frac{aj}{p}]$, then

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{j\in\Sigma}[\frac{aj}{p}]}.$$

Chapter 5

Finite Fields

5.1 Class Notes 17-02-07

Definition 5.1.1 A finite field is a field with finite many elements

Example 7 $\mathbb{Z}/p\mathbb{Z}$ is a finite field

We know that there is always a homomorphism from $\mathbb{Z}$to a ring. Let K be a finite field, the homomorphism $f : \mathbb{Z} \to K$ can't be injective, so the kernal of f is not zero, i.e., the kernal is $n\mathbb{Z}$ for some n. Let ring P be the image of f, then there is an isomorphism $\phi : \mathbb{Z}/n\mathbb{Z} \to P$. So we may identify $\mathbb{Z}/n\mathbb{Z}$ and P. On the other hand, P is a subring of a field, therefore P is also an integral domain. But an integral domain with finite elements is a field. So equivalently, $\mathbb{Z}/n\mathbb{Z}$ has to be a field, which implies that n is a prime. So we conclude:

Theorem 5.1.1 Every finite field K has a subfield isomorphic to $\mathbb{Z}/p\mathbb{Z}$. We say K has charateristic p and denote $F_p = \mathbb{Z}/p\mathbb{Z}$.

If $F \subset E$ are fields, we may view E as a vector space over F, or a $F-$vector space. We will write $\dim E := [E : F]$ and say E is a finite extension of F.

Example 8 $[\mathbb{C} : \mathbb{R}] = 2$

Notice that if K is a finite field, then $[K : F_p]$ is finite, say n. Let $x_1, x_2, \ldots, x_n$ be the basis of the F_p-field, then explicitly,

$$K = \{c_1x_1 + c_2x_2 + \ldots + c_nx_n\}, \quad \forall c_i \in F_p,$$

which implies that $|K| = p^n$.
Let K be a field with p^n elements, then the multiplicative subgroup (equivalently, the group of units), $K^\times$ is finite, and therefore cyclic. We have

$$\alpha^{p^n-1} = 1, \quad \forall \alpha \in K^\times$$

or

$$\alpha^{p^n} = \alpha, \quad \forall \alpha \in K.$$

Since a polynomial f of degree $\deg f$ has at most $\deg f$ roots in a field, $x^{p^n} = x$ has at most p^n roots in K. So the p^n roots of the polynomail $x^{p^n} = x$ form exactly the field K.
We now want to explicitly construct a field of order p^n (or equivalently, a field in which $x^{p^n} - x$ factors completely).

Exercise 5.1.1 Let L, E, F be fields. E is a field extension of F, L is a field extension of E. Prove that

$$[E : F][L : E] = [L : F]$$

Proof. Just write down the basis. ∎

5.2 Class Notes 17-02-09

Proposition 5.2.1 Let K be a field of order p^n, then K admits a unique sobfield of size $p^d, \forall d \mid n$.

Proof. Let K', K'' be two such subfields, Then

$$K' = \{\text{roots of } x^{p^n - 1} - x \text{ in } K\} = K''.$$

For existence, let $K' = \{\text{roots of } x^{p^d} - x\}$, we just need to show K' is a field. Clearly, $1, 0 \in K'$. Using $(x + y)^p = (x^p + y^p)$ in charateristic p field K', we can also show K' is closed in addition, multiplication and division. Thus K' is a field. Note that $d \mid n$ is necessary since we must have $x^{p^d} - x \mid x^{p^n} - x$, and that implies $d \mid n$. ■

The general problem is that let $f(x) \in K[x]$ be a non-constant polynomial, can we construct an extension of K such that $f(x)$ can be linearly factored? Let $L := K[x]/(f(x))$, $f(x)$ is irreducible in K. We have

Theorem 5.2.2
- L is a field.
- In L, f has a root, namely the class of x such that $f(x) = 0$.

Example 9 $\mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$

Exercise 5.2.1 Prove that $\mathbb{R}[x]/(x^2 + 1)$ is isomorphic to $\mathbb{R}[x]/(x^2 + 5)$.

Proof. We apply the bijection $x \mapsto x/\sqrt{5}$. ■

Theorem 5.2.3 $[L : K] = \deg f$

Corollary 5.2.4 $L = K[\alpha] = K(\alpha)$. $K[\alpha]$ is the ring generated by K and α. $K(\alpha)$ is the field generated by K and α.

5.3 Class Notes 17-02-14

Construction of a field of size p^n: We can find a field K such that $x^{p^n} - x$ splits completely. First notice that $x^{p^n} - x$ has no multiple roots. This is because if we define $f(x) := x^{p^n} - x$, we have $(f(x), f'(x)) = (x^{p^n} - x, p^n x^{p^n - 1} - 1) = 1$.

Theorem 5.3.1 Any two field with p^n elements are isomorphic.

Proof. Suppose $\|L\| = p^n$, I claim: $\exists \alpha \in L$, such that $\mathbb{F}_p(\alpha) = \mathbb{F}_p[\alpha]$. Let K be a field with p^n element, $K = \mathbb{F}_p(\alpha), K^\times = \langle \alpha \rangle$, Let ϕ be the homomorphism from $\mathbb{F}_p[x] \to \mathbb{F}_p[\alpha]$, $\ker \phi = (f(x)), f(x) \in \mathbb{F}_p[x]$, $\Rightarrow \frac{\mathbb{F}_p[x]}{(f(x))} \sim \mathbb{F}_p[\alpha] = \mathbb{F}_p(\alpha) = K, \Rightarrow f(x)$ is an irreducible (K is a field).

$$[K : \mathbb{F}_p] = \deg f.$$

α satisfies $x^{p^n} - x = 0$. Because of the isomorphism, α satisfies $f(x)$. $\Rightarrow \alpha$ satisfies the gcd. But $\gcd(x^{p^n} - x, f(x)) = f(x) \Rightarrow f(x) \mid (x^{p^n} - x)$ ■

So far, we proved, $\exists \alpha$, such that $K = \mathbb{F}_p(\alpha)$.
1. any such α is a root of an irreducible polynomial in $\mathbb{F}_p[x]$ that divides $x^{p^n} - x$.
2. $K \sim \frac{\mathbb{F}_p[x]}{f(x)}$ for some irreducible $f(x)$, $f(x) \mid (x^{p^n} - x)$.

3. Let $g(x)$ be any irreducible factor of $x^{p^n} - x$ of degree n, $K' = \frac{\mathbb{F}_p}{(g(x))}$, we know $[K' : \mathbb{F}_p] = n$, $\Rightarrow x^{p^n} - x$ splits completely in K', $\Rightarrow f$ has a root $\beta \in K'$.

Exercise 5.3.1 How many monic irreducible polynomial of deg 9 over $\mathbb{F}_7$?

Proof. Consider the finite extension of the field $\mathbb{F}_7$. Over the field $\mathbb{F}_{7^9}$, $x^{7^9} - x$ splits completely. So

$$x^{7^9} - x = (x^{7^3} - x) * \prod_{\deg g = 9, \text{irr over } \mathbb{F}_7} g,$$

So ans$= \frac{7^9 - 7^3}{9}$. ∎

We now want to prove the quadratic reciprocity using finite field.

Proof.

********Not Complete********

∎

5.4 Class Notes 17-02-16

Definition 5.4.1 Let E/K be extension of fields. An element $\alpha \in E$ is said to be algebraic over K if it's the root of some non-zero polynomial with coefficient in K.

Example 10
1. $\sqrt{2}i$ is algebraic over $\mathbb{Q}$.
2. π is not algebraic over $\mathbb{Q}$

$k(\alpha)$ is the smallest subfield of K containing K and α. $k[\alpha]$ is the smallest subring of E containing K and α. We have

$$k(\alpha) = \{\frac{p(\alpha)}{q(\alpha)} \text{ with } p(x), q(x) \in K[x], q(x) \neq 0\}$$

$$k[\alpha] = \{p(\alpha), p(x) \in K[x]\}$$

Theorem 5.4.1 Suppose α is algebraic over K, then $K(\alpha) = K[\alpha]$

Proof. Let $I = \{p(x) \in K[x], p(\alpha) = 0\} \subset k[x]$, I is an ideal in $K[\alpha]$. Since $K[x]$ is a PID, $I = (f(x))$. Consider the homomorphism ϕ from $K[x]$ to $K[\alpha]$ is surjective, so $\frac{K[x]}{(f(x))}$ is isomorphic to $K[\alpha]$. But $K[\alpha] \subset K(\alpha)$ is a subring of a field, and therefore an integral domain, so $f(x)$ is irreducible. By the claim that $\frac{K[x]}{(f(x))}$ is a field, we have $K(\alpha) = K[\alpha]$. ∎

Exercise 5.4.1 $\alpha = 2^{1/3} \in \mathbb{C}$, write $\frac{1+\alpha}{1+\alpha^2}$ as a polynomial in $\alpha$with $\mathbb{Q}$coefficient.

Proof. Just find the inverse of $1 + \alpha^2$. *Hint,* use Euclidean to find the gcd of $x^3 - 2$ and $x^2 + 1$. ∎

Theorem 5.4.2 All algebraic numbers over a field K is a field.

Proof.
1. Evidently, if α is algebraic over K, so is K^{-1}.

2. To prove closure under multiplication and addition. Suppose we have two algebraic number α and β and $[k(\alpha) : k] = m, [k(\beta) : k] = n$. Let $r_{ij} = \alpha^i \beta^j$, where $0 \leq i \leq m-1, 0 \leq j \leq n-1$. Let $\gamma = \alpha + \beta, N = mn$. We can then write down the following equitions.

$$\begin{aligned}
\gamma \cdot r_1 &= c_{11} r_1 + \cdots + c_{1N} r_N \\
\gamma \cdot r_1 &= c_{21} r_1 + \cdots + c_{2N} r_N \\
&\vdots\vdots\vdots \\
\gamma \cdot r_N &= c_{N1} r_1 + \cdots + c_{NN} r_N
\end{aligned}$$

Let A be the matrix of c_{ij}, then

$$\gamma r = A r$$

or

$$\det(A - \gamma I) = 0$$

Therefore closed under multiplication and addition.

■

Chapter 6

Gauss and Jocobi Sums

6.1 Class Notes 17-03-07

Definition 6.1.1 A multiplicative character on $\mathbb{F}_p$ is a map χ from $\mathbb{F}_p^\times$ to the nonzero complex numbers that satisfies

$$\begin{aligned}\chi : \mathbb{F}_p^\times &\to \mathbb{C}^\times \\ \chi(ab) =& \chi(a)\chi(b) \quad \text{for all } a, b \in \mathbb{F}_p^\times\end{aligned}$$

■ **Example 11** Let $p = 5$, Find all multiplicative characters modulo p.

	1	2	$4(2^2)$	$3(2^3)$
ε	1	1	1	1
χ_1	1	-1	1	-1
χ_2	1	i	-1	$-i$
χ_3	1	$-i$	-1	i

Table 6.1: The characters of the group $\mathbb{F}_5$

Proof. ■

Proposition 6.1.1 Let χ be a multiplicative character and $a \in \mathbb{F}_p^\times$. Then

1. $\chi(1) = 1$.
2. $\chi(a)$ is a $(p-1)_{st}$ root of unity.
3. $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Proof.

1. We have $\chi(1) = \chi(1^2) = (\chi(1))^2$, so $\chi(1) = 0$ or $\chi(1) = 1$. But $\chi(1)$ can't be zero, thus $\chi(1) = 1$.
2. $(\chi(a))^{p-1} = \chi(a^{p-1}) = \chi(1) = 1$.
3. $1 = \chi(aa^{-1}) = \chi(a)\chi(a^{-1})$, so $\chi(a^{-1}) = \chi(a)^{-1}$. Also, since $1 = \|\chi(a)\| = \chi(a)\overline{\chi(a)}$, $\overline{\chi(a)} = (\chi(a))^{-1}$.

■

Proposition 6.1.2 Let χ be a multiplicative character.

1. If $\chi \neq \varepsilon$, then $\sum_t \chi(t) = 0$, where the sum is over all $t \in \mathbb{F}_p$.
2. If $\chi = \varepsilon$, then $\sum_t \varepsilon(t) = p$, the sum is over all $t \in \mathbb{F}_p$.

Proof.

1. if $\chi \neq \varepsilon$, there exist some $a \in \mathbb{F}_p^\times$ such that $\chi(a) \neq 1$. Then $\sum_t \chi(t) = \sum_t \chi(at) = \sum_t \chi(a)\chi(t) = \chi(a)\sum_t \chi(t)$. Thus $\sum_t \chi(t) = 0$.
2. if $\chi = \varepsilon$, trivially, $\sum_t \chi(t) = p$.

■

Proposition 6.1.3
1. Let $G = \mathbb{F}_p$, then the multiplicative characters of G form a cyclic group of order $p-1$.
2. If $a \in \mathbb{F}_p^\times$ and $a \neq 1$, then there is a character χ such that $\chi(a) \neq 1$.

Definition 6.1.2 The group of the multiplicative characters of a group G is denoted by $\hat{G}$.

Proof.
1. It's easy to verify that if χ, λ are characters, then $\chi\lambda$ is also a character. Also, the inverse χ^{-1} defined by $\chi^{-1} : a \mapsto \chi(a)^{-1}$ is a character. So all characters form a group. Let g be a primitive root modulo p, then $\xi := \chi(g)$ is a primitive $p-1_{st}$ root of unity (why? For if exists some a least $u < p-1, u \neq 0$ such that $\xi^u = 1$, then $\chi(g^u) = 1$. But then exists $v \equiv p-1 \pmod{u}$ such that $\xi^v = 1$, which contradicts our assumption). If there is some n such that $\chi^n = \varepsilon$, then $(\chi(g))^n = \varepsilon(g) = 1$. Then $\xi^n = 1 \Rightarrow (p-1) \mid n$. But the order of ξ is at most $p-1$, so the order of ξ is $p-1$.
2.

********Not Complete********

■

Corollary 6.1.4 If $a \in \mathbb{F}_p^\times, a \neq 1$, then $\sum_{\chi\in\hat{G}} \chi(a)$=0.

Proof. If $a \neq 1$, then

$$\begin{aligned}\sum_{\chi\in\hat{G}} \chi(a) &= \sum_{\chi\in\hat{G}} (\mu\chi)(a)\\ &= \mu(a)\sum_{\chi\in\hat{G}} \chi(a).\end{aligned}$$

So $\sum_{\chi\in\hat{G}} \chi(a) = 0$. ■

6.2 Class Notes 17-03-09

We now have the question that whether $x^n = a$ has a root in $\mathbb{F}_p$?

Proposition 6.2.1 Let $d = \gcd(n, p-1)$, then $x^n = a$ has a root in $\mathbb{F}_p \Leftrightarrow x^d = a$ has a solution in $\mathbb{F}_p$ and in this case the number of roots is d.

Proof. We have proved this result. (Using the fact that $\mathbb{F}_p^\times$ is a cyclic group) ■

Another question is that let $n \mid (p-1)$, does $x^n = a$ has solutions in $\mathbb{F}_p$.

Theorem 6.2.2 Let $n \mid p-1, a \in \mathbb{F}_p^\times$, then

$$N(x^n = a \text{ in } \mathbb{F}_p^\times) = \sum_{\chi\in\hat{G}, \chi^n=\varepsilon} \chi(a)$$

.

■ **Example 12**
1. $n = 2$, p is an odd prime. Then

$$N(x^2 = a \text{ in } \mathbb{F}_p^\times) = \sum_{\chi\in\hat{G}, \chi^2=\varepsilon} \chi(a) = \varepsilon(a) + \left(\frac{a}{p}\right)$$

2. $n = 3$, p is an odd prime. Then

$$N(x^3 = a \text{ in } \mathbb{F}_p^\times) = \sum_{\chi \in \hat{G}, \chi^3 = \varepsilon} \chi(a) = \varepsilon(a) + \chi(a) + \chi^2(a)$$

where χ is a character of order 3.

We can extend the character $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ to $\chi : \mathbb{F}_p \to \mathbb{C}$ by setting $\varepsilon(0) = 1$ and for $\chi \neq \varepsilon$, $\chi(0) = 0$. So Table 6.1 becomes

	0	1	2	$4(2^2)$	$3(2^3)$
ε	1	1	1	1	1
χ_1	0	1	-1	1	-1
χ_2	0	1	i	-1	$-i$
χ_3	0	1	$-i$	-1	i

Table 6.2: The characters of the group $\mathbb{F}_5$

Proof. For $a = 0$, the only solution for $x^n = 0$ is $x = 0$. Trivially, RHS is 1. We can assume $a \neq 0$. There are two cases.

case 1: If a is not a n_{th} power, then LHS is 0. We have

$$\text{RHS} = \sum_{\mu^n = \varepsilon} \varepsilon(a).$$

We claim:
If a is not n_{th} power, then there exists $\chi \in \hat{G}$, $\chi^n \in \varepsilon$, such that $\chi(a) \neq 1$.

Proof. a is not a n_{th} power is equivalent to say $a^{\frac{p-1}{n}} = 1$ has no solution or $a^{\frac{p-1}{n}} \neq 1$. But then there exists a character λ such that $\lambda(a^{\frac{p-1}{n}}) \neq 1$ or $\lambda^{\frac{p-1}{n}}(a) \neq 1$. Clearly, $\chi := \lambda^{\frac{p-1}{n}}$ is a character such that $\chi(a) \neq 1$. ∎

Using this lemma, we have

$$\begin{aligned}
\text{RHS} &= \sum_{\mu^n = \varepsilon} \mu(a) \\
&= \sum_{\mu^n = \varepsilon} (\chi\mu)(a) \\
&= \chi(a) \sum_{\mu^n = \varepsilon} \mu(a) \\
&\Rightarrow \sum_{\mu^n = \varepsilon} \mu(a) = 0
\end{aligned}$$

case 2: If a is a n_{th} power, then LHS is n.

$$\begin{aligned}
\text{RHS} &= \sum_{\chi^n = \varepsilon} \chi(a) \\
&= \sum_{\chi^n = \varepsilon} \chi(b^n) \\
&= \sum_{\chi^n = \varepsilon} \chi^n(b) = n
\end{aligned}$$

∎

Example 13 Let $p = 7, n = 3, a = 2$, verify the theorem.

Proof. The first step is to write down the table of characters So $N(x^3 = 2) = \varepsilon(2) + \chi^2(2) + \chi^4(2) = 1 + \xi^2 + \xi^4 = 0$ ∎

	0	1	3	2	6	4	5
ε	1	1	1	1	1	1	1
χ	0	1	ξ	ξ^2	ξ^3	ξ^4	ξ^5
χ^2	0	1	ξ^2	ξ^4	1	ξ^2	ξ^4
χ^3	0	1	ξ^3	1	ξ^3	1	ξ^3
χ^4	0	1	ξ^4	ξ^2	1	ξ^4	ξ^2
χ^5	0	1	ξ^5	ξ^4	ξ^3	ξ^2	ξ

Table 6.3: The characters of the group $\mathbb{F}_7$

Definition 6.2.1 Let χ be a multiplicative character modulo p. Let ξ be a fixed primitive p_{th} root of unity. Let $a \in \mathbb{F}_p$, we define

$$g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t)\xi^{at}$$

g_a is called a Gauss sum on $\mathbb{F}_p$ belonging to the character χ.

We have the following proposition

Proposition 6.2.3

- if $a = 0, \chi = \varepsilon$, then $g_a(\chi) = \sum_{t \in \mathbb{F}_p} \varepsilon(t) = p$.
- if $a = 0, \chi \neq \varepsilon$, then $g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t) = 0$.
- if $a \neq 0, \chi = \varepsilon$, then $g_a(\chi) = \sum_{t \in \mathbb{F}_p} \xi^{at} = 0$.
- if $a \neq 0, \chi \neq \varepsilon$, then $g_a(\chi) = \chi^{-1}(a)g(\chi) = \chi(a^{-1})g(\chi)$.

Proof. The first 3 argument are trivial. For the last statement, we have

$$\begin{aligned}\chi(a)g_a(\chi) &= \chi(a)\sum_t \chi(t)\xi^{at} \\ &= \sum_t \chi(at)\xi^{at} \\ &= \sum_t \chi(t)\xi^t = g(\chi).\end{aligned}$$

So $g_a(\chi) = \chi^{-1}(a)g(\chi) = \chi(a^{-1})g(\chi)$. ∎

Theorem 6.2.4 If χ is a non-trivial character, then

$$\|g(x)\| = \sqrt{p}$$

Proof. We prove this theorem by evaluating $\sum_{a \in \mathbb{F}_p^\times} g_a(\chi)\overline{g_a(\chi)}$ twice. We have

$$\begin{aligned}\sum_{a \in \mathbb{F}_p^\times} g_a(\chi)\overline{g_a(\chi)} &= \sum_{a \in \mathbb{F}_p^\times} \chi(a^{-1})g(\chi)\overline{\chi(a^{-1})g(\chi)} \\ &= \sum_{a \in \mathbb{F}_p^\times} g(\chi)\overline{g(\chi)} \\ &= (p-1)\|g(\chi)\|^2\end{aligned}$$

Also

$$\begin{aligned}
\sum_{a\in\mathbb{F}_p^\times} g_a(\chi)\overline{g_a(\chi)} &= \sum_{a\in\mathbb{F}_p^\times}\left(\sum_{t\in\mathbb{F}_p}\chi(t)\xi^{at}\right)\left(\sum_{t\in\mathbb{F}_p}\chi(t)\xi^{at}\right)\\
&= \sum_{a\in\mathbb{F}_p^\times}\sum_{s,t}\chi(t)\overline{\chi(s)}\xi^{a(t-s)}\\
&= \sum_{t,s}\chi(t)\overline{\chi(s)}\sum_{a\in\mathbb{F}_p}\xi^{a(t-s)}
\end{aligned}$$

But

$$\sum_{a\in\mathbb{F}_p}\xi^{a(t-s)} = \begin{cases} p & \text{if } p = s\\ 0 & \text{if } t \neq s\end{cases}$$

So

$$\begin{aligned}
\sum_{a\in\mathbb{F}_p^\times} g_a(\chi)\overline{g_a(\chi)} &= \sum_{t,s}\chi(t)\overline{\chi(s)}\sum_{a\in\mathbb{F}_p}\xi^{a(t-s)}\\
&= \sum_{t}\chi(t)\overline{\chi(t)}p\\
&= (p-1)p
\end{aligned}$$

Thus $(p-1)p = (p-1)\|g(\chi)\|^2 \Rightarrow \|g(\chi)\| = \sqrt{p}$. ■

6.3 Class Notes 17-03-14