

## 1 Lecture 14 (April 19th)

**Theorem.** (5.57) (Third Isomorphism Theorem) Let  $R$  be a ring and let  $I$  be an ideal of  $R$ . Let  $J$  be an ideal containing  $I$  ( $I \subset J$ ). Then  $\bar{J} = J/I$  is an ideal of  $R/I$ , and all ideals of  $R/I$  may be realised in this way. Furthermore, the natural map  $R/I \rightarrow R/J$  (given by  $\bar{r} \mapsto \bar{r}$ ) induces an isomorphism

$$R/I \big/ J/I \cong R/J$$

*Proof.* We start by proving that  $\bar{J}$  is an ideal.

- (1) If  $J$  containing  $I$  is an ideal of  $R$ ,

$$\bar{J} = J/I = \{\bar{j} \mid j \in J\} \triangleleft R/I$$

is an ideal of  $R/I$  as it is the image of an ideal under a surjective homomorphism  $\pi : R \rightarrow R/I$ .

- (2) There is a bijection between the set of ideals of  $R$  containing  $I$  and the set of ideals of  $R/I$ .

- (2-1) Let  $\bar{J}$  be an ideal of  $R/I$ , that is,  $\bar{J} \triangleleft R/I$ . This implies that  $I \subset \pi^{-1}(\bar{J}) \triangleleft R$ . To show that  $I \subset \pi^{-1}(\bar{J})$ , let  $i \in I$ . We want to verify that  $\pi(i) \in \bar{J}$ . Note that  $\pi(i) = \bar{i} = \bar{0} \in \bar{J}$ .

- (2-2) We have seen that all ideals containing  $I$  have images that are ideals of  $R/I$  and the converse. Lastly notice that  $J \mapsto \bar{J}$  and  $\bar{J} \mapsto \pi^{-1}(\bar{J})$  are inverses of each other.

- (3) Note that there is a well-defined ring homomorphism  $p : R/I \rightarrow R/J : \bar{r} \mapsto \bar{r}$  ( $\bar{r} = \bar{s} \in R/I \implies \bar{r} = \bar{s} \in R/J$ ).

- (3-1)  $p$  is surjective.

- (3-2)  $r \in \ker p \iff p(\bar{r}) = \bar{r} = \bar{0} \in R/J \iff r - 0 = r \in J$ . So,  $\ker p = J/I$ .

- (3-3) Using the 1st isomorphism theorem, we see that

$$R/I \big/ \ker p = R/I \big/ J/I \cong R/J$$

□

**Example.** (i) Consider the ideals of  $\mathbf{Z}/6\mathbf{Z}$ , which are also the ideals of  $\mathbf{Z} = \{(n) \mid n \in \mathbf{Z}\}$  containing  $6\mathbf{Z} = (6)$ . They are  $\{(1), (2), (3), (6)\}$ , and

$$\mathbf{Z}/6\mathbf{Z} = \{\overline{(1)}, \overline{(2)}, \overline{(3)}, \overline{(6)}\}$$

## Chapter 6 Integral Domains

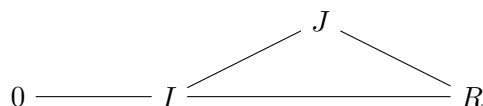
**Remark.** There are some key properties of  $\mathbf{Z}$ , such as

- (i) (Division algorithm)  $a = bq + r$  which generalises to Euclidean domains (EDs)
- (ii) (Every ideal is principle)  $(n) = I \triangleleft \mathbf{Z}$  which generalises to principle ideal domains (PIDs)
- (iii) (There exists an unique factorisation)  $n = p_1 p_2 \dots p_r$  which generalises to unique factorisation domains (UFDs)

### Chapter 6.1 Prime and Maximal Ideals

**Definition.** (6.4, 6.9) Let  $R$  be commutative ring, and  $I$  be an ideal of  $R$ .

- (i) A prime ideal  $I$  satisfies  $I \neq R$  ( $I$  is proper) and if  $a$  and  $b$  are in  $R$  such that  $ab \in I$ , then  $a \in I$  or  $b \in I$ .
- (ii) A maximal ideal  $I$  satisfies  $I \neq R$  and if  $J$  is an ideal containing  $I$ , then  $J = I$  or  $J = R$



**Remark.** (i) If  $p$  is a prime number, then  $(p) \subset \mathbf{Z}$  is a prime ideal.

(ii)  $0 \subset \mathbf{Z}$  is a prime ideal.

**Proposition.** (6.3) Every maximal ideal is a prime ideal.

*Proof.* Let  $I$  be a maximal ideal of  $R$ . Since  $I$  is maximal,  $I \neq R$ . Suppose now that  $ab \in I$  but  $a$  is not in  $I$ . In this case,  $I + (a)$  is an ideal properly containing  $I$ , so that  $I + (a) = R$  by the maximality of  $I$ . In particular,  $1 = i + ca$  for some  $c \in R$ . Then  $b = b \cdot 1 = b(i + ca) = bi + cab \in I$ , because  $ab \in I$ .  $\square$

**Theorem.** (6.1) Let  $R$  be a commutative ring, and  $I$  be an ideal of  $R$ . Then  $I$  is a prime ideal if and only if  $R/I$  is an integral domain.

**Theorem.** (6.2) Let  $R$  be a commutative ring, and  $I$  be an ideal of  $R$ . Then  $I$  is a maximal ideal if and only if  $R/I$  is a field.

## 2 Lecture 15 (May 6th)

### Chapter 6.2 Primes and Irreducibles

**Definition.** (6.15) Let  $R$  be a commutative ring. Let  $a$  and  $b$  be elements of  $R$ . We say that  $b$  divides  $a$  and write  $b|a$  if  $a \in (b)$ .

**Definition.** (6.18) Let  $R$  be an integral domain. Then  $p \in R$  is a prime element if it is nonzero, nonunit, and if  $p|ab$ , then  $p|a$  or  $p|b$ .

**Example.** In  $\mathbb{Z}$ , a prime number is a prime element.

**Lemma.** Let  $R$  be an integral domain and let  $p$  be a nonzero element of  $R$ . Then  $p$  is a prime element if and only if  $(p)$  is a prime ideal of  $R$ .

**Definition.** (6.20) Let  $R$  be an integral domain and let  $q$  be an element of  $R$ . We say that  $q$  is irreducible if it is nonunit and if  $q = ab$ , then  $a$  or  $b$  is a unit.

**Remark.** An irreducible element is nonzero.

**Theorem.** (6.23) Let  $R$  be an integral domain. Then every prime element is irreducible.

*Proof.* Let  $p \in R$  be a prime element. Note that  $p$  is not a unit. Assume that  $p = ab$ . Then,  $p|a$  or  $p|b$  because  $p|ab$ . If  $p$  divides  $a$ , then  $a = pc$  for some  $c \in R$ . Therefore,  $p = ab = pcb$ . This implies that  $b$  is a unit.  $\square$

**Example.** (6.21) In  $\mathbb{C}[x, y]/(y^2 - x^3)$ , the element  $\bar{x}$  is irreducible, but not prime.

### Chapter 6.3 Euclidean Domains and Principle Ideal Domains

**Definition.** (6.24) Let  $R$  be an integral domain. We say that  $R$  is a Euclidean domain if there exists a function

$$\nu : R \setminus \{0\} \rightarrow \mathbb{Z}^{\geq 0}$$

satisfying the following property: for every  $a \in R$  and every nonzero  $b \in R$ , there exists  $q$  and  $r$  in  $R$  such that

$$a = bq + r$$

where  $r = 0$  or  $\nu(r) < \nu(b)$ . The function  $\nu$  is called a Euclidean valuation.

**Example.** (i) Consider  $(\mathbb{Z}, |\cdot| : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{Z}^{\geq 0})$ . This implies that  $\mathbb{Z}$  is an Euclidean domain.

(ii) Let  $K$  be a field. Consider  $(K[x], \deg : K[x] \setminus \{0\} \rightarrow \mathbb{Z}^{\geq 0})$ . This implies that  $K[x]$  is a Euclidean domain.

**Definition.** (6.25) Let  $R$  be an integral domain. We say that  $R$  is a principle ideal domain or PID, if every ideal in  $R$  is principle. That is, if  $I$  is an ideal of  $R$ , then  $I = (r)$  for some  $r \in R$ .

**Theorem.** (6.26) Every Euclidean domain is a PID.

*Proof.* Let  $R$  be a ED. Let  $I$  be an ideal of  $R$ . If  $I = 0$ , then  $I = (0)$ . Otherwise, consider the set  $\{\nu(a) : a \in I \setminus \{0\}\}$ . Since this set is nonempty, it contains the smallest element by the well-ordering principle  $b$  for  $\mathbf{Z}^{\geq 0}$ . We claim that  $I = (b)$ . Since  $b \in I$ ,  $(b) \subset I$ . So it suffices to show that  $I \subset (b)$ . Let  $a \in I$ . Then  $a = bq + r$ , where  $r = 0$  or  $\nu(r) < \nu(b)$ . If  $\nu(r) < \nu(b)$ , then  $r \in I \setminus \{0\}$ . This contradicts to the fact that  $b$  is the smallest element of the set  $\{\nu(a) \mid a \in I \setminus \{0\}\}$ . Therefore,  $r = 0$ , and  $a = bq \in (b)$ .  $\square$

**Example.** (6.27, 28)

- (i)  $\mathbf{Z}$  is a PID
- (ii) Every field is a PID (the ideals of  $K$  are  $0 = (0)$  and  $K = (1)$ )
- (iii) If  $K$  is a field, then  $K[x]$  is a ED, hence a PID
- (iv)  $\mathbf{Z}[x]$  is not a PID. The ideal  $(2, x)$  is not principle.

**Proposition.** (6.30) Let  $R$  be a PID. Let  $I$  be a nonzero prime ideal. Then  $I$  is a maximal ideal.

*Proof.* Suppose we are given an ideal  $J$  such that  $I \subset J \subset R$ . Since  $R$  is a PID, we can set  $I = (a)$  and  $J = (b)$ . Then  $a = bc$  for some  $c \in R$ . Note that  $a \neq 0$ . Since  $I = (a)$  is a prime ideal,  $a$  is a prime element. Therefore,  $a|b$  or  $a|c$ . If  $a|b$ , then  $I = J$  and if  $a|c$ ,  $b = (1) = R$ .  $\square$

**Proposition.** (6.32) Let  $R$  be a PID. Then it satisfies the ascending chain condition on principle ideals: if  $I_1 \subset I_2 \subset \dots$  is a chain of ideals in  $R$ , then there is an index  $m$  such that  $I_m = I_{m+1} = I_{m+2} = \dots$  and so on.

*Proof.* Let  $I$  be the union of the ideals  $I_k$  (verify that  $I$  is an ideal of  $R$ ). Since  $R$  is a PID,  $I = (r)$  for some  $r \in R$ . In particular,  $r \in I_m$  for some  $m \geq 1$ . This implies that  $I_m = I_{m+i}$  for every  $i \geq 0$ .

$$I_m \subset I = \bigcup I_k = (r) \subset I_m$$

$\square$

## Chapter 6.4 Principle Ideal Domains and Unique Factorisation Domains

**Definition.** (6.37) Let  $R$  be an integral domain. Then  $R$  is a unique factorization domain or UFD if it satisfies the following condition: suppose that  $a \in R$  is nonzero and nonunit. Then there exists finitely many irreducible elements  $q_1, q_2, \dots, q_r$  such that  $a = q_1 q_2 \dots q_r$ . Moreover, this factorisation is unique in the sense that if

$$a = q_1 q_2 \dots q_r = p_1 p_2 \dots p_s$$

where all  $p_i$  and  $q_j$  are irreducible, then  $s = r$  and after reordering factors we have  $(p_i) = (q_i)$  for all  $i$ .

**Proposition.** (6.33) Let  $R$  be a PID and let  $q \in R$  be an irreducible element. Then  $(q)$  is a maximal ideal.

*Proof.* Since  $q$  is nonunit,  $(q) \neq R$ . Let  $I$  be an ideal of  $R$  such that  $(q) \subset I \subset R$ . Since  $R$  is a PID,  $I = (a)$  for some  $a \in R$ . Then  $q = ab$  for some  $b \in R$ .  $\square$

**Lemma.** Let  $R$  be a PID. Let  $a$  be a nonzero and nonunit element of  $R$ . If  $(a)$  is maximal, then  $a$  is irreducible.

*Proof.* Let  $a = bc$ . Then  $(a) \subset (b) \subset R$ . As  $(a)$  is maximal,  $(b) = (1) = R$  or  $(b) = (a)$  and either  $b$  or  $c$  are units.  $\square$

**Theorem.** (6.35) Every PID is a UFD.

*Proof.* Let  $R$  be a PID. We make the following observation: let  $a$  be a non-zero and non-unit element of  $R$ . If  $a$  is not irreducible, then there exists an irreducible element  $q \in R$  such that  $q|a$ . By lemma,  $(a)$  is not maximal. That is, we can find  $(a) \subsetneq (a_1) \subsetneq R$ . If  $(a_1)$  is maximal, then  $a_1$  is irreducible by lemma. Otherwise, we can find  $(a_1) \subsetneq (a_2) \subsetneq R$ .

For existence, let  $a$  be a nonzero nonunit element of  $R$ . If  $a$  is irreducible, then we're done. Otherwise, we can find an irreducible factor  $q_1$  of  $a$  by observation, so that  $a = q_1 a_1$ . Note that  $a_1$  is nonzero and nonunit (in particular,  $(a) \subsetneq (a_1) \subsetneq R$ ). If  $a_1$  is irreducible, then we're done. Otherwise, we can find an irreducible factor  $q_2$ , so that

$$a_1 = q_2 a_2$$

Try uniqueness on your own.  $\square$

**Remark.** (6.39) Not every UFD is a PID. For example,  $\mathbb{Z}[x]$  and  $\mathbb{C}[x, y]$ .

$$\text{ED} \subset \text{PID} \subset \text{UFD} \subset \text{ID}$$

### 3 Lecture 16 (May 17th)

#### Chapter 6.5 The Field of Fractions of an Integral Domain

**Remark.** In this chapter, we try to generalise the construction of the field of integers  $\mathbb{Q}$  of rational numbers from the ring  $\mathbb{Z}$  of integers.

**Lemma.** (6.42) Let  $R$  be an integral domain. Let  $\hat{F}$  be the set defined as follows:

$$\{(n, d) \in R \times R \mid d \neq 0\}$$

We define the relation on  $\hat{F}$  as follows:

$$(n_1, d_1) \sim (n_2, d_2) \iff n_1 d_2 = n_2 d_1$$

The relation  $\sim$  on  $\hat{F}$  is an equivalence relation.

*Proof.* We prove reflexivity, symmetry, and transitivity.

- (i) (Reflexivity)  $(r, s) \sim (r, s)$
- (ii) (Symmetry)  $(r_1, s_1) \sim (r_2, s_2)$  implies that  $(r_2, s_2) \sim (r_1, s_1)$
- (iii) (Transitivity)  $(r_1, s_1) \sim (r_2, s_2)$  and  $(r_2, s_2) \sim (r_3, s_3) \implies (r_1, s_1) \sim (r_3, s_3)$ . For transitivity, we want to show that  $r_1 s_3 = r_3 s_1$ . Note that

$$\begin{aligned} (r_1 s_3) s_2 &= r_1 (s_3 s_2) = r_1 (s_2 s_3) = r_1 (s_2 s_3) = (r_1 s_2) s_3 = (r_2 s_1) s_3 \\ &= r_2 (s_1 s_3) = r_2 (s_3 s_1) = (r_2 s_3) s_1 = (r_3 s_2) s_1 = r_3 (s_2 s_1) = (r_3 s_1) s_2 \end{aligned}$$

Since  $s_2$  is nonzero and  $R$  is an integral domain,  $r_1 s_2 = r_3 s_1$ .

□

**Definition.** Let  $R$  be an integral domain. The field of fractions of  $R$  is the quotient  $F = \hat{F} / \sim$  endowed with the following addition and multiplication.

$$\overline{(r_1, s_1)} + \overline{(r_2, s_2)} = \overline{(r_1 s_2 + r_2 s_1, s_1 s_2)}$$

and

$$\overline{(r_1, s_1)} \cdot \overline{(r_2, s_2)} = \overline{(r_1 r_2, s_1 s_2)}$$

**Remark.** The addition and multiplication are well-defined! In other words,  $\overline{(r_1, s_1)} = \overline{(r'_1, s'_1)}$  and  $\overline{(r_2, s_2)} = \overline{(r'_2, s'_2)}$  implies that  $\overline{(r_1 r_2, s_1 s_2)} = \overline{(r'_1 r'_2, s'_1 s'_2)}$ . We first do multiplication. Suppose that  $(r_1, s_1) \sim (r'_1, s'_1)$  and  $(r_2, s_2) \sim (r'_2, s'_2)$ . We wish to show that

$(r_1 r_2, s_1 s_2) \sim (r'_1 r'_2, s'_1 s'_2)$ . We see that

$$\begin{aligned} (r_1 r_2)(s'_1 s'_2) &= (r_1 s'_1)(r_2 s'_2) \\ &= (r'_1 s_1)(r_2 s'_2) \\ &= (r'_1 s_1)(r'_2 s_2) \\ &= (r'_1 r'_2)(s_1 s_2) \end{aligned}$$

**Proposition.**  $(F, +, \cdot)$  forms a field. For the proof, we need to verify the following:

- (i)  $(F, +, \cdot)$  forms a ring
- (ii) The multiplication on  $F$  is commutative
- (iii)  $(F, +, \cdot)$  is nontrivial
- (iv) If  $\overline{(r, s)}$  is nonzero in  $F$ , it has a multiplicative inverse.

*Proof.* For (ii), we see that

$$\overline{(r_1, s_1)} \cdot \overline{(r_2, s_2)} = \overline{(r_1 r_2, s_1 s_2)} = \overline{(r_2 r_1, s_2 s_1)} = \overline{(r_2, s_2)} \cdot \overline{(r_1, s_1)}$$

For (iii), we claim that  $\overline{(0, 1)} \neq \overline{(1, 1)}$ . Suppose not. Then  $0 \cdot 1 = 1 \cdot 1$  which is a contradiction because  $R$  is an integral domain.

For (iv), assume that  $\overline{(r, s)} \neq \overline{(0, 1)}$  in  $F$ . Then  $r \neq 0$  and  $\overline{(s, r)}$  is a multiplicative inverse of  $\overline{(r, s)}$ . Indeed,

$$\overline{(r, s)} \cdot \overline{(s, r)} = \overline{(s, r)} \cdot \overline{(r, s)} = \overline{(sr, rs)} = \overline{(rs, sr)} = \overline{(1, 1)}$$

□

**Remark.** (i) Just like there is an injective ring homomorphism  $\mathbf{Z} \rightarrow \mathbf{Q}$  by sending  $n$  to  $n/1$ , there exists an injective ring homomorphism

$$i : R \rightarrow F : r \mapsto \overline{(r, 1)}$$

Where (1)  $i$  is a ring homomorphism, and (2) we have

$$\begin{aligned} r \in \ker i &\iff \overline{(r, 1)} = \overline{(0, 1)} \\ &\iff r \cdot 1 = 0 \cdot 1 \end{aligned}$$

in  $R$ .

**Theorem.** (6.45) Let  $R$  be an integral domain. Let  $F$  be the field of fractions of  $R$  and let  $i : R \rightarrow F$  denote the ring homomorphism given by  $r \mapsto \overline{(r, 1)}$ . Let  $K$  be a field and let

$i_K : R \rightarrow K$  be an injective ring homomorphism. Then there exists a unique injective ring homomorphism  $j : F \rightarrow K$  such that  $i_K = j \circ i$ .

*Proof.* We claim that there exists a unique injective ring homomorphism  $j$  such that  $j \circ i = i_K$ . For existence, define  $j : F \rightarrow K$  to be defined as  $j(\overline{(r, s)}) = i_K(r) \cdot (i_K(s))^{-1}$ . Then

$$\begin{aligned} j(\overline{(r, s)}) &= j(\overline{(r, 1)} \cdot \overline{(1, s)}) \\ &= j(\overline{(r, 1)}) \cdot j(\overline{(1, s)}) \\ &= j(i(r)) \cdot j(\overline{(s, 1)}^{-1}) \\ &= j(i(r)) \cdot j(i(s))^{-1} \\ &= (j \circ i)(r) \cdot ((j \circ i)(s))^{-1} \\ &= i_K(r) \cdot (i_K(s))^{-1} \end{aligned}$$

The remaining task is to verify that  $j$  is well defined, that it is a ring homomorphism,  $j$  is injective, and that  $j \circ i = i_K$ .

For uniqueness, suppose that  $i'_K : F \rightarrow K$  is another injective ring homomorphism with  $j' \circ i = i'_K$ . We need to show that  $j = j'$ .  $\square$

#### 4 Lecture 17 (May 8th)

**Recall.** (5.57) (The 3rd Isomorphism Theorem) Let  $R$  be a ring and  $I \subset J$  be ideals of  $R$ . Then,

$$R/I \big/ J/I \cong R/J$$

**Example.** (5.38) Observe that

$$\mathbf{Z}[x] / (2, x) \cong \mathbf{Z} / 2\mathbf{Z} \quad \text{as} \quad \mathbf{Z}[x] / (2, x) \cong \mathbf{Z}[x] / (x) \big/ (2, x) / (x)$$

**Example.** Here are some points that are worth considering.

- (1) Let  $R$  be a commutative ring.  $R$  is an integral domain if and only if  $0$  is a prime ideal.
- (2-1)  $0 \neq (p) \subset \mathbf{Z}$  is a prime ideal if and only if  $p$  is a prime number.
- (2-2)  $0 \subset \mathbf{Z}$  is a prime ideal.
- (3-1) Is  $(x) \subset \mathbf{Z}[x]$  a prime ideal? Well,  $(a) \neq \mathbf{Z}[x]$  and  $(x) \mid f(x) \cdot g(x)$  implies that  $(x) \mid f(x)$  or  $(x) \mid g(x)$ . An equivalent question would be whether  $\mathbf{Z}[x] / (x)$  is an integral domain. By the 1st isomorphism theorem, it is isomorphic to  $\mathbf{Z}$  and this is true.



(3-2) Since  $\mathbf{Z}[x] / (x)$  is not a field,  $(x)$  is not a maximal ideal of  $\mathbf{Z}[x]$ . Notice that there exists  $(x, 2)$ .

(4)  $(y - x^2) \subset \mathbf{C}[x, y]$  is prime. Notice that the following is an integral domain

$$\mathbf{C}[x, y] / (y - x^2) \cong \mathbf{C}[x]$$

(5) Let  $I \subset \mathbf{Z}$  be an ideal.  $I$  is maximal if and only if  $I$  is a nonzero prime ideal.

(6) Let  $K$  be a field. Then  $(x)$  is a maximal ideal in  $K[x]$ . However,  $(x)$  is not maximal in  $K[x, y]$ , as

$$(x) \subsetneq (x, y) \subsetneq K[x, y]$$

Note that  $(x, y) \subset K[x, y]$  is maximal.

## 5 Lecture 18 (May 13th)

**Remark.** Last time, we learned about prime and maximal ideals. Today, we will be learning some basics on polynomials.

### Chapter 7 Polynomial Rings and Factorization

#### Chapter 7.2 The Polynomial Rings with Coefficients in a Field

**Definition.** (7.1) Let  $R$  be a ring. Let  $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$  be a nonzero polynomial with  $a_n \neq 0$ . Then the integer  $n$  is called the degree of  $f$ ;  $a_n$  is the leading coefficient of  $f$ ;  $a_0$  is the constant term of  $f$ .

**Theorem.** (7.2) Let  $K$  be a field. Then  $K[x]$  is a Euclidean domain.

**Proposition.** (7.3) Let  $R$  be a ring and let  $f(x)$  and  $g(x)$  be elements of  $R[x]$  with  $g(x) \neq 0$ . Suppose that the leading coefficient of  $g(x)$  is a unit. Then there exists  $q(x)$  and  $r(x)$  in  $R[x]$  such that  $f(x) = g(x) \cdot q(x) + r(x)$ , where  $r(x) = 0$  or  $\deg r(x) < \deg g(x)$ .

*Proof.* The proof is omitted for now. Loosely speaking, one we set the minimum order  $n$  for  $f(x)$  such that the division algorithm doesn't work, we find that it doesn't work for  $n - 1$  either, which is a contradiction.  $\square$

**Example.** (7.5)  $R$  is a ring,  $f(x) \in R[x]$ . Then  $(x - a)$  is a factor of  $f(x)$  if and only if  $f(a) = 0$ . For the if direction, write  $f(x) = (x - a) \cdot q(x) + r(x)$ . Then  $r(x)$  must be 0.

**Definition.** (7.6) Let  $R$  be a ring and  $f(x) \in R[x]$  be a polynomial. We will say that  $a \in R$  is a zero of  $f(x)$  if  $f(a) = 0$ .

**Corollary.** (7.7) If  $K$  is a field, then  $K[x]$  is a PID.

**Corollary.** (7.8) If  $K$  is a field, then  $K[x]$  is a UFD.

**Proposition.** (7.9) Let  $R$  be an integral domain. Let  $f(x)$  and  $g(x)$  be polynomials over  $R[x]$  with  $g(x) \neq 0$ . Suppose that the leading coefficient of  $g(x)$  is a unit. Then the quotient  $q(x)$  and the remainder  $r(x)$  are unique.

*Proof.* See how

$$g_1(x) - g_2(x) = (q_1(x) - q_2(x))f(x) + (r_1(x) - r_2(x))$$

If  $(r_1(x) - r_2(x)) \neq 0$ , we find that neither of the left terms are zero and as  $\deg f(x) > \deg r(x)$  the statement is a contradiction.  $\square$

**Theorem.** (7.11) Let  $K$  be a field and let  $f(x)$  be a nonzero polynomial of degree  $n$ . Then  $K[x] / (f(x))$  is an  $n$ -dimensional vector space over  $K$ .

*Proof.* We briefly sketch a proof. First note how

$$a \in K, \overline{g(x)} \in K[x] / (f(x)) \implies a \cdot \overline{g(x)} = \overline{a \cdot g(x)}$$

and that  $K[x] / (f(x))$  is closed under scalar multiplication. We further note how the subset  $\{\overline{x^0}, \overline{x^1}, \overline{x^2}, \dots, \overline{x^{n-1}}\} \subset K[x] / (f(x))$  forms a basis for the  $K$ -vector space  $K[x] / (f(x))$ . See that for any  $\overline{g(x)} \in K[x] / (f(x))$ ,

$$\overline{g(x)} = \overline{f(x)} \cdot \overline{q(x)} + \overline{r(x)} = \overline{r(x)} = \overline{b_0} \cdot \overline{1} + \dots + \overline{b_{n-1}} \cdot \overline{x^{n-1}}$$

and that a polynomial can be expressed in terms of the basis.  $\square$

## 6 Lecture 19 (May 15th)

Last time we have learned some definitions about polynomials. Today, we will learn about irreducible polynomials.

### Chapter 7.3 Irreducibility in Polynomial Rings

**Example.** (7.13) If  $K$  is a field and  $a$  is nonzero, then  $ax + b$  is irreducible. Note that, first of all, it is a non-zero non-unit element ( $ax + b \notin (K[x])^\times = K^\times = K$ ). Secondly, if  $ax + b = f(x) \cdot g(x)$ , we observe that  $f(x)$  or  $g(x)$  is in  $K$ , which would make it a unit.

**Remark.** We make two short remarks. Let  $R$  be an integral domain.

- (i)  $f(x), g(x) \in R[x]$  implies that  $\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x)$
- (ii)  $(R[x])^\times = R^\times$

**Remark.** The condition that  $K$  is a field is essential. Note how  $2x \in \mathbf{Z}[x]$  is not irreducible (it is reducible) as it can be expressed as  $2 \cdot x$  with both 2 and  $x$  being non-unit non-zero elements.

**Proposition.** (7.14) Let  $K$  be a field and let  $f(x) \in K[x]$  be a polynomial of degree at least 2 ( $\deg f(x) \geq 2$ ). If  $f(x)$  has a zero, then  $f(x)$  is reducible.

*Proof.* Assume that  $f(a) = 0$  for some  $a \in K$ . We can write  $f(x) = (x - a)g(x)$ , where  $\deg g(x) \geq 1$  ( $\deg f(x) = \deg(x - a) + \deg g(x)$ ).  $g(x)$  is not a unit and  $(x - a)$  isn't either. Therefore,  $f(x)$  is reducible. The converse isn't true, with examples such as  $(x^2 + 1)^2 \in \mathbf{R}[x]$ .  $\square$

**Proposition.** (7.15) Let  $K$  be a field and let  $f(x) \in K[x]$  be a polynomial of degree 2 or 3. Then  $f(x)$  is irreducible if and only if  $f(x)$  has no zeros in  $K$ .

*Proof.* Thanks to the above proposition, it suffices to prove that if  $f(x)$  has no zeros,  $f(x)$  is irreducible. We prove by contraposition, that if  $f(x)$  is reducible (it is trivially non-zero and non-unit),  $f(x)$  has zeros in  $K$ . As  $f(x)$  is reducible

$$f(x) = g(x) \cdot h(x)$$

for non-unit  $g(x)$  and  $h(x)$ . Then, the degree of  $g(x)$  and  $h(x)$  are atleast 1, telling us that either one of them has to be 1 due to the fact that

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

Now, as  $f(x)$  contains a linear factor  $(ax + b)$  with  $a \neq 0$ ,  $f(x)$  has a zero.  $\square$

**Remark.** (7.16)

- (i) The fact that the ring of choice is a field is critical. For example,  $(2x - 1)^2 \in \mathbf{Z}[x]$  is reducible, but has no zero in  $\mathbf{Z}$ .
- (ii) We can't extend the argument to higher degrees. Take, for example,  $x^4 - 4 = (x^2 + 2)(x^2 - 2) \in \mathbf{Q}[x]$ . The polynomial is reducible and has no zeros in  $\mathbf{Q}$ .

**Theorem.** (7.17) (Fundamental theorem of algebra) Every non-constant polynomial over  $\mathbf{C}$  has a zero in  $\mathbf{C}$ .

**Corollary.** A polynomial  $f(x) \in \mathbf{C}[x]$  is irreducible if and only if its  $\deg f(x) = 1$ .

**Proposition.** (7.20) Let  $f(x) \in \mathbf{R}[x]$  be a polynomial. Then  $f(x)$  is irreducible if and only if

- (i)  $\deg f(x) = 1$
- (ii)  $\deg f(x) = 2$  and  $f(x) = ax^2 + bx + c$  with  $b^2 - 4ac < 0$

*Proof.* The if part should be trivial. We prove the only if part. For degrees higher than 3, Let  $f(x) = c(x - a_1)(x - a_2) \dots (x - a_n) \in \mathbf{C}[x]$  and  $f(x) \in \mathbf{R}[x] \subset \mathbf{C}[x]$ . From here, if  $a_i \in \mathbf{C}$ ,  $f(a_i) = 0$  implies that  $f(\bar{a}_i) = 0$ . With this knowledge,  $(x - a_i)(x - \bar{a}_i)$  is a polynomial with real coefficients that divides  $f(x)$ .  $\square$

## 7 Lecture 20 (May 20th)

Last time, we have learned about irreducible polynomials over  $\mathbf{C}$  and  $\mathbf{R}$ . Today, we'll do  $\mathbf{Q}$  and  $\mathbf{Z}$ .

### Chapter 7.4 Irreducibility in $\mathbf{Q}[x]$ and $\mathbf{Z}[x]$

**Definition.** (6.16) Let  $R$  be an integral domain and let  $a$  and  $b$  be elements in  $R$ . We will say that  $g \in R$  is a greatest common divisor of  $a$  and  $b$  if

- (i)  $(a) + (b) \subset (g)$
- (ii) If  $(a) + (b) \subset (g')$  for  $g' \in R$ ,  $(g) \subset (g')$

**Definition.** (7.25) Let  $R$  be a UFD and  $f(x)$  be a nonzero polynomial over  $R$ . Then, the content of  $f(x)$  denoted  $\text{cont}(f)$  is defined as the greatest common divisor of its coefficients. We say that  $f(x) \in R[x]$  is primitive if its content is 1.

**Remark.** Let  $R$  be a UFD and  $f(x) \neq 0$  be in  $R[x]$ . Then we can write  $f(x) = \text{cont}(f) \cdot f_1(x)$  where  $f_1(x) \in R[x]$  is primitive.

## 8 Lecture 21 (May 22nd)

Today, we will learn about Gauss' lemma.

**Remark.** In a UFD  $R$ , if  $p \in R$  is irreducible,  $p$  is prime.

**Theorem.** (Gauss' lemma) Let  $R$  be a UFD, and let  $f(x)$  and  $g(x)$  be nonzero polynomials over  $R$ . Then

$$\text{cont}(fg) = \text{cont}(f) \cdot \text{cont}(g)$$

In particular, if  $f$  and  $g$  are primitive, then so is  $f \cdot g$ .

*Proof.* It will suffice to show that if  $f(x)$  and  $g(x)$  are primitive, then so are  $f(x) \cdot g(x)$ . Then, the theorem follows automatically from the fact that

$$\text{cont} \left( \text{cont}(f) f_1 \right) = \text{cont}(f) \text{cont}(f_1)$$

Suppose that  $f(x)g(x)$  is not primitive. Then there exists an irreducible  $p$  in  $R$  such that the image of  $f(x)g(x)$  under the ring homomorphism

$$\phi : R[x] \rightarrow (R/(p))[x]$$

is zero. That is,

$$\overline{f(x) \cdot g(x)} = 0$$

This tells us that, as  $R/(p)$  is an integral domain, one of the polynomials are zero. However, this implies that one of the polynomials has a coefficient that isn't 1, that is, one of the polynomials are not primitive. This is a contradiction.  $\square$

**Corollary.** (7.26) Let  $R$  be a UFD and  $f(x) \in R[x]$  be primitive. Then  $f(x)$  is irreducible in  $R[x]$  if and only if  $f(x)$  is irreducible in  $Q[x]$ , where  $Q = \text{Frac}(R)$ .

**Corollary.** (7.27) If  $R$  is a UFD, then  $R[x]$  is also a UFD.

**Remark.** If  $R$  is a UFD,  $R[x_1, \dots, x_n]$  is also a UFD.

**Remark.** Let  $f(x) \in Q[x]$  be a nonzero polynomial ( $R$  is a UFD and  $Q = \text{Frac}(R)$ ). We can write

$$f(x) = \frac{a}{b} f_1(x)$$

where  $a$  and  $b$  are nonzero elements in  $R$  and  $f_1(x) \in R[x]$  is primitive polynomial over  $R$ . Remark that the irreducibility of  $Q$  is equivalent to the irreducibility of  $f_1(x)$  over  $Q$ .

## 9 Lecture 22 (May 27th)

Last time, we have learned Gauss' lemma. Today, we will be learning irreducibility tests.

**Recall.** (Gauss' lemma) Let  $R$  be a UFD. For  $f(x), g(x) \in R[x]$ ,

$$\text{cont}(f \cdot g) = \text{cont}(f) \cdot \text{cont}(g)$$

**Corollary.** (7.26) Let  $R$  be a UFD,  $Q = \text{Frac}(R)$  and  $f(x) \in R[x]$  be a primitive polynomial.  $f(x)$  is irreducible in  $R[x]$  if and only if  $f(x)$  is irreducible in  $Q[x]$ .

*Proof.* We do the only if part first. Suppose that  $f(x) = g(x)h(x)$  in  $Q[x]$ . Write for  $f(x) = g(x)h(x)$  for  $g(x), h(x) \in Q[x]$ . Write  $g(x) = (a/b)g_1(x)$  and  $h(x) = (c/d)h_1(x)$

where  $a, b, c, d \in R \setminus \{0\}$ , and  $g_1(x)$  and  $h_1(x)$  are primitives in  $R[x]$ . Then  $bd \cdot f(x) = ac \cdot g_1(x)h_1(x)$ .  $\square$

**Corollary.** (7.27) If  $R$  is a UFD, so is  $R[x_1, x_2, \dots, x_n]$ .

**Example.** (i)  $\mathbf{Z}[x_1, \dots, x_n]$  is a UFD.

(ii) If  $K$  is a field,  $K[x_1, \dots, x_n]$  is a UFD.

**Theorem.** (7.22) For a UFD  $R$ , let  $f(x) \in R[x]$ . If  $f(x) = g(x) \cdot h(x)$  in  $Q[x]$ , there exists  $a, b \in Q$  such that  $f(x) = (a \cdot g(x))(b \cdot h(x))$  where  $a \cdot g(x)$  and  $b \cdot h(x)$  are in  $R[x]$ . By Gauss' lemma,  $u \cdot bd = ac$  for some  $u \in R^\times$ . Then  $f(x) = u \cdot g_1(x) \cdot h_1(x)$ . Since  $f(x) \in R[x]$  is irreducible, either  $g_1(x)$  and  $h_1(x)$  is in  $R^\times$ . Consequently, either

$$g(x) = \frac{a}{b}g_1(x) \in Q^\times \quad \text{or} \quad h(x) = \frac{c}{d}h_1(x) \in Q^\times$$

**Example.**  $R = \mathbf{Z}$  and  $Q = \mathbf{Q}$ . Test the irreducibility of

$$f(x) = \frac{4}{3} - \frac{6}{5}x^7$$

#### Chapter 7.4 Irreducibility Tests in $R[x]$ Where $R$ is a UFD

**Proposition.** (7.29) (The rational root test) Let  $R$  be a UFD. Let  $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$  be a polynomial of degree  $n$ . Let  $c = p/q \in \mathbf{Q}$  be a zero of  $f(x)$ , where  $p, q \in R$  with  $(p, q) = 1$ . Then  $p|a_0$  and  $q|a_n$ .

*Proof.* Notice that

$$0 = f\left(\frac{p}{q}\right) = a_0 + a_1\left(\frac{p}{q}\right) + \dots + a_n\left(\frac{p}{q}\right)^n$$

and multiplying  $q^n$ , we have

$$0 = a_0q^n + (a_1pq^{n-1} + \dots + a_np^n)$$

carefully examining the expression, we find that  $p$  divides  $a_0$  and  $q$  divides  $a_n$ .  $\square$

**Example.** (7.30, 31, 32)

(i)  $f(x) = 4x^3 + 2x^2 - 5x + 3$  is irreducible in  $\mathbf{Q}[x]$ . The possible roots are

$$\pm\left(1, 3, \frac{1}{2}, \frac{3}{2}, \frac{1}{4}, \frac{3}{4}\right)$$

however, none of these is a zero of  $f(x)$ .

- (ii)  $g(x) = 3 - 4x + 2x^2 + 4x^3$  is a reducible polynomial. This is because  $g(-3/2) = 0$ .
- (iii)  $h(x) = 1 - 3x^2 + x^4$  has no rational roots. It does not follow that  $h(x)$  is irreducible. In fact,  $h(x) = (-1 + x + x^2)(-1 - x + x^2)$ , so  $h(x)$  is reducible in  $\mathbf{Q}[x]$ .

**Theorem.** (7.35) (Eisenstein's criterion) Let  $R$  be a UFD and let  $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$  be a polynomial of degree  $n$ . Let  $p \in R$  be an irreducible element. Suppose that

- (i)  $p \nmid a_n$
- (ii)  $p \mid a_0, a_1, \dots, a_{n-1}$
- (iii)  $p^2 \nmid a_0$

Then  $f(x)$  cannot be written as a product of two polynomials of positive degrees, and hence it is irreducible in  $\mathbf{Q}[x]$ .

**Example.** Let  $f(x) = 5 + 10x + x^4 \in \mathbf{Z}[x] \subset \mathbf{Q}[x]$ . Take  $p = 5$  which is a prime number in  $\mathbf{Z}$ .  $5 \nmid 1$ ,  $5 \mid 5, 10$  and  $5^2 = 25 \nmid 5$ . Altogether, they imply that  $f(x)$  is irreducible in  $\mathbf{Q}[x]$ .

## 10 Lecture 23 (May 29th)

Last time, we learned about irreducibility tests including Eisenstein's criterion. Today we learn about some applications of the criterion and group theory.

**Theorem.** (7.35) (Eisenstein's criterion) Take  $R$  to be a UFD. Let  $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$  be a polynomial of degree  $n$ . Let  $p \in R$  be irreducible. If

- (i)  $p \nmid a_n$
- (ii)  $p \mid a_0, a_1, \dots, a_{n-1}$
- (iii)  $p^2 \nmid a_0$

then  $f(x)$  is irreducible in  $\mathbf{Q}[x]$ .

**Example.** (i)  $f(x) = x^4 + 10x + 5 \in \mathbf{Z}[x]$ . By taking  $p = 5$ , we notice that  $f(x)$  is irreducible over  $\mathbf{Q}[x]$ .

- (ii)  $f(x) = x^4 + 1 \in \mathbf{Z}[x]$ . The function is irreducible if and only if  $f(x+1) \in \mathbf{Z}[x]$  is irreducible. That is,

$$f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$$

is irreducible. Taking  $p = 2$ , we notice that  $f(x)$  is irreducible over  $\mathbf{Q}[x]$ .

**Corollary.** (7.38) There are irreducible polynomials in  $\mathbf{Q}[x]$  of arbitrary high degree.

*Proof.* For each  $n \geq 1$ , consider  $x^n - 2 \in \mathbf{Q}[x]$  □

**Example.** (7.38) Let  $p \in \mathbf{Z}$  be a prime number. Then the cyclotomic polynomial

$$\Phi_p(x) = 1 + x + x^2 + \dots + x^{p-1}$$

is irreducible in  $\mathbf{Q}[x]$ . For this, we note that  $\Phi_p(x)$  is irreducible over  $\mathbf{Q}$  if and only if  $\Phi_p(x+1)$  is irreducible over  $\mathbf{Q}$ . Since

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}$$

we have

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{i=1}^p {}^pC_i x^{i-1} = {}^pC_1 + {}^pC_2 x + \dots + {}^pC_p x^{p-1}$$

Using the fact that  $p \mid {}^pC_i$  for  $1 \leq i \leq p-1$ , we can apply Eisenstein's criterion to deduce that  $\Phi_p(x+1) \in \mathbf{Q}[x]$  is irreducible.

**Remark.** Read proposition (7.33) and example (7.34).

## Chapter 11 Groups-Preliminaries

### Chapter 11.1 Groups and their Categories

**Definition.** (11.1) A group consists of a set  $G$  along with a binary operation on  $G$  such that

- (i) (Associativity)  $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$  for all  $g_1, g_2, g_3 \in G$
- (ii) (Identity element) There exists  $e \in G$  such that  $g * e = e * g = g$  for all  $g \in G$
- (iii) (Inverse element) For each  $g_1 \in G$ , there exists  $g_2 \in G$  such that  $g_1 * g_2 = e$

**Definition.** For group  $G$ , we say that  $G$  is abelian if

$$g_1 * g_2 = g_2 * g_1$$

for all  $g_1, g_2 \in G$ .

**Example.** If  $(R, +, \cdot)$  is a ring, then  $(R, +)$  is an abelian group.

**Remark.**  $(R, \cdot)$  is not necessarily a group.

**Remark.** (i) The identity  $e$  is unique

- (ii) For each  $g \in G$ , the inverse of  $g$  is unique



(iii)  $(g^{-1})^{-1} = g$

(iv) (Cancellation holds in groups) If  $g_1 * h = g_2 * h$  or  $h * g_1 = h * g_2$ , then  $g_1 = g_2$

**Remark.** In the future, we will write

$$g * h \rightarrow gh$$

and

$$g * g * g \rightarrow g^3$$

## 11 Lecture 24 (June 5th)

Last time, we learned the basics of group theory. Today, we'll learn basic properties of groups.

**Remark.** A group is called abelian if  $g * h = h * g$ .

- (i) (Uniqueness of the identity element)  $e$  is unique
- (ii) (Uniqueness of inverses)  $g^{-1}$  is unique
- (iii)  $(g^{-1})^{-1} = g$
- (iv) (Cancellation law)  $g_1 * h = g_2 * h$  implies that  $g_1 = g_2$
- (v) We use multiplicative notation
- (vi) We use additive notation for abelian groups

**Definition.** (11.2) Let  $G$  and  $H$  be groups. A function  $\phi : G \rightarrow H$  is a group homomorphism if it satisfies

$$\phi(g_1 * g_2) = \phi(g_1) * \phi(g_2)$$

for all  $g_1$  and  $g_2$  in  $G$ .

**Example.** (The trivial group homomorphism) The function  $G \rightarrow H : g \mapsto e$  is a group homomorphism, where  $1$  is the identity element.

**Proposition.** (11.3)

- (i) The map  $\text{id} : G \rightarrow G$  is a group homomorphism
- (ii) A composition of group homomorphisms is also a group homomorphism. That is, if  $\phi : G \rightarrow H$  and  $\psi : H \rightarrow K$  are group homomorphisms, then so is the composition  $\psi \circ \phi : G \rightarrow K$  as

$$(\psi \circ \phi)(g_1 * g_2) = \psi(\phi(g_1) * \phi(g_2)) = \psi(\phi(g_1)) * \psi(\phi(g_2))$$

**Definition.** (11.5) Let  $\phi : G \rightarrow H$  be a group homomorphism. We will say that  $\phi$  is an isomorphism if there exists a group homomorphism  $\psi : H \rightarrow G$  such that  $\psi \circ \phi = \text{id}_G$  and  $\phi \circ \psi = \text{id}_H$ .

**Remark.** (i)  $\phi$  is an isomorphism if and only if it is bijective

(ii) Being isomorphic is an equivalence relation

(iii)  $\phi(e) = e$

**Definition.** Let  $A$  be a nonempty set. Then the pair

(the set of all bijections on  $A$ , their composition)

is called a symmetric group on  $A$  and is denoted  $S_A$ . Notationwise, if  $|A| = n$ , we will denote  $S_A$  by  $S_n$ .

**Remark.** If  $|A| = |B|$ , then  $S_A$  is isomorphic to  $S_B$ . Thus, we justify our notation from above.

**Definition.** (11.6) Let  $G$  be a group and  $H$  be a subset of  $G$ . We say that  $H$  is a subgroup of  $G$  if

(i)  $H$  is closed under the group operation

(ii)  $e$  is in  $H$

(iii) For each  $h \in H$ ,  $h^{-1} \in H$

**Example.** (11.8, 11.9, 11.10)

(i) If  $H$  and  $K$  are subgroups of  $G$ , then  $H \cap K$  is also a subgroup of  $G$

(ii) Let  $\phi : G \rightarrow G'$  be a group homomorphism. If  $H$  is a subgroup of  $G$ , then  $\phi(H)$  is a subgroup of  $G'$ . In particular,  $\text{im } \phi = \phi(G)$  is a subgroup of  $G'$ . If  $H'$  is a subgroup of  $G'$ , then  $\phi^{-1}(H')$  is a subgroup of  $G$ .

**Definition.** (11.49) Let  $\phi : G \rightarrow H$  be a group homomorphism. Then the kernel of  $\phi$ , denoted by  $\ker \phi$ , is the subgroup of  $\phi^{-1}(\{1\})$ .

**Remark.** If  $\phi : R \rightarrow S$  is a ring homomorphism, then

$$\ker(\phi : (R, +, \cdot) \rightarrow (S, +, \cdot)) = \ker(\phi : (R, +) \rightarrow (S, +))$$

**Example.** (11.14, 11.15, 11.16)

(i) A singleton set is a group

(ii) If  $(R, +, \cdot)$  is a ring, then  $(R, +)$  is an abelian group

- (iii) If  $V$  is a vector space, then  $(V, +)$  is an abelian group
- (iv) If  $R$  is a ring, then the set  $R^\times$  of units in  $R$  is a group under multiplication. In particular,  $GL_n(\mathbf{R}) = (M_{n \times n}(\mathbf{R}))^\times$  is a group with matrix multiplication
- (v) The set of  $2 \times 2$  real matrices whose determinants are 1 forms a subgroup of  $GL_2(\mathbf{R})$

$$SL_2(\mathbf{R})$$

## Lecture 25 (June 10th)

Last time, we went over some properties of groups. Today, we learn about the symmetric group  $S_n$ , normal subgroups  $H \triangleleft G$ , and cyclic groups. Next time, we will learn about the classification of finite abelian groups.

**Example.** (i) The general linear group over  $\mathbf{R}$

$$GL_n(\mathbf{R}) = \{M \in M_{n \times n}(\mathbf{R}) \mid \det M \neq 0\}$$

(ii) The special linear group over  $\mathbf{R}$

$$SL_2(\mathbf{R}) = \{M \in M_{2 \times 2}(\mathbf{R}) \mid \det M = 1\}$$

(iii) The symmetric group

$$S_n = (\sigma, \circ)$$

where  $\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$  is a bijection.

**Definition.** (11.32) (Dihedral group  $D_{2n}$ )

**Definition.** (11.41) For each  $r \geq 2$ , an  $r$ -cycle  $(a_1, a_2, \dots, a_r)$  is a permutation cyclically permuting  $r$  elements,  $a_1$  through  $a_r$ . That is,

$$\begin{cases} a_i \mapsto a_{i+1} & 1 \leq i \leq r-1 \\ a_r \mapsto a_1 & i = r \end{cases}$$

A transposition, meanwhile, is a 2-cycle. Observe how  $(123) = (13)(12)$ .

**Lemma.** (11.45)

$$(a_1 \dots a_r) = (a_1 a_r)(a_1 a_{r-1}) \dots (a_1 a_2)$$

**Remark.** Two cycles are disjoint if their nontrivial orbits are disjoint.

**Proposition.** (11.44) Every nontrivial permutation can be written as product of disjoint nontrivial cycles.

**Theorem.** Every permutation can be written as a product of transpositions. Furthermore, the parity of the number of transpositions in each decomposition is the same.

**Example.** There is no unique decomposition of a permutation.

$$\begin{aligned}\sigma &= (123)(67) \\ &= (13)(12)(67) \\ &= (13)(12)(67)(52)(52)\end{aligned}$$

**Definition.** The sign of a permutation is defined as

$$\text{sgn}(\sigma) = \begin{cases} 1 & \text{if even} \\ -1 & \text{if odd} \end{cases}$$

as in the number of transpositions that construct  $\sigma$ . We will call  $\sigma$  even if  $\text{sgn}(\sigma) = 1$  and odd if  $\text{sgn}(\sigma) = -1$ . This is called the permutation's parity.

## Chapter 11.4

**Definition.** We can define an equivalence relation on  $G$  by saying, for a subgroup  $H$ ,

$$a \sim b \iff a^{-1}b \in H$$

The following set is called a left coset

$$aH = \{ah \mid h \in H\} = \bar{a}$$

The set of equivalence classes can be denoted

$$G/H = \{aH \mid a \in G\} = \{\bar{a} \mid a \in G\}$$

We notice that the definition of an ideal of a ring is exactly the definition of a coset where the ring addition is identified as the group operation.

**Definition.** (11.52) We will say that  $H$  is a normal subgroup if  $aH = Ha$  for all  $a \in G$ .

**Remark.** (11.53)  $H$  is a normal in  $G$  if and only if  $aHa^{-1} \subset H$  for all  $a \in G$ .