

# Aluffi Problems

Hui Sun

August 11, 2025

# Contents

<b>1</b>	<b>Category Theory</b>	<b>3</b>
<b>2</b>	<b>Groups I</b>	<b>4</b>
<b>3</b>	<b>Rings and Modules</b>	<b>8</b>
<b>4</b>	<b>Groups II</b>	<b>14</b>
4.1	Class Formula . . . . .	14
4.2	Sylow . . . . .	17
4.3	Commutator subgroup and Solvability . . . . .	20
4.4	$S_n$ and $A_n$ . . . . .	21
4.5	Semidirect Products . . . . .	23
4.6	Classification of Finite Abelian Group . . . . .	25
<b>5</b>	<b>Ring Theory II, Irreducibility of Polynomials</b>	<b>27</b>
5.1	factorizations . . . . .	27
5.2	UFD, PID, ED . . . . .	28
5.3	. . . . .	29
5.4	. . . . .	30
5.5	Irreducibility . . . . .	30
5.6	CRT . . . . .	32
<b>6</b>	<b>Linear Algebra I</b>	<b>33</b>
6.1	Basis . . . . .	33
6.2	Nakayama's Lemma . . . . .	34
6.3	Invariants . . . . .	35
6.4	Classification of Finitely Generated Modules over PID . . . . .	37
<b>7</b>	<b>Fields</b>	<b>38</b>
<b>8</b>	<b>Linear Algebra II</b>	<b>39</b>

## **Chapter 1**

# **Category Theory**

# Chapter 2

## Groups I

**Problem 2.1 (1.8).** Let  $G$  be a finite abelian group with exactly one element  $f$  of order 2. Prove that  $\prod_{g \in G} g = f$ .

*Proof.* It suffices to see that  $\prod_g g^2 = e$ , which is true by every element has an inverse. □

**Problem 2.2 (1.13).** Give an example showing that  $|gh|$  is not necessarily equal to  $\text{lcm}(|g|, |h|)$ , even if  $g$  and  $h$  commute.

*Proof.* Let  $g = h = 1 \in \mathbb{Z}/2\mathbb{Z}$ . □

**Problem 2.3 (1.14).** If  $g$  and  $h$  commute and  $\gcd(|g|, |h|) = 1$ , then  $|gh| = |g||h|$ . (Hint: Let  $N = |gh|$ ; then  $g^N = (h^{-1})^N$ . What can you say about this element?)

*Proof.* We know that  $g^N = (h^{-1})^N = e$ . □

**Problem 2.4 (6.7).** If  $\text{Aut}(G)$  is cyclic, then  $G$  is abelian.

*Proof.* This implies  $\text{Inn}(G)$  is cyclic, which is iff  $\text{Inn}(G)$  is trivial, iff  $G$  is abelian. □

**Problem 2.5 (6.9).** Prove that every finitely generated subgroup of  $\mathbb{Q}$  is cyclic. Prove that  $\mathbb{Q}$  is not finitely generated.

*Proof.* Suppose we just have  $H = \langle \frac{p_1}{q_1}, \frac{p_2}{q_2} \rangle$ , find  $\text{lcm}(q_1, q_2) = q$ , then

$$H = \left\langle \frac{a_1}{q}, \frac{a_2}{q} \right\rangle$$

find  $\gcd(a_1, a_2) = p$ , we claim that

$$H = \left\langle \frac{p}{q} \right\rangle$$

If  $\mathbb{Q}$  were to be finitely generated, then it is cyclic,  $\mathbb{Q} = \langle \frac{p}{q} \rangle$ , then try  $(p+1)/q$ . □

**Problem 2.6 (8.1).** If a group  $H$  may be realized as a subgroup of two groups  $G_1$  and  $G_2$  and if

$$\frac{G_1}{H} \cong \frac{G_2}{H},$$

does it follow that  $G_1 \cong G_2$ ? Give a counterexample.

*Proof.* Let  $G_1 = S_3$ ,  $G_2 = \mathbb{Z}/6\mathbb{Z}$ , and  $H = \mathbb{Z}/3\mathbb{Z}$ . □

**Problem 2.7 (8.2).** Suppose  $G$  is a group and  $H \subseteq G$  is a subgroup of index 2, that is, such that there are precisely two cosets of  $H$  in  $G$ . Prove that  $H$  is normal in  $G$ .

*Proof.* For any  $g \notin H$ , we have

$$G = H \sqcup gH = H \sqcup Hg$$

Thus  $gH = Hg$ . □

**Problem 2.8 (8.13).** Let  $G$  be a finite group, and assume  $|G|$  is odd. Prove that every element of  $G$  is a square.

*Proof.* Consider the set function  $\varphi : g \mapsto g^2$ , this function is injective hence surjective. □

**Problem 2.9 (8.18).** Let  $G$  be an abelian group of order  $2n$ , where  $n$  is odd. Prove that  $G$  has exactly one element of order 2. (It has at least one, for example by Exercise [8.17]. Use Lagrange's theorem to establish that it cannot have more than one.) Does the same conclusion hold if  $G$  is not necessarily commutative?

*Proof.* There exists one element  $g$  of order 2, then take its quotient  $G/\langle g \rangle$ . □

**Problem 2.10 (9.11).** Let  $G$  be a finite group, and  $H$  be subgroup of index  $p$ , where  $p$  is the smallest prime dividing  $|G|$ , then  $H$  is normal in  $G$ .

*Proof.* (I will abuse the notation  $\left| \frac{G}{H} \right| = [G : H]$ ). Let  $G$  act on the cosets  $G/H$  by left multiplication, this action  $\sigma : G \rightarrow \text{Aut}(G/H)$  is not trivial, hence

$$\left| \frac{G}{\ker(\sigma)} \right| \text{ divides } p!$$

Moreover, we notice that  $\ker(\sigma) \subset H$ , hence  $p$  divides  $\left| \frac{G}{\ker(\sigma)} \right|$ . Now we recall that  $p$  is the smallest prime dividing  $|G|$ , we must have  $\left| \frac{G}{\ker(\sigma)} \right| = p$ , hence  $H = \ker(\sigma)$ . □

**Proposition 2.1 (1.12).** There exists elements  $g, h \in G$ , such that  $|g|, |h| < \infty$ , but  $|gh| = \infty$ .

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

**Proposition 2.2 (1.15).** Let  $G$  be a commutative group, and let  $g \in G$  be an element of maximal finite order, that is, such that if  $h \in G$  has finite order, then  $|h| \leq |g|$ . Then, if  $h$  has finite order in  $G$ , then  $|h|$  divides  $|g|$ .

**Proposition 2.3.** When  $n$  is odd, the center of  $D_{2n}$  is trivial, when  $n$  is even, the center consists of  $\{e, r^{\frac{n}{2}}\}$ .

$$r^{\frac{n}{2}}s = sr^{-\frac{n}{2}} = sr^{\frac{n}{2}}$$

**Proposition 2.4 (4.8).** The map  $g \mapsto (r_g : a \mapsto gag^{-1})$  defines a homomorphism from  $G \rightarrow \text{Aut}(G)$ .

**Proposition 2.5 (4.9).** Let  $m, n$  be positive integers such that  $\gcd(m, n) = 1$ , then

$$\frac{\mathbb{Z}}{mn\mathbb{Z}} \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$$

**Proposition 2.6 (4.14).** The order of the group of automorphisms of  $\mathbb{Z}/n\mathbb{Z}$  is the the number of generators of  $\mathbb{Z}/\mathbb{Z}$ , i.e.,

$$|\text{Aut}(\mathbb{Z}/n\mathbb{Z})| = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

**Proposition 2.7 (4.15).** Let  $p$  be a prime, then

$$\text{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$$

**Proposition 2.8 (6.3).** Every matrix in  $\text{SU}(2)$  may be written in the form

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} = \begin{pmatrix} \gamma & \omega \\ -\bar{\omega} & \bar{\gamma} \end{pmatrix},$$

where  $a, b, c, d \in \mathbb{R}$  and  $a^2 + b^2 + c^2 + d^2 = 1$ .

**Proposition 2.9 (6.10).** The set of  $2 \times 2$  matrices with integer entries and determinant 1 is denoted  $\text{SL}_2(\mathbb{Z})$ :

$$\text{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ such that } a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

Note that  $\text{SL}_2(\mathbb{Z})$  is generated by the matrices

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

**Proposition 2.10 (7.7).** Let  $G$  be a group and  $n$  a positive integer, let  $H \subset G$  be the subgroup generated by all elements of order  $n$  in  $G$ , then  $H$  is normal.

**Proposition 2.11 (7.14).**  $\text{Inn}(G)$  is a normal subgroup of  $\text{Aut}(G)$ .

**Proposition 2.12 (8.4).** The dihedral group  $D_{2n}$  can also be represented as

$$\langle a, b : a^2 = b^2 = (ab)^n = e \rangle$$

( $a, b$  are two reflections, take  $a = s, b = rs$ ).

**Proposition 2.13 (8.8).**  $\mathrm{SL}_n(\mathbb{R})$  is a normal subgroup of  $\mathrm{GL}_n(\mathbb{R})$ , and

$$\frac{\mathrm{GL}_n(\mathbb{R})}{\mathrm{SL}_n(\mathbb{R})} = (\mathbb{R}^\times, \cdot)$$

as groups.

## Chapter 3

# Rings and Modules

**Problem 3.1 (1.12).** Just as complex numbers may be viewed as combinations  $a + bi$ , where  $a, b \in \mathbb{R}$  and  $i$  satisfies the relation  $i^2 = -1$  (and commutes with  $\mathbb{R}$ ), we may construct a ring  $\mathbb{H}$  by considering linear combinations  $a + bi + cj + dk$  where  $a, b, c, d \in \mathbb{R}$  and  $i, j, k$  commute with  $\mathbb{R}$  and satisfy the following relations:

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Addition in  $\mathbb{H}$  is defined componentwise, while multiplication is defined by imposing distributivity and applying the relations. For example,

$$(1 + i + j) \cdot (2 + k) = 1 \cdot 2 + i \cdot 2 + j \cdot 2 + 1 \cdot k + i \cdot k + j \cdot k = 2 + 2i + 2j + k - j + i = 2 + 3i + j + k.$$

1. Verify that this prescription does indeed define a ring.
2. Compute  $(a + bi + cj + dk)(a - bi - cj - dk)$ , where  $a, b, c, d \in \mathbb{R}$ .
3. Prove that  $\mathbb{H}$  is a division ring.
4. List all subgroups of  $Q_8 := \{\pm 1, \pm i, \pm j, \pm k\}$ , and prove that they are all normal.
5. Prove that  $Q_8$  and  $D_8$  are not isomorphic.
6. Prove that  $Q_8$  admits the presentation  $\langle x, y \mid x^2y^{-2}, y^4, xyx^{-1}y \rangle$ .

Elements of  $\mathbb{H}$  are called *quaternions*. Note that  $Q_8$  forms a subgroup of the group of units of  $\mathbb{H}$ ; it is a noncommutative group of order 8, called the *quaternionic group*.

*Proof.* 1. :)

2.  $a^2 + b^2 + c^2 + d^2$ .
3. follows from 2.
4.  $\{\pm 1\}, \{\pm 1, \pm i\}, \{\pm 1, \pm j\}, \{\pm 1, \pm k\}$
5. Number of order 4 elements: 2 in  $D_8$  and 6 in  $Q_8$ .
6. Take  $x = i, y = j$ , then

$$Q_8 = \{1, i, i^2, i^3, j, ij, i^2j, i^3j\}$$

□



**Problem 3.2 (1.15).** Prove that  $R[x]$  is an integral domain if and only if  $R$  is an integral domain.

*Proof.* For sufficiency: observe that if  $f, g \neq 0 \in R[x]$ , then  $fg \neq 0$ . □

**Problem 3.3 (1.16).** Let  $R$  be a ring, and consider the ring of power series  $R[[x]]$  (cf. {1.3}).

1. Prove that a power series  $a_0 + a_1x + a_2x^2 + \cdots$  is a unit in  $R[[x]]$  if and only if  $a_0$  is a unit in  $R$ . What is the inverse of  $1 - x$  in  $R[[x]]$ ?
2. Prove that  $R[[x]]$  is an integral domain if and only if  $R$  is.

*Proof.* 1. For sufficiency: you do it term by term; the inverse of  $(1 - x)$  is  $1 + x + x^2 + \cdots = \sum_{i=0}^{\infty} x^i$ . □

**Problem 3.4 (2.11).** Prove (by hand) that division ring  $R$  of  $p^2$  elements where  $p$  is prime, is commutative.

*Proof.* Assume not commutative, then the center of  $R$  must contain  $p$  elements. Let  $r \in R$  such that  $r$  is not in the center, then the centralizer of  $r$  must be the entire ring  $R$ , and this holds for all such  $r$ . □

**Problem 3.5 (2.16).** Prove that there is (up to isomorphism) only one structure of ring with identity on the abelian group  $(\mathbb{Z}, +)$ . (Hint: Let  $R$  be a ring whose underlying group is  $\mathbb{Z}$ . By Proposition [2.7] there is an injective ring homomorphism  $\lambda : R \rightarrow \text{End}_{\text{Ab}}(R)$ , and the latter is isomorphic to  $\mathbb{Z}$ . Prove that  $\lambda$  is surjective.)

*Proof.* There exists an injective map

$$\lambda : R \rightarrow \mathbb{Z}$$

note that this map is also surjective. □

**Problem 3.6 (2.17).** Let  $R$  be a ring, and let  $E = \text{End}_{\text{Ab}}(R)$  be the ring of endomorphisms of the underlying abelian group  $(R, +)$ . Prove that the center of  $E$  is isomorphic to a subring of the center of  $R$ . (Prove that if  $\alpha \in E$  commutes with all right-multiplications by elements of  $R$ , then  $\alpha$  is left-multiplication by an element of  $R$ ; then use Proposition [2.7])

*Proof.* If  $\alpha$  commutes with all the right multiplications  $r_x$ , then

$$\alpha r_x(s) = \alpha(sx) = \alpha(s)x$$

letting  $s = 1$ , we see

$$\alpha(x) = \alpha(1)x$$

Thus  $\alpha$  is a left multiplication. Let  $\varphi : \alpha \mapsto \alpha(1)$ , this is injective, surjective onto its image. □

**Problem 3.7 (3.4).** Let  $R$  be a ring such that every subgroup of  $(R, +)$  is in fact an ideal of  $R$ . Prove that  $R \cong \mathbb{Z}/n\mathbb{Z}$ , where  $n$  is the characteristic of  $R$ .

*Proof.* It suffices to exhibit a surjective map from  $\mathbb{Z}$  to  $R$ , consider the subgroup  $\varphi(\mathbb{Z})$ , where  $\varphi : 1 \mapsto 1$ . We know that  $\varphi(\mathbb{Z})$  is an ideal, i.e., for every  $r \in R$ ,

$$r \cdot 1 \in \varphi(\mathbb{Z})$$

since  $1 \in \varphi(\mathbb{Z})$ , thus this map is surjective. □

**Problem 3.8 (4.5).** Let  $I, J$  be ideals in a commutative ring  $R$ , such that  $I+J = (1)$ . Prove that  $IJ = I \cap J$ .

*Proof.* We know  $IJ \subset I \cap J$ , now let  $r \in I \cap J$ , then

$$r \cdot 1 = r(i + j) = ri + rj \in IJ$$

□

**Problem 3.9 (4.6).** Let  $I, J$  be ideals in a commutative ring  $R$ . Assume that  $R/(IJ)$  is reduced (that is, it has no nonzero nilpotent elements). Prove that  $IJ = I \cap J$ .

*Proof.* Consider nonzero  $r \in I \cap J$ , then  $r^2 \in IJ$ , hence in  $R/IJ$ ,  $r = 0 + IJ$ , i.e.,  $r \in IJ$ . □

**Problem 3.10 (4.11).** Let  $R$  be a commutative ring,  $a \in R$ , and  $f_1(x), \dots, f_r(x) \in R[x]$ .

- Prove the equality of ideals

$$(f_1(x), \dots, f_r(x), x - a) = (f_1(a), \dots, f_r(a), x - a).$$

- Note the useful substitution trick

$$\frac{R[x]}{(f_1(x), \dots, f_r(x), x - a)} \cong \frac{R}{(f_1(a), \dots, f_r(a))}.$$

*Proof.* Use long division:  $f_1(x) = q(x)(x - a) + f_1(a)$ . □

**Problem 3.11 (4.17).** Let  $K$  be a compact topological space, and let  $R$  be the ring of continuous real-valued functions on  $K$ , with addition and multiplication defined pointwise.

- For  $p \in K$ , let  $M_p = \{f \in R \mid f(p) = 0\}$ . Prove that  $M_p$  is a maximal ideal in  $R$ .
- Prove that if  $f_1, \dots, f_r \in R$  have no common zeros, then  $(f_1, \dots, f_r) = (1)$ . (Hint: Consider  $f_1^2 + \dots + f_r^2$ .)
- Prove that every maximal ideal  $M$  in  $R$  is of the form  $M_p$  for some  $p \in K$ . (Hint: You will use the compactness of  $K$  and (ii).)

*Proof.* (i) Note that  $\frac{R}{M_p} \cong \mathbb{R}$ , given by evaluation at  $p$ .

(ii) Note that  $g(p) = f_1^2 + \cdots + f_r^2(p) > 0$  for all  $p \in K$ , thus one can construct an inverse. Namely,

$$1 = h(f_1^2 + \cdots + f_r^2)$$

where  $h = \frac{1}{g}$ .

(iii) Let  $M$  be a maximal ideal, suppose  $M$  is not contained in  $M_p$  for any  $p$ . This implies that there exists  $f \in M$  such that  $f(p) \neq 0$  for every  $p \in K$ . Then we consider the set

$$\{f^{-1}(\mathbb{R} \setminus \{0\}) : f \in M\}$$

This is an open cover of  $K$ , hence there exists  $f_1, \dots, f_r$  such that

$$\{f_i(\mathbb{R} \setminus \{0\}) : 1 \leq i \leq r\}$$

is also a cover of  $K$ . We know that  $f_1, \dots, f_r$  have no common roots, thus

$$(f_1, \dots, f_r) = R$$

which is a contradiction. □

**Problem 3.12 (4.23).** A ring  $R$  has Krull dimension 0 if every prime ideal in  $R$  is maximal. Prove that fields and Boolean rings have Krull dimension 0.

*Proof.* Let  $p$  be a prime ideal of a Boolean ring, then  $R/p \cong \mathbb{Z}/2\mathbb{Z}$ , which is a field, hence  $p$  is also a maximal ideal. □

**Problem 3.13 (6.3).** Let  $R$  be a ring,  $M$  an  $R$ -module, and  $p : M \rightarrow M$  an  $R$ -module homomorphism such that  $p^2 = p$ . (Such a map is called a projection.) Prove that  $M \cong \ker p \oplus \operatorname{im} p$ .

*Proof.* Let  $m \in M$ , then  $m = (m - p(m)) + p(m)$ . □

**Problem 3.14 (6.6).** Let  $R$  be a ring, and let  $F = R^{\oplus n}$  be a finitely generated free  $R$ -module. Prove that  $\operatorname{Hom}_{R\text{-Mod}}(F, R) \cong F$ . On the other hand, find an example of a ring  $R$  and a nonzero  $R$ -module  $M$  such that  $\operatorname{Hom}_{R\text{-Mod}}(M, R) = 0$ .

*Proof.* Define the map  $F \rightarrow \operatorname{Hom}(F, R)$  as

$$(r_1, \dots, r_n) \mapsto \left( \varphi : (a_1, \dots, a_n) \mapsto \sum_{i=1}^n a_i r_i \right)$$

Take  $M = \mathbb{Z}/2\mathbb{Z}$ ,  $R = \mathbb{Z}$  in the second question. □

**Problem 3.15 (6.16).** Let  $R$  be a ring. A (left-)  $R$ -module  $M$  is *cyclic* if  $M = \langle m \rangle$  for some  $m \in M$ .

(i) Prove that simple modules are cyclic.

(ii) Prove that an  $R$ -module  $M$  is cyclic if and only if  $M \cong R/I$  for some (left-)ideal  $I$ .

(iii) Prove that every quotient of a cyclic module is cyclic.

*Proof.* (i) Take any nonzero  $r \in R$ , then  $M = \langle r \rangle$ .

(ii) For the forward direction,  $M = \langle m \rangle$ , consider the map  $\varphi : m \mapsto 1$ ; for the backwards,  $1+I$  is a generator of  $R/I$ , where  $R/I$  viewed as a  $R$ -module.

(iii) Follows from (ii) and the second isomorphism theorem. □

**Problem 3.16 (6.18).** Let  $M$  be an  $R$ -module, and let  $N$  be a submodule of  $M$ . Prove that if  $N$  and  $M/N$  are both finitely generated, then  $M$  is finitely generated.

*Proof.* Suppose  $N = \langle r_1, \dots, r_k \rangle$ ,  $M/N = \langle r_{k+1} + N, \dots, r_{k+m} + N \rangle$ , then we claim  $M = \langle r_1, \dots, r_{k+m} \rangle$ . If  $m \in M$  is such that  $m \in N$ , then done; if  $m \notin N$ , then  $m \in r_i + N$  for some  $i$ , then

$$m = \sum a_i r_i \Rightarrow m - \sum a_i r_i \in N$$

thus again writing it as a finite sum, we are done. □

**Proposition 3.1 (2.8).** Every subring of a field is an integral domain.

**Proposition 3.2 (2.9).** The center of a division ring is a field.

**Proposition 3.3 (3.9).** A nonzero ring with ideals being only  $\{0\}$  and  $R$  are called simple rings. The only simple commutative rings are fields. Moreover,  $M_n(\mathbb{R})$  is also simple.

**Proposition 3.4 (3.14).** The characteristic of an integral domain is either 0 or a prime ideal  $p$ .

**Proposition 3.5 (4.4).** If  $k$  is a field, then  $k[x]$  is a PID.

**Proposition 3.6 (4.9).** Let  $R$  be a commutative ring, and let  $f(x)$  be a zero-divisor in  $R[x]$ . There exists  $\exists b \in R, b \neq 0$ , such that  $f(x)b = 0$ . (Let  $fg = 0$ , where  $g = b_e x^e + \dots + b_0$ , set  $b = b_e$ .)

**Proposition 3.7 (4.10).** Let  $d$  be an integer that is not the square of an integer, and consider the subset of  $\mathbb{C}$  defined by

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

Then  $\mathbb{Q}(\sqrt{d})$  is a field, and

$$\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[t]/(t^2 - d)$$

**Proposition 3.8 (4.19).** Let  $R$  be a commutative ring, let  $P$  be a prime ideal in  $R$ , and let  $I_j$  be ideals of  $R$ .

(i) Assume that  $I_1 \cdots I_r \subseteq P$ , then that  $I_j \subseteq P$  for some  $j$ .

(ii) By (i), if  $P \supseteq \bigcap_{j=1}^r I_j$ , then  $P$  contains one of the ideals  $I_j$ . The following is not true:  $P \supseteq \bigcap_{j=1}^{\infty} I_j$ , then  $P$  contains one of the ideals  $I_j$ . Consider  $I_j = (p_j)$  then  $\bigcap I_j = 0$ .

**Proposition 3.9 (4.20).** Let  $M$  be a two-sided ideal in a (not necessarily commutative) ring  $R$ . Then  $M$  is maximal if and only if  $R/M$  is a simple ring.

**Proposition 3.10 (4.21).** Let  $k$  be an algebraically closed field, and let  $I \subseteq k[x]$  be an ideal. Then  $I$  is maximal if and only if  $I = (x - c)$  for some  $c \in k$ .

**Proposition 3.11 (4.22).**  $(x^2 + 1)$  is maximal in  $\mathbb{R}[x]$ .

**Proposition 3.12 (5.4).** Let  $R$  be a ring. A nonzero  $R$ -module  $M$  is *simple* (or *irreducible*) if its only submodules are  $\{0\}$  and  $M$ . Let  $M, N$  be simple modules, and let  $\varphi : M \rightarrow N$  be a homomorphism of  $R$ -modules. Prove that either  $\varphi = 0$  or  $\varphi$  is an isomorphism. (This rather innocent statement is known as Schur's lemma.)

**Proposition 3.13 (5.5).** Let  $R$  be commutative, viewed as  $R$ -module over itself, let  $M$  be an  $R$ -module, then

$$\text{Hom}(R, M) \cong M$$

as  $R$ -modules.

**Proposition 3.14 (5.13).** Let  $R$  be an integral domain, let  $I$  be a nonzero principal ideal, then  $I$  is isomorphic to  $R$  as an  $R$ -module.

**Proposition 3.15 (5.16).** Let  $R$  be commutative,  $a \in R$  be nilpotent, consider the submodule  $aM$  of  $M$ . Then

$$M = 0 \iff aM = M$$

*Proof.* Multiplication by  $a$  is a surjective map, composition of surjective maps is still surjective.  $\square$

**Proposition 3.16 (6.16).** Let  $M$  be an  $R$ -module, it is cyclic if  $M = \langle m \rangle$ , then  $M$  is cyclic if and only if  $M \cong R/I$  for some ideal  $I$ .

**Proposition 3.17 (6.18).** Let  $M$  be an  $R$ -module, and let  $N$  be a submodule of  $M$ . Prove that if  $N$  and  $M/N$  are both finitely generated, then  $M$  is finitely generated.

# Chapter 4

## Groups II

### 4.1 Class Formula

**Problem 4.1.** Let  $p$  be a prime integer, let  $G$  be a  $p$ -group, and let  $S$  be a set such that  $|S| \not\equiv 0 \pmod{p}$ . If  $G$  acts on  $S$ , prove that the action must have fixed points.

*Proof.* The class formula  $|S| = |Z| + \sum_a [G : \text{Stab}(a)]$ . □

**Problem 4.2.** Find the center of  $D_{2n}$  using the size of conjugacy class.

*Proof.* For  $n$  odd, it suffices to show that there is only the identity that is its own conjugacy class. In other words, for any  $r, s$ , show that there are more things in their conjugacy class:

$$rsr^{-1} = sr^{-2} = s \iff r^{-2} = e$$

and there is no such  $r$ .

$$srs^{-1} = r^{-1}$$

again there is no element such that  $r = r^{-1}$ , hence the conjugacy class of  $r$  contains at least one other element  $r^{-1}$ . □

**Problem 4.3.** Prove that the center of  $S_n$  is trivial for  $n \geq 3$ . (Suppose that  $\sigma \in S_n$  sends  $a$  to  $b \neq a$ , and let  $c \neq a, b$ . Let  $\tau$  be the permutation that acts solely by swapping  $b$  and  $c$ . Then compare the action of  $\sigma\tau$  and  $\tau\sigma$  on  $a$ .)

*Proof.* You just do it and see  $\sigma\tau \neq \tau\sigma$ . □

**Proposition 4.1.** The center of  $S_n$  is trivial for all  $n \geq 3$ .

**Proposition 4.2.** Let  $G$  be a group, and let  $N$  be a subgroup of  $Z(G)$ . Prove that  $N$  is normal in  $G$ , note  $Z(G)$  is normal in  $G$ .

**Proposition 4.3.** Let  $G$  be a group, then

$$\frac{G}{Z(G)} \cong \text{Inn}(G)$$

Recall  $\text{Inn}(G)$  is cyclic iff  $G$  is commutative, this shows if  $G/Z(G)$  is cyclic, then  $G$  is commutative.

**Proposition 4.4.** Let  $p, q$  be prime integers, and let  $G$  be a group of order  $pq$ . Prove that either  $G$  is commutative or the center of  $G$  is trivial.

**Problem 4.4.** Prove or disprove that if  $p$  is prime, then every group of order  $p^3$  is commutative.

*Proof.* Consider the Heisenberg group over  $\mathbb{F}_p$ :

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{F}_p \right\},$$

which has order  $p^3$  and noncommutative. □

**Proposition 4.5.** Let  $G$  be a  $p$ -group,  $|G| = p^r$ , then there exists a normal subgroup of size  $p^k$  for every  $k \leq r$ .

**Problem 4.5.** Let  $p$  be a prime number, and let  $G$  be a  $p$ -group:  $|G| = p^r$ . Prove that  $G$  contains a normal subgroup of order  $p^k$  for every nonnegative  $k \leq r$ .

*Proof.* First the center is nontrivial and is normal, then we take the quotient  $G/\langle z \rangle$ , where  $z$  is an order  $p$  element in the center. Do the same and lift it to a normal subgroup of  $G$ . □

**Problem 4.6.** Let  $p$  be a prime number,  $G$  a  $p$ -group, and  $H$  a nontrivial normal subgroup of  $G$ . Prove that  $H \cap Z(G) \neq \{e\}$ .

*Proof.* Consider the action of  $G$  on  $H$  by conjugation:

$$|H| = |Z(G) \cap H| + \sum_h |[h]|$$

Hence

$$|Z(G) \cap H| \equiv 0 \pmod{p}$$

thus is nontrivial. □

**Proposition 4.6.** Let  $G$  be a  $p$ -group, and  $H$  be a nontrivial normal subgroup, then

$$H \cap Z(G) \neq \{e\}$$

In other words, there are nontrivial elements in  $H$  that commutes with every  $g \in G$ .

**Proposition 4.7.** The class formula for both  $D_8$  and  $Q_8$  is  $8 = 2 + 2 + 2 + 2$ . (Also note that  $D_8 \not\cong Q_8$ .)

**Problem 4.7 (1.13).** Let  $G$  be a noncommutative group of order 6. Then,  $G$  must have trivial center and exactly two conjugacy classes, of order 2 and 3.

- Prove that if every element of a group has order  $\leq 2$ , then the group is commutative. Conclude that  $G$  has an element  $y$  of order 3.
- Prove that  $\langle y \rangle$  is normal in  $G$ .
- Prove that  $[y]$  is the conjugacy class of order 2 and  $[y] = \{y, y^2\}$ .
- Prove that there is an  $x \in G$  such that  $yx = xy^2$ .

*Proof.* • Compute  $(ab)^2$ .

- It has index 2.
- Note that the centralizer  $C_G(y)$  has order dividing  $G$ , not all  $G$  ( $G$  is nonabelian), and contains  $\langle y \rangle$ , thus must be 3, hence  $[y]$  has order 2. □

**Problem 4.8 (1.14).** Let  $G$  be a group, and assume  $[G : Z(G)] = n$  is finite. Let  $A \subseteq G$  be any subset. Prove that the number of conjugates of  $A$  is at most  $n$ .

*Proof.* The number of conjugates of  $A$  is  $[G : N_G(A)]$ , and  $Z(G) \subset N_G(A)$ . □

**Problem 4.9.** Suppose that the class formula for a group  $G$  is  $60 = 1 + 15 + 20 + 12 + 12$ . Prove that the only normal subgroups of  $G$  are  $\{e\}$  and  $G$ .

*Proof.* Use the fact that normal subgroups divide  $|G|$  and are unions of conjugacy classes. □

**Proposition 4.8.** Let  $G$  be a finite group, and let  $H \subseteq G$  be a subgroup of index 2. For  $a \in H$ , denote by  $[a]_H$ , resp.,  $[a]_G$ , the conjugacy class of  $a$  in  $H$ , resp.,  $G$ . Then, either  $[a]_H = [a]_G$  or  $[a]_H$  is half the size of  $[a]_G$ , according to whether the centralizer  $Z_G(a)$  is not or is contained in  $H$ .

**Problem 4.10 (1.17).** Let  $H$  be a proper subgroup of a finite group  $G$ . Prove that  $G$  is not the union of the conjugates of  $H$ .

*Proof.* Suppose that  $G$  is a union of conjugates of  $H$ , then

$$\begin{aligned} |G| &= [G : H] \cdot |H| \\ &= [G : N_G(H)] \cdot [N_G(H) : H] \cdot |H| \\ &\leq [G : N_G(H)] \cdot |H| - 1 \end{aligned}$$

which is a contradiction. □



**Problem 4.11 (1.18).** Let  $S$  be a set endowed with a transitive action of a finite group  $G$ , and assume  $|S| \geq 2$ . Prove that there exists a  $g \in G$  without fixed points in  $S$ , that is, such that  $gs \neq s$  for all  $s \in S$ .

*Proof.* Follows from 1.17. □

**Problem 4.12 (1.19).** Let  $H$  be a proper subgroup of a finite group  $G$ . Prove that there exists a  $g \in G$  whose conjugacy class is disjoint from  $H$ .

*Proof.* Follows immediately from 1.17. □

**Proposition 4.9.** Let  $G = \text{GL}_2(\mathbb{C})$ , every  $2 \times 2$  matrix is conjugate to an upper triangular matrix.  
Warning: You need the fact that  $\mathbb{C}$  is algebraically closed. (Use Jordan canonical form).

**Problem 4.13 (1.21).** Let  $H, K$  be subgroups of a group  $G$ , with  $H \subseteq N_G(K)$ . Verify that the function  $\gamma : H \rightarrow \text{Aut}_{\text{Grp}}(K)$  defined by conjugation is a homomorphism of groups and that  $\ker \gamma = H \cap Z_G(K)$ , where  $Z_G(K)$  is the centralizer of  $K$ .

*Proof.*  $r_h(g) = hgh^{-1} = g$  for all  $g \in K$  implies that  $h \in Z_G(K)$ . □

**Problem 4.14 (1.22).** Let  $G$  be a finite group, and let  $H$  be a cyclic subgroup of  $G$  of order  $p$ . Assume that  $p$  is the smallest prime dividing the order of  $G$  and that  $H$  is normal in  $G$ . Prove that  $H$  is contained in the center of  $G$ . (Hint: By Exercise [1.21], there is a homomorphism  $\gamma : G \rightarrow \text{Aut}_{\text{Grp}}(H)$ ; by Exercise [II.4.14],  $\text{Aut}(H)$  has order  $p - 1$ . What can you say about  $\gamma$ ?)

*Proof.* To show  $H$  is contained in the center, it suffices to show that the centralizer  $Z_G(H) = G$ , by the previous exercise

$$\ker \gamma = G \cap Z_G(H)$$

It suffices to show that  $\ker \gamma = G$ . Suppose it is not the trivial map, then  $[G : \ker \gamma]$  divides both  $|G|$ , and  $(p - 1)$  because

$$\frac{G}{\ker \gamma} \cong \text{im}(\gamma) \subset \text{Aut}(H)$$

This contradicts with the fact that  $p$  is the smallest prime dividing  $|G|$ . □

## 4.2 Sylow

**Problem 4.15 (2.2).** Let  $G$  be a group. A subgroup  $H$  of  $G$  is characteristic if  $\varphi(H) \subseteq H$  for every automorphism  $\varphi$  of  $G$ .

- Prove that characteristic subgroups are normal.
- Let  $H \subseteq K \subseteq G$ , with  $H$  characteristic in  $K$  and  $K$  normal in  $G$ . Prove that  $H$  is normal in  $G$ .
- Let  $G, K$  be groups, and assume  $G$  contains a single subgroup  $H$  isomorphic to  $K$ . Prove that  $H$  is normal in  $G$ .

*Proof.* • conjugation is an automorphism.

- conjugation by  $g \in G$  on  $K$  is an automorphism, thus  $H$  is also preserved under conjugation by  $g$ .
- Let  $\varphi$  be any automorphism  $G \rightarrow G$ ,

$$\varphi(H) \cong H$$

since  $\varphi$  has trivial kernel, thus  $\varphi(H) = H$  by assumption, i.e.  $H$  is normal by taking  $\varphi$  as the conjugation action. □

**Proposition 4.10.** Let  $G$  be a nontrivial  $p$ -group, then  $G$  is not simple.

*Proof.* It has nontrivial center, and the center is normal. □

**Problem 4.16 (2.8).** Let  $G$  be a finite group,  $p$  a prime, and  $N$  the intersection of all  $p$ -Sylow subgroups of  $G$ . Prove:

- (1)  $N$  is a normal  $p$ -subgroup of  $G$ .
- (2) Every normal  $p$ -subgroup of  $G$  is contained in  $N$ .

*Proof.* (1) Let  $g \in G$ , then

$$gNg^{-1} = \bigcap_P gPg^{-1} = \bigcap_{P'} P' = N$$

where  $P, P'$  are  $p$ -Sylow subgroups.

- (2) Let  $N'$  be a normal  $p$ -subgroup, then  $N' \subset P$  for some  $p$ -Sylow subgroup of  $G$ , since  $N'$  is normal, we know

$$N' \subset \bigcap_{P'} P' = N$$

□

**Proposition 4.11.** Let  $P$  be a  $p$ -Sylow subgroup of  $G$ , and let  $P$  act by conjugation on the set of  $p$ -Sylow subgroups. Then  $P$  is the unique fixed point.

**Problem 4.17 (2.12).** Let  $P$  be a  $p$ -Sylow subgroup of  $G$ , and  $H \subseteq G$  a subgroup containing  $N_G(P)$ . Prove  $[G : H] \equiv 1 \pmod{p}$ .

*Proof.* We know

$$n_p = [G : N_G(P)] \equiv 1 \pmod{p}$$

Hence by

$$[G : N_G(P)] = [G : H] \cdot [H : N_G(P)]$$

it suffices to show that

$$[H : N_G(P)] \equiv 1 \pmod{p}$$

It suffices to see that

$$N_G(P) = \{g \in G : gPg^{-1} = P\} = N_H(P)$$

since  $H$  contains  $N_G(P)$ . □

**Problem 4.18 (2.15).** Classify all groups of order  $n \leq 15$  (except  $n = 8, 12$ ) up to isomorphism.

*Proof.* 1.  $n = 6$ :  $\mathbb{Z}/6\mathbb{Z}$  and  $S_3$ .

2.  $n = 8$ : abelian or  $D_8$  or  $Q_8$ .

3.  $n = 9$ : abelian.

4.  $n = 10$ : abelian or  $P_5 \rtimes P_2$ . The nontrivial action  $\mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong (\mathbb{Z}/5\mathbb{Z})^\times$  gives

$$G \cong \langle g, h : g^5 = h^2 = e, hgh^{-1} = g^4 \rangle$$



**Warning 4.1.** You know how to do this! The nontrivial action sends 1 to another order 2 element, which is 4, thus the automorphism is multiplication by 4, using the multiplicative notation, we have  $hgh^{-1} = g^4$ . (additive notation would have been  $h + g - h = 4g$ ).

5.  $n = 14$ .  $\mathbb{Z}/14\mathbb{Z}$  or  $D_{14}$ . (The nontrivial action inverts the elements of  $\mathbb{Z}/7\mathbb{Z}$ ).

□

**Problem 4.19 (2.19).** Let  $G$  be noncommutative of order  $pq$  ( $p < q$  primes).

- Show  $q \equiv 1 \pmod{p}$ .
- Prove  $Z(G)$  is trivial.
- Draw the subgroup lattice of  $G$ .
- Find the number of elements of each possible order.
- Find the number and size of the conjugacy classes in  $G$ .

*Proof.* • Consider  $n_q = 1$  or  $p$ , and  $n_q \equiv 1 \pmod{q}$ . This implies that  $n_q = 1$ . Let  $Q$  be the normal  $q$ -subgroup, and  $P$  be a  $p$ -Sylow subgroup, then consider the semidirect product

$$Q \rtimes P$$

For  $G$  to be noncommutative, this requires the map  $\theta : P \rightarrow \text{Aut}(Q)$  to be nontrivial, i.e.,  $p$  divides  $q - 1$ , i.e.

$$q \equiv 1 \pmod{p}$$

- If not trivial, then commutative.
- There are  $q$  subgroups of order  $p$ , and 1 subgroup of order  $q$ .
- Compute the size of the centralizer for an element  $g$  of order  $p$ : it is  $p$ , thus the conjugacy has order  $q$ .

□

**Problem 4.20 (2.21).** Let  $p < q < r$  be primes. Prove no group of order  $pqr$  is simple.

*Proof.* Suppose  $n_q, n_p, n_r \neq 1$ , then compute the smallest size allowed by Sylow theorems, this will exceed  $pqr$ . □

**Problem 4.21 (2.23).** For  $G$  simple,

- (1) Prove  $|G|$  divides  $N_p!$  for all primes  $p$  dividing  $|G|$ , where  $N_p$  is the number of  $p$ -Sylow subgroups.
- (2) If  $H \leq G$  has index  $N > 1$ , then  $|G|$  divides  $N!$ .

*Proof.* (1) The kernel  $\gamma : G \rightarrow \{P_1, \dots, P_{n_p}\}$  is trivial, hence  $|G|$  divides  $N_p!$ .

(2)  $G$  acts the cosets  $G/H$  transitively, thus same trivial kernel argument shows  $|G|$  divides  $N!$ . □

**Problem 4.22 (2.25).** Assume  $G$  is simple of order 60.

- Prove  $G$  has 5 or 15 Sylow 2-subgroups (15 elements of order 2 or 4).
- If 15 Sylow 2-subgroups, find  $g \in G$  of order 2 in two of them, and show  $C_G(g)$  has index 5.

*Proof.* •  $n_2 = 1, 3, 5, 15$ ,  $G$  simple and trivial kernel argument shows  $n_2 = 5, 15$ .

- The 2-Sylow subgroups must have overlap by a size argument; consider  $C_G(g)$ : we know that  $P_1, P_2 \subset C_G(g)$ , hence  $|C_G(g)| \geq 4$ , and  $|C_G(g)| \neq 60$  because that'd be nontrivial center, hence  $|C_G(g)| = 12$ , i.e., index 5. □

### 4.3 Commutator subgroup and Solvability

**Problem 4.23.**  $G$  is solvable iff  $N, G/N$  are solvable, where  $N$  is a normal subgroup of  $G$ .

**Problem 4.24 (3.10).** Let  $G$  be a group. Define inductively an increasing sequence  $Z_0 = \{e\} \subseteq Z_1 \subseteq Z_2 \subseteq \dots$  of subgroups of  $G$  as follows: for  $i \geq 1$ ,  $Z_i$  is the subgroup of  $G$  corresponding (as in Proposition II.8.9) to the center of  $G/Z_{i-1}$ .

- Prove that each  $Z_i$  is normal in  $G$ , so that this definition makes sense.

A group is *nilpotent* if  $Z_m = G$  for some  $m$ .

- Prove that  $G$  is nilpotent if and only if  $G/Z(G)$  is nilpotent.
- Prove that  $p$ -groups are nilpotent.
- Prove that nilpotent groups are solvable.
- Find a solvable group that is not nilpotent.

**Problem 4.25 (3.11).** Let  $H$  be a nontrivial normal subgroup of a nilpotent group  $G$  (cf. Exercise 3.10). Prove that  $H$  intersects  $Z(G)$  nontrivially. (Hint: Let  $r \geq 1$  be the smallest index such that  $\exists h \neq e, h \in H \cap Z_r$ . Contemplate a well-chosen commutator  $[g, h]$ .) Since  $p$ -groups are nilpotent, this strengthens the result of Exercise 1.9.

**Problem 4.26 (3.12).** Let  $H$  be a proper subgroup of a finite nilpotent group  $G$  (cf. Exercise 3.10). Prove that  $H \subset N_G(H)$ . (Hint:  $Z(G)$  is nontrivial. First dispose of the case in which  $H$  does not contain  $Z(G)$ , and then use induction to deal with the case in which  $H$  does contain  $Z(G)$ .) Deduce that every Sylow subgroup of a finite nilpotent group is normal.

**Problem 4.27 (3.15).** Let  $p, q$  be prime integers, and let  $G$  be a group of order  $p^2q$ . Prove that  $G$  is solvable. (This is a particular case of Burnside's theorem: for  $p, q$  primes, every group of order  $p^a q^b$  is solvable.)

*Proof.* Consider

$$\{e\} = G_0 \subset Q \subset G$$

where  $Q$  is the normal subgroup of order  $q$ , using Sylow theorems, one can show that  $n_q = 1$ .  $G/Q$  is abelian, so is  $Q$ .  $\square$

**Problem 4.28 (3.16).** Prove that every group of order  $< 60$  and  $\neq 60$  is solvable.

*Proof.* All  $p$ -groups,  $p^2q$  are solvable; moreover,  $G$  is solvable iff  $G/N, N$  are solvable, where  $N$  is a normal subgroup.  $\square$

## 4.4 $S_n$ and $A_n$

**Problem 4.29 (4.5).** Find the class formula for  $S_n$ , where  $n \leq 5$ .

*Proof.*

$$\begin{cases} S_3 = 1 + 2 + 3 \\ S_4 = 1 + 6 + 8 + 6 + 3 \\ S_5 = 1 + 24 + 30 + 20 + 15 + 10 + 20 \end{cases}$$

$\square$

**Problem 4.30 (4.7).**  $\triangleright$  Prove that  $S_n$  is generated by  $(12)$  and  $(12 \dots n)$ .

*Proof.* It suffices to generate all the transpositions: let  $\sigma = (12 \dots n)$ ,

$$\sigma(12)\sigma^{-1} = (\sigma(1)\sigma(2)) = (23)$$

thus this process allows us to get all the  $(n, n+1)$  adjacent swaps. Then we see that

$$(23)(12)(23)^{-1} = (13)$$

and we can generate all the transpositions like this.  $\square$

**Problem 4.31 (4.8).** For  $n > 1$ , prove that the subgroup  $H$  of  $S_n$  consisting of permutations fixing 1 is isomorphic to  $S_{n-1}$ . Prove that there are no proper subgroups of  $S_n$  properly containing  $H$ .

*Proof.* By a rearranging of indices, the first statement is true. Any subgroup properly containing  $H$  must contain  $\sigma$  such that  $\sigma(1) = i$ , and with transpositions in  $H$ , this generates  $S_n$ .  $\square$

**Proposition 4.12.** The subgroup  $H$  of  $S_n$ :

$$H = \{\sigma \in S_n : \sigma(1) = 1\}$$

is isomorphic to  $S_{n-1}$ .

**Proposition 4.13 (4.9).**  $(13)$  and  $(1234)$  generate a copy of  $D_8$  in  $S_4$ . Every subgroup of  $S_4$  of order 8 is conjugate to  $\langle (13), (1234) \rangle$ , and there are exactly 3 such subgroups. For all  $n \geq 3$ ,  $S_n$  contains a copy of the dihedral group  $D_{2n}$ .

**Proposition 4.14 (4.10).** 1. There are exactly  $(n-1)!$   $n$ -cycles in  $S_n$ .

2. More generally, the size of the conjugacy class of a permutation of given type in  $S_n$ :  $\sigma \in S_n$  with cycle type  $(1^{a_1}, 2^{a_2}, \dots, n^{a_n})$  (where  $a_k$  is the number of  $k$ -cycles), the size of its conjugacy class is:

$$\frac{n!}{\prod_{k=1}^n (k^{a_k} \cdot a_k!)}$$

**Problem 4.32 (4.11).** Let  $p$  be a prime integer. Compute the number of  $p$ -Sylow subgroups of  $S_p$ .

*Proof.* There are  $(p-1)!$   $p$ -cycles, and each  $p$ -Sylow subgroup contains  $(p-1)$  of these cycles, i.e., there are  $(p-2)!$   $p$ -Sylow subgroups. (This uses the fact that if  $N, H$  are subgroups of prime order  $p$ , then they either intersect trivially or are equal).  $\square$

**Problem 4.33 (4.12).** A subgroup  $G$  of  $S_n$  is *transitive* if the induced action of  $G$  on  $\{1, \dots, n\}$  is transitive.

1. Prove that if  $G \subseteq S_n$  is transitive, then  $|G|$  is a multiple of  $n$ .
2. Prove that the following subgroups of  $S_4$  are all transitive:
  - $\langle (1234) \rangle \cong C_4$  and its conjugates,
  - $\langle (12)(34), (13)(24) \rangle \cong C_2 \times C_2$ ,
  - $\langle (12)(34), (1234) \rangle \cong D_8$  and its conjugates,
  - $A_4$ , and  $S_4$ .

(These are the *only* transitive subgroups of  $S_4$ .)

*Proof.* 1.  $G$  acts on  $\{1, \dots, n\}$  transitively, thus the orbit of any  $i$ ,  $O(i) = \{1, \dots, i\}$ , thus  $n$  divides  $|G|$ .

2. really?

$\square$

**Proposition 4.15 (4.14).** The center of  $A_n$  is trivial for all  $n \geq 4$ . (This can be shown using the class formula of  $S_n$  and how conjugacy class splits to  $A_n$ ).

**Problem 4.34 (4.18).** For  $n \geq 5$ , let  $H$  be a proper subgroup of  $A_n$ . Prove that  $[A_n : H] \geq n$  and  $A_n$  has a subgroup of index  $n$  for all  $n \geq 3$ .

*Proof.* Consider the transitive action of  $A_n$  on the cosets  $A_n/H$ , this action is nontrivial, hence must be injective since  $A_n$  is simple for  $n \geq 5$ , this shows that

$$|A_n| \leq [A_n : H]!$$

which implies  $[A_n : H] \geq n$ .

The index  $n$  subgroup of  $A_n$  can be chosen as the subgroup  $H$  that fixes 1, then  $H \cong A_{n-1}$ .  $\square$

**Problem 4.35 (4.19).** 1. Prove that for  $n \geq 5$  there are no nontrivial actions of  $A_n$  on any set  $S$  with  $|S| < n$ .  
 2. Construct a nontrivial action of  $A_4$  on a set  $S$ ,  $|S| = 3$ .  
 3. Is there a nontrivial action of  $A_4$  on a set  $S$  with  $|S| = 2$ ?

*Proof.* 1. Same as above, using the simplicity of  $A_n$  for  $n \geq 5$ .

2.  $A_4$  has a normal subgroup  $N = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , thus is nontrivial transitive action on  $G/N$ .

3. The kernel  $\ker(\psi)$  must be nontrivial (size), and is normal with index 2, which  $A_4$  does not have.  $\square$

## 4.5 Semidirect Products

**Proposition 4.16 (5.1).** Let  $G$  be a finite group, and let  $P_1, \dots, P_r$  be its nontrivial Sylow subgroups. Assume all  $P_i$  are normal in  $G$ .

- Prove that  $G \cong P_1 \times \dots \times P_r$ .
- Prove that  $G$  is nilpotent. (Hint: Mod out by the center, and work by induction on  $|G|$ . What is the center of a direct product of groups?)

*Proof.* Think about their intersection, and what does the center look like.  $\square$

**Problem 4.36 (5.4).** Give an example of a SES that doesn't split.

*Proof.*

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

$\square$

**Problem 4.37 (5.7).** Let  $N$  be a group, and let  $\alpha : N \rightarrow N$  be an automorphism of  $N$ . Prove that  $\alpha$  may be realized as conjugation, in the sense that there exists a group  $G$  containing  $N$  as a normal subgroup and such that  $\alpha(n) = gng^{-1}$  for some  $g \in G$ .

*Proof.* Construct the semidirect product by taking  $H = \mathbb{Z}$  and  $\theta : \mathbb{Z} \rightarrow \text{Aut}(N)$  as

$$\theta_k(n) = \alpha^k(n)$$

□

**Problem 4.38 (5.8).** Prove that any semidirect product of two solvable groups is solvable. Show that semidirect products of nilpotent groups need not be nilpotent.

*Proof.* Construct sequence such that quotients are quotients from  $N, H$ ;  $S_3$  is a semidirect product of  $\mathbb{Z}/2\mathbb{Z}$  and  $\mathbb{Z}/3\mathbb{Z}$ . □

**Problem 4.39 (5.10).** Let  $N$  be a normal subgroup of a finite group  $G$ , and assume that  $|N|$  and  $|G/N|$  are relatively prime. Assume there is a subgroup  $H$  in  $G$  such that  $|H| = |G/N|$ . Prove that  $G$  is a semidirect product of  $N$  and  $H$ .

*Proof.* To prove  $G = N \rtimes H$ , you need

1.  $G = NH$ .
2.  $N \cap H = \{e\}$ .

The second is obvious: the first is done by showing  $|G| = |N||H|$ , recall

$$|NH| = \frac{|N| \cdot |H|}{|N \cap H|}$$

□

**Problem 4.40 (5.11).** For all  $n > 0$  express  $D_{2n}$  as a semidirect product  $C_n \rtimes_\theta C_2$ , finding  $\theta$  explicitly.

*Proof.*  $\mathbb{Z}/n\mathbb{Z} = \{1, r, \dots, r^{n-1}\}$  is an index 2 subgroup, hence normal, thus

$$D_{2n} = \langle r, s : r^n = s^2 = e, srs^{-1} = r^{-1} \rangle$$

□

**Problem 4.41 (5.12).** Classify groups  $G$  of order  $pq$ , with  $p < q$  prime: show that if  $|G| = pq$ , then either  $G$  is cyclic or  $q \equiv 1 \pmod{p}$  and there is exactly one isomorphism class of noncommutative groups of order  $pq$  in this case.

*Proof.* There is a normal subgroup of order  $q$ : then

$$\theta : \frac{\mathbb{Z}}{p\mathbb{Z}} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$$

If the action is trivial, then

$$G \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{q\mathbb{Z}} \cong \frac{\mathbb{Z}}{pq\mathbb{Z}}$$

i.e.,  $G$  is cyclic.

If  $q - 1 \equiv 0 \pmod{p}$ , then there exists  $r \in (\mathbb{Z}/q\mathbb{Z})^\times$  such that  $r^p = 1$ , thus we have

$$G = \langle g, h : g^q = h^p = e, hgh^{-1} = g^r \rangle$$

This is the noncommutative group. □



**Problem 4.42 (5.13).** Let  $G = N \rtimes_{\theta} H$  be a semidirect product, and let  $K$  be the subgroup of  $G$  corresponding to  $\ker \theta \subseteq H$ . Prove that  $K$  is the kernel of the action of  $G$  on the set  $G/H$  of left-cosets of  $H$ .

*Proof.*  $K$  is the largest normal subgroup of  $G$  contained in  $H$ . □

**Problem 4.43 (5.15).** Let  $G$  be a group of order 28.

1. Prove that  $G$  contains a normal subgroup  $N$  of order 7.
2. Recall that, up to isomorphism, the only groups of order 4 are  $C_4$  and  $C_2 \times C_2$ . Prove that there are two homomorphisms  $C_4 \rightarrow \text{Aut}_{Grp}(N)$  and two homomorphisms  $C_2 \times C_2 \rightarrow \text{Aut}_{Grp}(N)$  up to the choice of generators for the sources.
3. Conclude that there are four groups of order 28 up to isomorphism: the two direct products  $C_4 \times C_7$ ,  $C_2 \times C_2 \times C_7$ , and two noncommutative groups.
4. Prove that  $D_{28} \cong C_2 \times D_{14}$ . The other noncommutative group of order 28 is a generalized quaternionic group.

*Proof.* 1.  $n_7 = 1$ .

2. There is a trivial isomorphism for both;  $1 \mapsto r$ , where  $r^2 = 1$  for  $C_4$ ;  $(1, 0) \mapsto r$ ,  $(0, 1) \mapsto 0$  or the other way around which is the same.
3. By 2.
4. There is no element of order 4 in  $D_{28}$ . (There is an element of order 4 iff  $d$  divides  $n$  in  $D_{2n}$ ).

□

**Proposition 4.17 (5.16).** The quaternionic group  $Q_8$  cannot be written as a semidirect product of two nontrivial subgroups.

## 4.6 Classification of Finite Abelian Group

**Problem 4.44.** Complete the classification of groups of order 8.

*Proof.* There are 5:  $\mathbb{Z}/8\mathbb{Z}$ ,  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ,  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ,  $D_8$ ,  $Q_8$ . □

**Proposition 4.18.** Let  $G$  be a noncommutative group of order  $p^3$ , where  $p$  is a prime integer. Prove that  $Z(G) \cong \mathbb{Z}/p\mathbb{Z}$  and  $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ .

**Proposition 4.19.** Let  $p$  be a prime integer. Prove that the number of distinct isomorphism classes of abelian groups of order  $p^r$  equals the number of partitions of the integer  $r$ .

**Problem 4.45.** Classify abelian groups of order 400.

*Proof.* By the above, there are 10 isomorphism classes. □

**Proposition 4.20.** The dual of a finite group  $G$  is the abelian group  $G^\vee := \text{Hom}_{\text{Grp}}(G, \mathbb{C}^*)$ , where  $\mathbb{C}^*$  is the multiplicative group of  $\mathbb{C}$ .

- The image of every  $\sigma \in G^\vee$  consists of roots of 1 in  $\mathbb{C}$ , that is, roots of polynomials  $x^n - 1$  for some  $n$ .
- If  $G$  is a finite abelian group, then  $G \cong G^\vee$ . (Hint: First prove this for cyclic groups; then use the classification theorem to generalize to the arbitrary case.)

**Problem 4.46.** Finite abelian group classifications for modules:

1. Use the classification theorem for finite abelian groups to classify all finite modules over the ring  $\mathbb{Z}/n\mathbb{Z}$ .
2. Prove that if  $p$  is prime, all finite modules over  $\mathbb{Z}/p\mathbb{Z}$  are free.

*Proof.* 1. Any finite  $G$  is written as

$$G \cong \frac{\mathbb{Z}}{p_1^{a_1}} \oplus \cdots \oplus \frac{\mathbb{Z}}{p_k^{a_k}}$$

where the  $p$ 's are not necessarily distinct. The  $\mathbb{Z}/n\mathbb{Z}$ -module condition requires that for  $n \cdot m = 0$  for all  $m \in M$ , i.e.,  $p_i^{a_i}$  must divide  $n$  for all  $i$ . This shows that any finite abelian group over  $\mathbb{Z}/n\mathbb{Z}$  is of the form

$$G \cong \bigoplus_{p|n} \bigoplus_{i=1}^k \frac{\mathbb{Z}}{p^i \mathbb{Z}}$$

2. It shows that only  $\mathbb{Z}/p\mathbb{Z}$  terms are allowed in the above expression. □

**Proposition 4.21.** Let  $G, H$  be finite abelian groups such that, for all positive integers  $n$ ,  $G$  and  $H$  have the same number of elements of order  $n$ . Then  $G \cong H$ .

**Problem 4.47.** Let  $G$  be a finite abelian  $p$ -group, and assume  $G$  has only one subgroup of order  $p$ . Prove that  $G$  is cyclic.

*Proof.*  $G$  must take the form

$$G \cong \frac{\mathbb{Z}}{p^{a_1} \mathbb{Z}}$$

with no other factors. □

**Problem 4.48.** Let  $G$  be a finite abelian group, and let  $a \in G$  be an element of maximal order in  $G$ . Prove that the order of every  $b \in G$  divides  $|a|$ .

*Proof.* For different primes, the orders multiply. □

## Chapter 5

# Ring Theory II, Irreducibility of Polynomials

### 5.1 factorizations

**Problem 5.1 (1.4).** Show that the ring of real-valued continuous functions on  $[0, 1]$  is not Noetherian.

*Proof.* Let  $I_n$  be the functions  $f$  such that  $f(x) = 0$  on  $[\frac{1}{n+1}, 1]$ , then it fails acc. □

**Problem 5.2 (1.10).** Recall a ring  $R$  is Noetherian if and only if it satisfies the ascending chain condition for ideals. A ring is Artinian if it satisfies the descending chain condition for ideals.

1. Prove that if  $R$  is Artinian and  $I \subset R$  is an ideal, then  $R/I$  is Artinian.
2. Prove that if  $R$  is an Artinian integral domain, then it is a field. (Hint: Consider the descending chain  $(a) \supseteq (a^2) \supseteq (a^3) \supseteq \dots$  for a nonzero element  $a \in R$ .)

*Proof.* 1. Ideals in  $R/I$  have a one-to-one correspondence to ideals  $J \subset R$  containing  $I$ .  
2. Then  $(a^i) = (a^{i+1})$  for some  $i$ . This shows  $a$  is a unit. □

**Proposition 5.1.** An Artinian ring  $R$  that is also an integral domain is a field!

**Problem 5.3 (1.15).** Let  $S = \mathbb{Z}[x_1, \dots, x_n]$  be naturally identified with a subring of  $R = \mathbb{Z}[x_1, x_2, x_3, \dots]$ .

1. Prove that if  $f \in S$  and  $(f) \subseteq (g)$  in  $R$ , then  $g \in S$  as well.
2. Conclude that the ascending chain condition for principal ideals holds in  $R$ , and factorization exists.

*Proof.* is obvious. □

**Proposition 5.2.** A non-Noetherian ring where factorizations exist:

$$\mathbb{Z}[x_1, x_2, x_3, \dots]$$

**Problem 5.4 (1.17).** Consider the subring of  $\mathbb{C}$ :

$$\mathbb{Z}[\sqrt{-5}] := \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}.$$

1. Prove that this ring is isomorphic to  $\mathbb{Z}[t]/(t^2 + 5)$ . Prove that it is a Noetherian integral domain.
2. Define a norm  $N$  on  $\mathbb{Z}[\sqrt{-5}]$  by setting  $N(a + bi\sqrt{5}) = a^2 + 5b^2$ . Note that  $N(zw) = N(z)N(w)$ .
3. Prove that  $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$  are all irreducible nonassociate elements of  $\mathbb{Z}[\sqrt{-5}]$ .
4. Prove that no element listed in the preceding point is prime. (Rings obtained by modding out the ideals generated by these elements are not integral domains.)
5. Prove that  $\mathbb{Z}[\sqrt{-5}]$  is not a UFD.

*Proof.* 1. Establish by evaluation map at  $\sqrt{5}$ , and  $\mathbb{Z}$  is Noetherian, which implies  $\mathbb{Z}[t]/I$  is Noetherian. 3. Use norm. 4. For example quotient out by (2), then  $(1 + i\sqrt{5})(1 + i\sqrt{5}) = 0$ . 5.  $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ .  $\square$

## 5.2 UFD, PID, ED

**Problem 5.5 (2.5).** gcd exists in UFD's but they don't in general: Let  $R$  be the subring of  $\mathbb{Z}[t]$  consisting of polynomials with no term of degree 1:

$$R = \{a_0 + a_2t^2 + \cdots + a_dt^d \mid a_i \in \mathbb{Z}\}.$$

1. Prove that  $R$  is indeed a subring of  $\mathbb{Z}[t]$ , and conclude that  $R$  is an integral domain.
2. List all common divisors of  $t^5$  and  $t^6$  in  $R$ .
3. Prove that  $t^5$  and  $t^6$  have no gcd in  $R$ .

*Proof.* 2.  $t^2, t^3, t^4, t^5$ . 3.  $t^5$  doesn't work because  $t \notin R$ .  $\square$

**Problem 5.6 (2.8).** Let  $R$  be a UFD, and let  $I \neq (0)$  be an ideal of  $R$ . Prove that every descending chain of principal ideals containing  $I$  must stabilize.

*Proof.* There exists  $a \neq 0 \in I$ , consider its finite multiset of irreducible factors, every descending

$$(a_1) \supset (a_2) \supset \cdots$$

gives an ascending

$$m(a_1) \subset m(a_2) \subset \cdots$$

$\square$

**Problem 5.7 (2.11).** Let  $R$  be a PID, and let  $I$  be a nonzero ideal of  $R$ . Show that  $R/I$  is an Artinian ring, by proving explicitly that the d.c.c. holds in  $R/I$ .

*Proof.* Ideals in  $R/I$  corresponds to ideals  $J$  in  $R$  containing  $I$ , then using the above.  $\square$

**Problem 5.8 (2.19).** A **discrete valuation** on a field  $k$  is a surjective homomorphism of abelian groups  $v : (k^*, \cdot) \rightarrow (\mathbb{Z}, +)$  such that  $v(a + b) \geq \min(v(a), v(b))$  for all  $a, b \in k^*$  with  $a + b \in k^*$ .

1. Prove that the set  $R := \{a \in k^* \mid v(a) \geq 0\} \cup \{0\}$  is a subring of  $k$ .
2. Prove that  $R$  is a Euclidean domain.
3. Prove that the ring of rational numbers  $\frac{a}{b}$  with  $b$  not divisible by a fixed prime integer  $p$  is a DVR. (Rings arising in this fashion are called **discrete valuation rings** (DVR). Note that the Krull dimension of a DVR is 1.)

*Proof.* 2. You show that  $v$  is a Euclidean valuation: let  $a \in R, b \neq 0$ , then

$$v(a/b) = v(a) - v(b)$$

if  $\geq 0$ , then  $a/b \in R$ , we set  $q = 1, r = 0$ ; if  $< 0$ , then set  $q = 0$ , then  $r = a$ , we have  $v(r) < v(b)$ . 3. Set  $v(p) = 1, v(m) = 0$  for  $m$  not divisible by  $p$ .  $\square$

**Problem 5.9 (2.20).** DVRs are Euclidean domains. In particular, they must be PIDs. Check this directly, as follows. Let  $R$  be a DVR, and let  $t \in R$  be an element such that  $v(t) = 1$ . Prove that if  $I \subseteq R$  is any nonzero ideal, then  $I = (t^k)$  for some  $k \geq 1$ . (The element  $t$  is called a **local parameter** of  $R$ .)

*Proof.* Let  $b \in I$  be such that  $v(b)$  is minimal in  $I$ , let  $k = v(b)$ , we claim  $I = (t^k)$ .  $\square$

## 5.3

**Problem 5.10 (3.13).** Let  $R$  be a commutative ring, and let  $N$  be its nilradical. Let  $r \notin N$ .

1. Consider the family  $\mathcal{F}$  of ideals of  $R$  that do not contain any power  $r^k$  of  $r$  for  $k > 0$ . Prove that  $\mathcal{F}$  has maximal elements.
2. Let  $I$  be a maximal element of  $\mathcal{F}$ . Prove that  $I$  is prime.
3. Conclude that  $r \notin N$  implies  $r$  is not in the intersection of all prime ideals of  $R$ .

This shows the nilradical of a commutative ring  $R$  equals the intersection of all prime ideals of  $R$ .

*Proof.* 1. Zorn's lemma: suffices to show every chain  $\{I_\alpha\}$  has an upper bound, which is the union.

2. Consider  $ab \in I$ , suppose  $a, b \notin I$ , then  $I + (a), I + (b)$  are not in  $\mathcal{F}$ , then it shows  $I$  is not in  $\mathcal{F}$ , contradiction.
3.  $r \notin I$ , done.  $\square$

**Problem 5.11 (3.14).** The **Jacobson radical** of a commutative ring  $R$  is the intersection of the maximal ideals in  $R$ . (Thus, the Jacobson radical contains the nilradical.)

Prove that  $r$  is in the Jacobson radical if and only if  $1 + rs$  is invertible for every  $s \in R$ .

*Proof.* If  $r$  is in every  $\mathfrak{m} \in M$ , then for every  $s \in R$ ,  $rs \in \mathfrak{m}$  for every  $\mathfrak{m}$ , this implies that  $1 + rs \notin \mathfrak{m}$  for any  $\mathfrak{m}$ , i.e.,  $1 + rs$  is a unit. This is because if it is not a unit, then we can consider  $(1 + rs)$ , by Zorn's lemma, it is contained in some  $\mathfrak{m}$ , which is a contradiction.

For the reverse reflection, suppose  $r \notin \mathfrak{m}$  for some  $\mathfrak{m}$ , then

$$\mathfrak{m} \subset \mathfrak{m} + (r) \Rightarrow \mathfrak{m} + (r) = R$$

i.e., for  $1 = rs + m$  for some  $m \in \mathfrak{m}$ , i.e.,  $m$  is a unit, which is a contradiction.  $\square$

## 5.4

**Proposition 5.3 (4.18).** Let  $R$  be an integral domain. Prove the invertible elements in  $R[x]$  are exactly the units of  $R$  (as constant polynomials).

**Problem 5.12 (4.19).** An element  $a \in R$  is **nilpotent** if  $a^n = 0$  for some  $n \geq 0$ . Prove that if  $a$  is nilpotent, then  $1 + a$  is a unit.

*Proof.*  $a$  is in the intersection of all prime ideals, hence all maximal ideals, this implies  $1 + a$  cannot be in any maximal ideal, i.e.,  $1 + a$  is a unit. (If  $1 + a$  is not a unit, then  $(a + 1)$  is contained in some  $\mathfrak{m}$ ).  $\square$

## 5.5 Irreducibility

**Problem 5.13 (5.4).** Prove that  $f(x) = x^4 + x^2 + 1$  is reducible over  $\mathbb{Z}$ , and that it has no rational roots.

*Proof.* It can be factored completely:

$$f(x) = \frac{x^6 - 1}{x^2 - 1} = \frac{(x^3 + 1)(x^3 - 1)}{(x + 1)(x - 1)} = (1 - x + x^2)(1 + x + x^2)$$

The rational root theorem states  $\alpha = \pm 1$ , and neither are roots.  $\square$

**Problem 5.14 (5.6).** Construct fields of 27 and 121 elements.

*Proof.*  $f(x) = x^3 + 2x + 1$  has no roots in  $\mathbb{F}_3$  and  $g(x) = x^2 + x + 7$  has no roots in  $\mathbb{F}_{11}$ .  $\square$

**Problem 5.15 (5.7).** Let  $R$  be an integral domain, let  $f \in R[x]$  be of degree  $d$ , prove that  $f(x)$  is determined uniquely by  $d + 1$  points in  $R$ .

*Proof.* Suppose  $f(x_i) = g(x_i)$  for  $1 \leq i \leq d + 1$ , then consider  $h = f - g$ , then  $h(x_i) = 0$  for all  $i$ , since nonzero polynomials of degree  $d$  can have at most  $d$  roots, this shows  $h = 0$ .  $\square$

**Problem 5.16 (5.10).** Prove that  $(x - 1)(x - 2) \dots (x - n) - 1$  is irreducible over  $\mathbb{Q}$  for all  $n \geq 1$ .

*Proof.* When  $n$  is odd, suppose  $F(x) = f(x)g(x)$ , then WLOG assume  $f$  has degree  $\leq \frac{n-1}{2}$ , and we know for  $x_i = i$ ,  $f(x_i)g(x_i) = \pm 1$ , i.e., consider either  $f(x) - 1$  or  $f(x) + 1$ , we get a polynomial with more zeros than its degree, i.e.,  $f \equiv 0$ .

If  $n$  is even (and the only case remaining is when  $\deg(f) = \deg(g) = \frac{n}{2}$ ), consider  $f(x)^2 - 1$ , this polynomial also has degree  $n$ , and has roots at  $x = 1, \dots, n$ , since  $f$  is monic, we know

$$f(x)^2 - 1 = (x - 1) \dots (x - n)$$

This implies that

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

which is impossible. □

**Problem 5.17 (5.14).** How many different embeddings of the field  $\mathbb{Q}[t]/(t^3 - 2)$  are there in  $\mathbb{R}$  and  $\mathbb{C}$ .

*Proof.* Embeddings refer to the homomorphisms

$$\varphi : \mathbb{Q}[t]/(f(t)) \rightarrow \mathbb{R}$$

where

$$\varphi : t \mapsto \alpha \text{ where } f(\alpha) = 0$$

Thus there is 1 embedding into  $\mathbb{R}$  and 3 into  $\mathbb{C}$ . □

**Problem 5.18 (5.18).** Let  $f \in \mathbb{Z}[x]$  be a cubic polynomial such that  $f(0), f(1)$  are odd and with odd leading coefficients. Prove that  $f$  is irreducible over  $\mathbb{Q}$ .

*Proof.* Suffices to prove  $f$  is irreducible over  $\mathbb{Z}/p\mathbb{Z}$  for some  $p$ . Consider  $\mathbb{Z}/2\mathbb{Z}$ , then let  $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ , we see  $f(x)$  can be  $x^3 + x^2 + 1$  or  $x^3 + x + 1$ , and both are irreducible over  $\mathbb{Z}/2\mathbb{Z}$ . □

**Problem 5.19 (5.20).** Prove that  $x^6 + 4x^3 + 1$  is irreducible by Eisenstein.

*Proof.* Replace  $x$  with  $x + 1$ , then done. □

**Problem 5.20 (5.21).** Prove that  $1 + x + x^2 + \dots + x^{n-1}$  is reducible over  $\mathbb{Z}$  if  $n$  is not prime.



**Warning 5.1.**  $1 + x + x^2 + \dots + x^{p-1}$  is irreducible by Eisenstein.

*Proof.* Let  $n = ab$ ,

$$f(x) = \frac{x^n - 1}{x - 1}$$

where

$$(x^a)^b - 1 = (x^a - 1)(1 + x^a + \dots + x^{a(b-1)})$$

Then we see  $f$  is reducible. □

## 5.6 CRT

**Proposition 5.4 (6.2).** Recall idempotent:  $a \in R$  such that  $a^2 = a$ , if  $R$  contains an idempotent, then

$$R \cong \frac{R}{(a)} \times \frac{R}{(1-a)}$$

(Proof sketch: endow  $(a)$  with a ring structure with  $(a)$  as the identity, then  $(a) \cong R/(1-a)$ ).

**Proposition 5.5 (6.8).** Let  $n \in \mathbb{Z}$ , and  $n = p_1^{n_1} \dots p_r^{n_r}$ , then

$$\frac{\mathbb{Z}}{(n)} \cong \frac{\mathbb{Z}}{(p_1^{n_1})} \times \dots \times \frac{\mathbb{Z}}{(p_r^{n_r})}$$

and

$$\left( \frac{\mathbb{Z}}{(n)} \right)^* \cong \left( \frac{\mathbb{Z}}{(p_1^{n_1})} \right)^* \times \dots \times \left( \frac{\mathbb{Z}}{(p_r^{n_r})} \right)^*$$

where  $(\mathbb{Z}/n\mathbb{Z})^*$  is the group of units.



## Chapter 6

# Linear Algebra I

### 6.1 Basis

**Problem 6.1 (1.5).** Let  $R$  be an integral domain. Prove or disprove the following:

- Every linearly independent subset of a free  $R$ -module may be completed to a basis.
- Every generating subset of a free  $R$ -module contains a basis.

*Proof.* Both are not true.  $(2) \subset \mathbb{Z}, (2), (3) \subset \mathbb{Z}$ . □

**Problem 6.2 (1.11).** Let  $R$  be a commutative ring, and let  $F = R^{\oplus B}$  be a free module over  $R$ . Let  $\mathfrak{m}$  be a maximal ideal of  $R$ , and let  $k = R/\mathfrak{m}$  be the quotient field. Prove that

$$F/\mathfrak{m}F \cong k^{\oplus B}$$

as  $k$ -vector spaces. Prove that commutative rings satisfy the IBN (Invariant Basis Number) property.

*Proof.* We can reduce any commutative ring to the field case. □

**Problem 6.3 (1.12).** Let  $V$  be a vector space over a field  $k$ , and let  $R = \text{End}_{k\text{-Vect}}(V)$  be its ring of endomorphisms (cf. Exercise [III]5.9). (Note that  $R$  is not commutative in general.)

- Prove that  $\text{End}_{k\text{-Vect}}(V \oplus V) \cong R^4$  as an  $R$ -module.
- Prove that  $R$  does not satisfy the IBN property if  $V = k^{\oplus \mathbb{N}}$ .

(Note that  $V \cong V \oplus V$  if  $V = k^{\oplus \mathbb{N}}$ .)

*Proof.* Let  $\varphi : V \oplus V \rightarrow V \oplus V$ , then  $\varphi$  can be viewed as a  $2 \times 2$  matrix.  
For  $V = k^{\oplus \mathbb{N}}$ , we have

$$R = \text{End}(V) = \text{End}(V \oplus V) = R^4$$

□

**Problem 6.4 (1.19).** Let  $k$  be a field, and let  $f(x) \in k[x]$  be any polynomial. Prove that there exists a multiple of  $f(x)$  in which all exponents of nonzero monomials are prime integers.

*Example:* For  $f(x) = 1 + x^5 + x^6$ ,

$$(1 + x^5 + x^6)(2x^2 - x^3 + x^5 - x^8 + x^9 - x^{10} + x^{11}) = 2x^2 - x^3 + x^5 + 2x^7 + 2x^{11} - x^{13} + x^{17}.$$

*Proof.* Note that  $k[x]/(f(x))$  is a finitely generated  $k$ -module, i.e., a vector space of finite dimensions, hence the polynomials of prime powers are linearly dependent and thus a nontrivial combination is in  $(f(x))$ .  $\square$

## 6.2 Nakayama's Lemma

**Problem 6.5 (3.7).** Let  $R$  be a commutative ring,  $M$  a finitely generated  $R$ -module, and let  $J$  be an ideal of  $R$ . Assume  $JM = M$ . Prove that there exists an element  $b \in J$  such that  $(1 + b)M = 0$ .

*Proof.* Let  $M = \langle m_1, \dots, m_r \rangle$ , since  $JM = M$ , we can write any  $m_i \in M$  as

$$m_i = \sum_{j=1}^r b_{ij} m_j$$

defining matrix  $B = (b_{ij})$ , we see that

$$B \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}$$

Thus  $(B - I)m = 0$  for all  $m \in M$ , by previous exercise, we know  $\det(B - I) = 0$ , we see that there exists  $b \in J$  such that

$$(1 + b)M = 0$$

$\square$

**Problem 6.6 (3.8).** Let  $R$  be a commutative ring,  $M$  be a finitely generated  $R$ -module, and let  $J$  be an ideal of  $R$  contained in the Jacobson radical of  $R$ . Prove that

$$M = 0 \iff JM = M.$$

*Proof.* It follows directly from the above exercise. If  $JM = M$ , then there exists  $b \in J$  such that  $(1 + b)M = 0$ , moreover, if  $b \in J$ , then  $1 + b$  is a unit, i.e.,  $m = 0$  for all  $m \in M$ .  $\square$

**Problem 6.7 (3.9).** Let  $R$  be a commutative local ring, that is, a ring with a single maximal ideal  $\mathfrak{m}$ , and let  $M, N$  be finitely generated  $R$ -modules. Prove that if  $M = \mathfrak{m}M + N$ , then  $M = N$ . (Hint: apply Nakayama's to  $M/N$  and note that  $\mathfrak{m}$  is the Jacobson ideal).

*Proof.* Directly follows from the hint.  $\square$

**Problem 6.8 (3.10).** Let  $R$  be a commutative local ring, and let  $M$  be a finitely generated  $R$ -module. Note that  $M/\mathfrak{m}M$  is a finite-dimensional vector space over the field  $R/\mathfrak{m}$ ; let  $m_1, \dots, m_r \in M$  be elements whose cosets mod  $\mathfrak{m}M$  form a basis of  $M/\mathfrak{m}M$ . Prove that  $m_1, \dots, m_r$  generate  $M$ . Hint: Show that  $\langle m_1, \dots, m_r \rangle + \mathfrak{m}M = M$ ; then apply Nakayama's lemma in the form of Exercise 3.9.

*Proof.* We will write out this: for every  $m \in M$ , we know there exists  $a_i$  such that

$$m - \sum_{i=1}^i a_i m_i \in mM$$

hence

$$\langle m_1, \dots, m_r \rangle + mM = M$$

Then it follows from if  $M = mM + N$ , then  $M = N$ . □

## 6.3 Invariants

**Proposition 6.1.** Let  $R$  be an integral domain,  $\alpha$  is injective iff  $\det(\alpha) \neq 0$ , and  $\alpha$  is surjective iff  $\det(\alpha)$  is a unit.

**Problem 6.9 (6.10).** Let  $F_1, F_2$  be free  $R$ -modules of finite rank, and let  $\alpha_1$ , resp.,  $\alpha_2$ , be linear transformations of  $F_1$ , resp.,  $F_2$ . Let  $F = F_1 \oplus F_2$ , and let  $\alpha = \alpha_1 \oplus \alpha_2$  be the linear transformation of  $F$  restricting to  $\alpha_1$  on  $F_1$  and  $\alpha_2$  on  $F_2$ .

- Prove that  $P_\alpha(t) = P_{\alpha_1}(t)P_{\alpha_2}(t)$ . That is, the characteristic polynomial is multiplicative under direct sums.
- Find an example showing that the minimal polynomial is not multiplicative under direct sums.

*Proof.* The determinant of block diagonal matrices is the product of the determinant. Let both be the identity matrix. □

**Problem 6.10 (6.13).** Let  $A$  be a square matrix with integer entries. Prove that if  $\lambda$  is a rational eigenvalue, then  $\lambda \in \mathbb{Z}$ .

*Proof.* Let  $p(t) = a_0 + a_1t + \dots + a_nt^n$  be the characteristic polynomial of  $A$ , then  $p(\lambda) = 0$ , letting  $\lambda = \frac{p}{q}$ , then

$$p \mid a_0, \quad q \mid a_n$$

we know that  $p$  is monic, thus  $a_n = 1$ , hence  $\lambda \in \mathbb{Z}$ . □

**Problem 6.11 (7.3).** Prove that two linear transformations of a vector space of dimension  $\leq 3$  are similar if and only if they have the same characteristic and minimal polynomials. Is this true in dimension 4?

*Proof.* Two matrices are similar iff they have the same Jordan form. For  $n = 4$ : consider

$$T_1 = \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix} \quad T_2 = \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{pmatrix}$$

Both  $T_1, T_2$  have  $p(t) = (t - \lambda)^4$  and  $m(t) = (t - \lambda)^2$ , but they are not similar ( $\lambda$  has 2 eigenvectors in  $T_1$  but 3 in  $T_2$ ). □

**Proposition 6.2 (7.4).** Let  $k$  be a field, and let  $K$  be a field containing  $k$ . Then  $A$  and  $B$  are similar over  $k$  if and only if they are similar over  $K$ .

**Problem 6.12 (7.7).** Let  $V$  be a  $k$ -vector space of dimension  $n$ , and let  $\alpha \in \text{End}_k(V)$ . Prove that the minimal and characteristic polynomials of  $\alpha$  coincide if and only if there is a vector  $v \in V$  such that

$$\{v, \alpha(v), \dots, \alpha^{n-1}(v)\}$$

is a basis of  $V$ .

*Proof.* The minimal and characteristic of  $\alpha$  coincide iff

$$V \cong \frac{k[t]}{(f(t))}$$

as  $k[t]$  modules, where  $f(t) = b_n t^n + \dots + b_0$  has an action on  $V$  as

$$f(t)(v) = b_n \alpha^n(v) + \dots + b_0 v$$

The RHS has basis  $\{1, t, \dots, t^{n-1}\}$ , and we are given an isomorphism  $\varphi : \frac{k[t]}{(f(t))} \rightarrow V$  as  $\varphi : t \mapsto \alpha(\varphi(1))$ , hence we see

$$\{\varphi(1), \alpha(\varphi(1)), \dots, \alpha^{n-1}(\varphi(1))\}$$

is a basis of  $V$ . □

here

**Problem 6.13 (7.8).** Let  $V$  be a  $k$ -vector space of dimension  $n$ , and let  $\alpha \in \text{End}_k(V)$ . Prove that the characteristic polynomial  $P_\alpha(t)$  divides a power of the minimal polynomial  $m_\alpha(t)$ .

*Proof.* Assume that  $k$  is algebraically closed, and polynomials factors, the minimal polynomial  $m_\alpha$  contains all the  $(t - \lambda_i)$  for distinct  $\lambda_i$ 's by Lemma 7.12. Thus  $P_\alpha$  divides  $(m_\alpha)^n$ .

The more general case follows directly from decomposition theorem: there exists monic  $f_1, \dots, f_m$  such that

$$V \cong \frac{k[t]}{(f_1(t))} \oplus \dots \oplus \frac{k[t]}{(f_m(t))}$$

as  $k[t]$ -modules, where  $f_1(t) \mid \dots \mid f_m(t)$ . The characteristic and minimal polynomials are such that

$$P_\alpha(t) = f_1(t) \dots f_m(t)$$

and

$$m_\alpha(t) = f_m(t)$$

□

**Problem 6.14 (7.12).** Let  $V$  be a finite-dimensional  $k$ -vector space, and let  $\alpha \in \text{End}_k(V)$  be a diagonalizable linear transformation. Assume that  $W \subseteq V$  is an invariant subspace, so that  $\alpha$  induces a linear transformation  $\alpha|_W \in \text{End}_k(W)$ . Prove that  $\alpha|_W$  is also diagonalizable. (Use Proposition 7.18.)

*Proof.* Assume that characteristic polynomial factors completely over  $k$ , then  $\alpha$  is diagonalizable iff minimal polynomial  $m_\alpha$  has no repeated roots, thus  $\alpha|_W$  also has no repeated roots as it divides  $m_\alpha$ . □

**Problem 6.15 (7.13).** Let  $R$  be an integral domain. Assume that  $A \in \mathcal{M}_n(R)$  is diagonalizable, with distinct eigenvalues. Let  $B \in \mathcal{M}_n(R)$  be such that  $AB = BA$ . Prove that  $B$  is also diagonalizable, and in fact it is diagonal w.r.t. a basis of eigenvectors of  $A$ . (If  $P$  is such that  $PAP^{-1}$  is diagonal, note that  $PAP^{-1}$  and  $PBP^{-1}$  also commute.)

*Proof.* It suffices to see that if  $v_1 \neq 0$  is such that  $Av_1 = \lambda_1 v_1$ , then

$$\begin{aligned} A(Bv_1) &= B(Av_1) \\ &= B\lambda_1 v_1 \\ &= \lambda_1(Bv_1) \end{aligned}$$

Thus  $Bv_1$  is contained in the one-dimensional subspace generated by  $v_1$ . □

**Problem 6.16 (7.14).** Prove that "commuting transformations may be simultaneously diagonalized", in the following sense. Let  $V$  be a finite-dimensional vector space, and let  $\alpha, \beta \in \text{End}_k(V)$  be diagonalizable transformations. Assume that  $\alpha\beta = \beta\alpha$ . Prove that  $V$  has a basis consisting of eigenvectors of both  $\alpha$  and  $\beta$ . (Argue as in Exercise 7.13 to reduce to the case in which  $V$  is an eigenspace for  $\alpha$ ; then use Exercise 7.12.)

*Proof.* Separate into eigenspaces: consider eigenspace  $E_1$  of  $\alpha$ , then diagonalize  $\beta$  in  $E_1$  (by 7.12), note that  $E_1$  is invariant under  $\beta$ . □

**Problem 6.17 (7.15).** A **complete flag** of subspaces of a vector space  $V$  of dimension  $n$  is a sequence of nested subspaces

$$0 = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_{n-1} \subsetneq V_n = V$$

with  $\dim V_i = i$ . In other words, a complete flag is a composition series in the sense of Exercise 1.16. Let  $V$  be a finite-dim vector space over algebraically closed  $k$ . Prove that every linear transformation  $\alpha$  of  $V$  preserves a complete flag: there is a complete flag as above and such that  $\alpha(V_i) \subset V_i$ .

Find a linear transformation of  $\mathbb{R}^2$  that does not preserve a complete flag.

*Proof.* It suffices take  $V_i$  as the subspaces generated by eigenvectors. An example in  $\mathbb{R}^2$ :

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

□

## 6.4 Classification of Finitely Generated Modules over PID

5.2, 5.13, 5.14

## **Chapter 7**

# **Fields**

## **Chapter 8**

# **Linear Algebra II**