Aluffi Problems

Hui Sun

August 5, 2025

Contents

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 $\mathrm{lcm}(|g|, |h|)$, 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 $\mathrm{Aut}(G)$ is cyclic, then G is abelian.

Proof. This implies $\mathrm{Inn}(G)$ is cyclic, which is iff $\mathrm{Inn}(G)$ 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 $H = \left\langle \frac{p_1}{q_1}, \frac{p_2}{q_2} \right\rangle$, find $\mathrm{lcm}(q_1, q_2) = q$, 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 notatoin $\left|\frac{G}{H}\right| = [G : H]$). Let G act on the cosets G/H by left multiplication, this action $\sigma : G \to \text{Aut}(G/H)$ 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 $\{e, r^{\frac{n}{2}}\}$.

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

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

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.,

$$|\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})| = \left|(\mathbb{Z}/n\mathbb{Z})^{\times}\right|$$

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

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

Proposition 2.8 (6.3)**.** Every matrix in $\mathrm{SU}(2)$ 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 2×2 matrices with integer entries and determinant 1 is denoted $\mathrm{SL}_2(\mathbb{Z})$:

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

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

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

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)**.** $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

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 $\langle x, y \mid x^2 y^{-2}, y^4, xyx^{-1}y \rangle$.

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

□

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 $fg \neq 0$. $\square$

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 $1 + x + x^2 + \cdots = \sum_{i=0}^{\infty} x^i$. $\square$

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. $\square$

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 $\lambda : R \to \mathrm{End}_{Ab}(R)$, and the latter is isomorphic to $\mathbb{Z}$. Prove that λ is surjective.)

Proof. There exists an injective map

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

note that this map is also surjective. $\square$

Problem 3.6 (2.17). Let R be a ring, and let $E = \mathrm{End}_{Ab}(R)$ 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 α is left-multiplication by an element of R; then use Proposition [2.7])

Proof. If α 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 α is a left multiplication. Let $\varphi : \alpha \mapsto \alpha(1)$, this is injective, surjective onto its image. $\square$

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 $f_1(x), \ldots, f_r(x) \in R[x]$.

- Prove the equality of ideals

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

- Note the useful substitution trick

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

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.

(i) For $p \in K$, let $M_p = \{f \in R \mid f(p) = 0\}$. Prove that M_p is a maximal ideal in R.

(ii) Prove that if $f_1, \ldots, f_r \in R$ have no common zeros, then $(f_1, \ldots, f_r) = (1)$. (Hint: Consider $f_1^2 + \cdots + f_r^2$.)

(iii) 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 maxiaml ideal. □

Problem 3.13 (6.3). Let R be a ring, M an R-module, and $p : M \to M$ 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 $F \to \operatorname{Hom}(F, R)$ 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 directin, $M = \langle m \rangle$, 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 writting 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 $g = b_e x^e + \cdots + b_0$, 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 $\cap I_j = 0$.

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 $\varphi : M \to N$ be a homomorphism of R-modules. Prove that either $\varphi = 0$ or φ 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

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

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. □

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

Entire of chapter 4 will be included.

Problem 4.1. Let p be a prime integer, let G be a p-group, and let S be a set such that $|S| \neq 0 \mod p$. 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 τ 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

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

Recall $\mathrm{Inn}(G)$ 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 $\mathbb{F}_p$:

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

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

$$|Z(G) \cap H| \equiv 0 \mod p$$

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. 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 ≤ 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 $yx = xy^2$.

Problem 4.8. 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.

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. □

Problem 4.10. 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. Prove that 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. (Hint: Note that H is normal in G, by Exercise [II.8.2]; apply Proposition [II.8.11].) [§4.4]

Problem 4.11. Let H be a proper subgroup of a finite group G. Prove that G is not the union of the conjugates of H. (Hint: You know the number of conjugates of H; keep in mind that any two subgroups overlap, at least at the identity.)

Problem 4.12. 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 $s \in S$. (Hint: By Proposition [II.9.9], you may assume $S = G/H$, with H proper in G. Use Exercise [1.17].)

Problem 4.13. 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.

Proposition 4.8. Let $G = \mathrm{GL}_2(\mathbb{C})$, every 2×2 matrix is conjugate to an upper triangular matrix.
Warning: You need the fact that $\mathbb{C}$ is algebraically closed.

Problem 4.14. Let H, K be subgroups of a group G, with $H \subseteq N_G(K)$. Verify that the function $\gamma : H \to \mathrm{Aut}_{Grp}(K)$ 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 4.15. 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 $\gamma : G \to \mathrm{Aut}_{Grp}(H)$; by Exercise [II.4.14], $\mathrm{Aut}(H)$ has order $p-1$. What can you say about γ?)

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

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

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

Chapter 5

Irreducibility of polynomials

Chapter 6

Linear Algebra I

Problem 6.1 (6.10). Let F_1, F_2 be free R-modules of finite rank, and let α_1, resp., α_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 α_1 on F_1 and α_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.

here

Problem 6.2 (6.13). Let A be a square matrix with integer entries. Prove that if λ is a rational eigenvalue, then $\lambda \in \mathbb{Z}$.

Proof. Let $p(t) = a_0 + a_1 t + \cdots + a_n t^n$ 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 6.3 (7.3). Prove that two linear transformations of a vector space of dimension ≤ 3 are similar if and only if they have the same characteristic and minimal polynomials. Is this true in dimension 4? [§6.2]

here

Problem 6.4 (7.4). Let k be a field, and let K be a field containing k. Two square matrices $A, B \in M_n(k)$ may be viewed as matrices with entries in the larger field K. Prove that A and B are similar over k if and only if they are similar over K.

here

Proof. For the interesting direction, if A, B are similar in K: □

Problem 6.5 (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 α 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.

here

Problem 6.6 (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_α contains all the $(t - \lambda_i)$ for distinct λ_i's by Lemma 7.12. Thus P_α divides $(m_\alpha)^n$. □

Problem 6.7 (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 α 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 α is diagonalizable iff minimal polynomial m_α has no repeated roots, thus $\alpha|_W$ also has no repeated roots as it divides m_α. □

Problem 6.8 (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 6.9 (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 α and β. (Argue as in Exercise 7.13 to reduce to the case in which V is an eigenspace for α; then use Exercise 7.12.)

Proof. Separate into eigenspaces: consider eigenspace E_1 of α, then diagonalize β in E_1 (by 7.12), note that E_1 is invariant under β. □

Problem 6.10 (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 α 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 $\mathbb{R}^2$:

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

□

Chapter 7

Fields

Chapter 8

Linear Algebra II