

Abstract Algebra Exercise Solutions

2026-09-12 · Updated 2026-10-15

#Abstract Algebra #Math

Warning

The problems and solutions are only reviewed by AI and provided “as is”, without warranty of any kind, express or implied, including but not limited to the warranties of correctness of proof, fitness for a particular purpose and noninfringement.

Contents

1	Groups, Orders, and Permutation Groups	2
2	Normal Subgroups, Quotient Groups, and Commutators	9
3	Normal Subgroups and Automorphisms	16
4	Direct Products, Free Products, and Semidirect Products	21
5	Group Actions and the Sylow Theorems	24
6	Rings, Ideals, and Nilpotent Elements	26
7	Ring Homomorphisms, Polynomial Rings, and Ideals	28
8	Domains, Fields of Fractions, and Factorization	31
9	Eisenstein’s Criterion, Modules, and Finite Abelian Groups	34
10	Field Extensions and Algebraic Elements	36
11	Splitting Fields and Embeddings	38
12	Normal and Separable Extensions	40
13	Galois Theory and the Fundamental Theorem	42
14	Möbius Inversion and Finite Fields	44

1 Groups, Orders, and Permutation Groups

Problem 1.1

Prove that every subgroup of $(\mathbb{Z}, +)$ is of the form

$$m\mathbb{Z} = \{mt \mid t \in \mathbb{Z}\},$$

where $m \in \mathbb{Z}_{\geq 0}$.

Proof. Let $G \leq (\mathbb{Z}, +)$. When $G = \{0\}$, $G = 0\mathbb{Z}$. Otherwise, G contains at least one non-zero element and its inverse, which implies it contains at least one positive integer. Let $m = \min\{g \in G \mid g > 0\}$.¹

- (a) Prove $G \subseteq m\mathbb{Z}$. For any $g \in G$, if $g \notin m\mathbb{Z}$, write $g = km + r$ where $k \in \mathbb{Z}$, $r \in \mathbb{N}$ and $0 < r < m$. Then $r = g - km \in G$, contradiction.
- (b) $m\mathbb{Z} \subseteq G$ is obvious because $m \in G$ and $m\mathbb{Z} = \langle m \rangle \leq G$. ■

Problem 1.2

In a group G , let $H_1 \leq G$ and $H_2 \leq G$, and define

$$H_1 H_2 := \{h_1 h_2 \mid h_1 \in H_1, h_2 \in H_2\}.$$

Give an example showing that, in general, $H_1 H_2$ need not be a subgroup.

Proof. Let $G = S_3$ be a symmetric group, $H_1 = \langle (12) \rangle = \{e, (12)\}$, $H_2 = \langle (23) \rangle = \{e, (23)\}$. $H_1 H_2 = \{e, (12), (23), (123)\}$ ², but $(123)(12) = (13) \notin H_1 H_2$. ■

Problem 1.3

Let G be a finite group. Prove that for any two distinct elements $a, b \in G$, $o(ab) = o(ba)$.

Note that ab and ba conjugate. In fact, conjugate elements have the same order.

Proposition 1.4

Let G be a group. Prove that for any two conjugate elements $a, b \in G$, $o(ab) = o(ba)$.

Proof. Write $b = gag^{-1}$ where $g \in G$. For any positive integer n ,

$$b^n = (gag^{-1})^n = ga^n g^{-1},$$

which implies

$$b^n = e \Leftrightarrow ga^n g^{-1} = e \Leftrightarrow a^n = e. \quad \blacksquare$$

¹Well-ordering principle.

²Using the usual right-to-left composition, $(12)(23) = (123)$.

Problem 1.5

- (a) Let G be a group and let $g \in G$ be an element of finite order n . Let r be a positive integer and let $d = \gcd\{r, n\}$ be the greatest common divisor of r and n . Prove that $o(g^r) = \frac{n}{d}$.
- (b) Let G be a cyclic group of order m ($m > 1$). Determine all generators of G .

(a) *Proof.* Note that

$$(g^r)^{\frac{n}{d}} = (g^n)^{\frac{r}{d}} = e^{\frac{r}{d}} = e,$$

so $o(g^r) \mid \frac{n}{d}$. There exists $k \in \mathbb{N}^+$ such that $\frac{n}{d} = ko(g^r)$, which implies $dk \mid n$.

We shall prove $k = 1$. On the other hand,

$$e = (g^r)^{o(g^r)} = g^{\frac{rn}{dk}} \Rightarrow n \mid \frac{rn}{dk} \Rightarrow dk \mid r.$$

So dk is a common divisor of r and n . Given $d = \gcd\{r, n\}$, $dk \mid d$. Hence $k = 1$. ■

- (b) Let $G = \langle g \rangle = \{e, g, g^2, \dots, g^{m-1}\}$, $r \in \{1, 2, \dots, m-1\}$. We prove the following are equivalent:
- (1) g^r generates G ;
 - (2) $o(g^r) = m$;
 - (3) $\gcd\{r, m\} = 1$.

Proof. (1) $\Leftrightarrow$ (2) is trivial. (2) $\Leftrightarrow$ (3) is a special case of (a). ■

Problem 1.6

Let G be a group of order 10. Prove that G contains at most 4 nontrivial elements of order 5.

Proof. If there is no element of order 5, we are done. Otherwise choose $g \in G$ of order 5. By [Problem 1.5](#), g^2, g^3, g^4 are order 5 elements since their exponents are coprime to 5. The order of g ensures that g, g^2, g^3, g^4 are distinct.

If there is another element $h \in G \setminus \langle g \rangle$ of order 5, then h, h^2, h^3, h^4 also are distinct elements of order 5. Observe that $\{g, g^2, g^3, g^4\} \cap \{h, h^2, h^3, h^4\} = \emptyset$.³

Now we have identified 9 distinct elements in G : $\{e, g, \dots, g^4, h, \dots, h^4\}$. Let x denote the remaining one. We wish to derive a contradiction by questioning its order. Recall $o(x) \mid o(G) = 10$.

- (i) $o(x) = 1$ is definitely impossible.
- (ii) $o(x) = 2$, in which case $gh = hg = x$.⁴ It follows that

$$e = g^5 h^5 = (gh)^5 = x^5 = x,$$

contradicting the choice of x .

- (iii) $o(x) = 5$ makes G contain x^2, x^3, x^4 that are disjoint from $\langle g \rangle$ and $\langle h \rangle$. So you get at least $1 + 4 + 4 + 4 = 13$ elements.
- (iv) $o(x) = 10$. In $G = \langle x \rangle$, the four elements x^2, x^4, x^6, x^8 form the unique subgroup of order 5.⁵ Thus if g is one of them, then h must also lie in $\langle g \rangle$, contradicting the choice of h .

³Otherwise one could deduce $h \in \{g, g^2, g^3, g^4\}$.

⁴Verified through elimination: it always leads to contradiction if gh is equal to any other element in G . Same for hg .

⁵By [Problem 1.5](#).

Therefore, all order-5 elements lie in $\langle g \rangle$, which has exactly four nontrivial elements. ■

Problem 1.7

Let $\mathbb{R}$ denote the set of real numbers and let $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. For any $a \in \mathbb{R}^*$ and $b \in \mathbb{R}$, define a map $f_{a,b} : \mathbb{R} \rightarrow \mathbb{R}$ as follows:

$$f_{a,b}(x) = ax + b, \forall x \in \mathbb{R}.$$

Let $G = \{f_{a,b} \mid a \in \mathbb{R}^*, b \in \mathbb{R}\}$ be the set of all such maps.

- (a) Prove that G forms a group under composition of maps.
- (b) Find the center of G .

(a) *Proof.* Composition of maps is associative. For every $f_{a,b}, f_{c,d} \in G$:

$$(f_{a,b} \circ f_{c,d})(x) = a(cx + d) + b = acx + ad + b = f_{ac, ad+b}(x) \in G,$$

so G is closed under multiplication. Clearly, $f_{1,0}$ is the identity of G , and $f_{a,b}^{-1} = f_{\frac{1}{a}, -\frac{b}{a}}$. ■

(b) *Solution.* For every $f_{\alpha,\beta} \in Z(G)$:

$$\forall f_{a,b} \in G, \forall x \in \mathbb{R}, f_{\alpha,\beta} f_{a,b}(x) = f_{a,b} f_{\alpha,\beta}(x).$$

By definition of $f_{a,b}$:

$$\begin{aligned} \alpha(ax + b) + \beta &= a(\alpha x + \beta) + b \\ \beta a + (1 - \alpha)b &= \beta, \quad \forall a \in \mathbb{R}^*, b \in \mathbb{R}. \end{aligned}$$

Hence $\alpha = 1, \beta = 0$. G has a trivial center $\{f_{1,0}\}$.

Problem 1.8

Let

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

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

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Proof. Clearly, $\text{SL}_2(\mathbb{Z})$ forms a group under matrix multiplication with identity I_2 . It suffices to prove that, by multiplying $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ by finitely many T, S, T^{-1} , we can always reduce it to I_2 .

We use the notation $A \xrightarrow{P} B$ to denote $PA = B$.

When $c \neq 0$, write $a = kc + r$ where $k \in \mathbb{Z}, 0 \leq r < |c|$. Do the following transformation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \xrightarrow{T^{-k}} \begin{pmatrix} r & * \\ c & * \end{pmatrix} \xrightarrow{S} \begin{pmatrix} c & * \\ -r & * \end{pmatrix}$$

finitely many times to reduce c to 0.⁶

1 Groups, Orders, and Permutation Groups

When $c = 0$, A has the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix}$ since $\det A = 1$. Then we can further reduce it to I_2 :

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \xrightarrow{T^{-b}} I_2;$$

$$\begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} \xrightarrow{T^b} -I_2 \xrightarrow{S^2} I_2.$$

■

Problem 1.9

Compute the cycle decomposition of $\sigma = (1357)(2345)(567) \in S_7$.

Solution.

$$\begin{aligned} 1 &\rightarrow 1 \rightarrow 1 \rightarrow 3 \\ 3 &\rightarrow 3 \rightarrow 4 \rightarrow 4 \\ 4 &\rightarrow 4 \rightarrow 5 \rightarrow 7 \\ 7 &\rightarrow 5 \rightarrow 2 \rightarrow 2 \\ 2 &\rightarrow 2 \rightarrow 3 \rightarrow 5 \\ 5 &\rightarrow 6 \rightarrow 6 \rightarrow 6 \\ 6 &\rightarrow 7 \rightarrow 7 \rightarrow 1 \end{aligned}$$

$$(1357)(2345)(567) = (1347256).$$

Problem 1.10

Let $\sigma \in S_n$ ($n > 2$). Write σ as a product of finitely many disjoint cycles $\sigma_1, \sigma_2, \dots, \sigma_k$ where σ_i has length r_i . Find the order of σ .

Lemma 1.11

Let $\sigma_1, \sigma_2, \dots, \sigma_k$ ($k \geq 2$) be disjoint cycles in S_n , then $\langle \sigma_1 \rangle \cap \langle \sigma_2, \dots, \sigma_k \rangle = \{e\}$.

Proof. Let

$$\sigma = \sigma_1^{a_1} = \prod_{i=2}^k \sigma_i^{a_i}, a_i \in \mathbb{Z} \text{ for each } 1 \leq i \leq k.$$

We shall prove $\sigma = e$. If $\sigma_1 = e$, we are done. Otherwise, take $x \in \text{supp}(\sigma_1)$, then $x \notin \text{supp}(\sigma_i)$ for each $2 \leq i \leq k$, which implies $\sigma_i^{a_i}(x) = x$. Therefore

⁶This process terminates because the absolute value of the lower-left entry strictly decreases. It is essentially the Euclidean algorithm on the first column.

$$\begin{aligned}
\sigma_1^{a_1}(x) &= \left(\prod_{i=2}^k \sigma_i^{a_i} \right) (x) \\
&= \left(\prod_{i=2}^{k-1} \sigma_i^{a_i} \right) (\sigma_k^{a_k}(x)) \\
&= \left(\prod_{i=2}^{k-1} \sigma_i^{a_i} \right) (x) \\
&= \dots \\
&= \sigma_2^{a_2}(x) = x.
\end{aligned}$$

Let r be the length of σ_1 , since σ_1 is a cycle, $r \mid a_1$. Note that $o(\sigma_1) = r$, so $\sigma = \sigma_1^{a_1} = e$. ■

Proposition 1.12

Let $\sigma_1, \sigma_2, \dots, \sigma_k$ be disjoint cycles in S_n , then

$$G = \prod_{i=1}^k \langle \sigma_i \rangle$$

is a direct product.

Proof. Every element of $\langle \sigma_i \rangle$ commutes with every element of $\langle \sigma_j \rangle$ since disjoint cycles commute. For each i ,

$$\begin{aligned}
\langle \sigma_i \rangle \cap \langle \sigma_1 \rangle \cdots \langle \sigma_{i-1} \rangle \langle \sigma_{i+1} \rangle \cdots \langle \sigma_k \rangle &= \langle \sigma_i \rangle \cap \langle \sigma_1, \dots, \sigma_{i-1}, \sigma_{i+1}, \dots, \sigma_k \rangle \\
&= \{e\}
\end{aligned}$$

by [Lemma 1.11](#). ■

Hence

$$o(\sigma) = \text{lcm}\{o(\sigma_1), \dots, o(\sigma_k)\} = \text{lcm}\{r_1, \dots, r_k\}.$$

Problem 1.13

Let $n > 2$.

- (a) Let r denote the transformation of D_n that sends the vertex pair $(1, 2)$ to $(2, 3)$, and let s denote the transformation that sends $(1, 2)$ to $(2, 1)$. Prove that

$$D_n = \langle r, s \mid r^n = s^2 = rsrs = e \rangle.$$

- (b) Find all elements of order 2 and all elements of order n in D_n .

- (a) *Proof.* According to geometry, rotations of a regular n -gon are r^i ($1 \leq i \leq n-1$) and reflections are $r^i s$ ($0 \leq i \leq n-1$), hence

$$D_n = \{e, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\}.$$

Obviously, $r^n = s^2 = e$ and $rsrs = r^{-1}$, which implies $rsrs = e$. ■

- (b) *Solution.* Elements of order n are rotations r^i ($1 \leq i \leq n-1$) where $\gcd\{n, i\} = 1$.⁷ Elements of order 2 are all reflections: $r^i s$ ($0 \leq i \leq n-1$) and the 180° rotation $r^{\frac{n}{2}}$ when n is even.

Problem 1.14

Find the number of permutations of order 6 in S_8 .

Solution.

- (i) Permutations of type $[1^3 2^1 3^1]$: $\frac{8!}{3! \cdot 2! \cdot 3} = 1120$;
- (ii) Permutations of type $[1^1 2^2 3^1]$: $\frac{8!}{2^2 \cdot 2! \cdot 3} = 1680$;
- (iii) Permutations of type $[2^1 3^2]$: $\frac{8!}{2 \cdot 3^2 \cdot 2!} = 1120$;
- (iv) Permutations of type $[1^2 6^1]$: $\frac{8!}{2! \cdot 6} = 3360$;
- (v) Permutations of type $[2^1 6^1]$: $\frac{8!}{2 \cdot 6} = 3360$.

Hence there are 10640 permutations of order 6.

Problem 1.15

Let $\sigma \in S_n$. Write σ as a product of finitely many disjoint nontrivial cycles, and let $c(\sigma)$ be the sum of the number of these cycles and the number of fixed points of σ .

- (a) Prove that σ is an even permutation if and only if $n - c(\sigma)$ is even.
- (b) Let τ be a transposition. Prove that

$$c(\sigma\tau) = c(\sigma) + 1 \quad \text{or} \quad c(\sigma\tau) = c(\sigma) - 1,$$

and explain when each of the two cases above occurs.

- (c) Prove that the minimum number of transpositions needed to express σ as a product of transpositions is $n - c(\sigma)$.

- (a) *Proof.* Write $\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$ where σ_i has length $r_i \geq 2$. By definition,

$$k + (n - r_1 - r_2 - \cdots - r_k) = c(\sigma).$$

So σ is an even permutation if and only if

$$(r_1 - 1) + (r_2 - 1) + \cdots + (r_k - 1) = r_1 + r_2 + \cdots + r_k - k = n - c(\sigma)$$

is even. ■

- (b) *Proof.* Write

$$\sigma_i = (a_{i1} a_{i2} \cdots a_{ir_i}), 1 \leq i \leq k.$$

Let $\tau = (a, b)$. Since σ_i and σ_j are disjoint for all $i \neq j$, there are only four cases for the relation between τ and the cycles σ_i .⁸

Case I: τ is disjoint from all σ_i , then $\sigma\tau = \sigma_1 \cdots \sigma_k \tau$ (disjoint nontrivial cycles), so $\sigma\tau$ gets an additional cycle τ while losing two fixed points a and b , thus $c(\sigma\tau) = c(\sigma) - 1$.

⁷By [Problem 1.5](#).

⁸If we allow trivial cycles (fixed points) in the product representation of σ , there would be only two cases: either τ splits a cycle or τ merges two cycles.

The original problem handles nontrivial cycles and fixed points separately.

Case II: τ is contained in one σ_i and disjoint from any other $\sigma_j (j \neq i)$, i.e. there exists $1 \leq p \neq q \leq r_i$ such that $a_{ip} = a$ and $a_{iq} = b$.

For simplicity, we only consider $p + 1 < q < r_i$. Compute

$$\begin{aligned}\sigma_i \tau &= (a_{i1} a_{i2} \cdots a_{ir_i}) (a_{ip} a_{iq}) \\ &= (a_{ip} a_{i,q+1} a_{i,q+2} \cdots a_{ir_i} a_{i1} a_{i2} \cdots a_{i,p-1}) (a_{i,p+1} a_{i,p+2} \cdots a_{iq}).\end{aligned}$$

Hence $\sigma_i \tau$ can be expressed as two disjoint nontrivial cycles that are also disjoint from any other $\sigma_j (j \neq i)$. Since disjoint cycles commute,

$$\sigma \tau = \sigma_1 \sigma_2 \cdots \sigma_k \tau = \sigma_1 \cdots \sigma_{i-1} (\sigma_i \tau) \sigma_{i+1} \cdots \sigma_k,$$

so $\sigma \tau$ gets one additional cycle with fixed points unchanged, hence $c(\sigma \tau) = c(\sigma) + 1$.

Similarly, one can compute $\sigma_i \tau$ under other conditions of p and q , and $c(\sigma \tau) = c(\sigma) + 1$ still holds.

Case III: one endpoint of τ lies in σ_i and the other lies in $\sigma_j (i \neq j)$. Similarly, one can prove $\sigma \tau$ loses one cycle with fixed points unchanged, hence $c(\sigma \tau) = c(\sigma) - 1$.

Case IV: one endpoint of τ lies in σ_i and the other is a fixed point of σ . Similarly, this case also gives $c(\sigma \tau) = c(\sigma) - 1$. ■

- (c) *Proof.* Note that $c(e) = n$, and $c(x)$ changes by ± 1 each time we multiply x by a transposition. So the minimum number of transpositions needed to express σ as a product of transpositions is no less than $n - c(\sigma)$.

On the other hand, write

$$\sigma = \prod_{i=1}^k \sigma_i = \prod_{i=1}^k \prod_{j=1}^{r_i-1} (a_{ij} a_{i,j+1}),$$

there are exactly

$$r_1 + r_2 + \cdots + r_k - k = n - c(\sigma)$$

transpositions. ■

2 Normal Subgroups, Quotient Groups, and Commutators

Problem 2.1

Let G be a group and let $A \trianglelefteq G$. Define

$$[A, G] = \langle a^{-1}g^{-1}ag \mid a \in A, g \in G \rangle.$$

Prove that $[A, G] \trianglelefteq G$.

Proof. For every $a^{-1}g^{-1}ag \in [A, G]$ and $g' \in G$, $g'^{-1}ag' \in A$ because $A \trianglelefteq G$. Hence

$$\begin{aligned} & g'^{-1}a^{-1}g^{-1}agg' \\ &= (g'^{-1}a^{-1}g')(g'^{-1}g^{-1}g')(g'^{-1}ag')(g'^{-1}gg') \\ &= (g'^{-1}ag')^{-1}(g'^{-1}gg')^{-1}(g'^{-1}ag')(g'^{-1}gg') \\ &= [g'^{-1}ag', g'^{-1}gg'] \in [A, G]. \end{aligned}$$

■

Problem 2.2

Let $D_n = \langle r, s \mid r^n = s^2 = rsrs = e \rangle$ be the dihedral group ($n \geq 3$). Prove the following statements:

- (a) If n is odd, then $[D_n, D_n] = \langle r \rangle = \langle r^2 \rangle$;
- (b) If n is even, then $[D_n, D_n] = \langle r^2 \rangle$.

Proof. $D_n / \langle r \rangle = \{\bar{e}, \bar{s}\}$ is abelian, so $[D_n, D_n] \subseteq \langle r \rangle$.⁹ Furthermore, we have $\langle r^2 \rangle \subseteq [D_n, D_n] \subseteq \langle r \rangle$ because $r^2 = (srs)^{-1}r = s^{-1}r^{-1}sr = [s, r] \in [D_n, D_n]$.

- (a) If n is odd, $\langle r \rangle = \langle r^2 \rangle$, so $\langle r^2 \rangle = [D_n, D_n] = \langle r \rangle$;
- (b) If n is even, $D_n / \langle r^2 \rangle = \{\bar{e}, \bar{r}, \bar{s}, \bar{rs}\} \cong C_2 \times C_2$ is abelian, hence $[D_n, D_n] \subseteq \langle r^2 \rangle$, then $[D_n, D_n] = \langle r^2 \rangle$.

■

Problem 2.3

Let S be a set of representatives of left cosets of a subgroup $H \leq G$, i.e. $G = \bigsqcup_{a \in S} aH$. Prove that S^{-1} is a set of representatives of right cosets of H , i.e. $G = \bigsqcup_{a' \in S^{-1}} Ha'$.

Proof.

$$G = G^{-1} = \bigsqcup_{a \in S} (aH)^{-1} = \bigsqcup_{a \in S} H^{-1}a^{-1} = \bigsqcup_{a \in S} Ha^{-1} = \bigsqcup_{a' \in S^{-1}} Ha'.$$

■

Problem 2.4

Let G be a group and let $N \trianglelefteq G$. If G/N is finite and $|G/N| = n$, prove that $a^n \in N$ for every $a \in G$.

Proof. Note that $aN \in G/N$ and $o(aN) \mid |G/N| = n$, so $(aN)^n = a^nN = N$, which implies $a^n \in N$.

■

⁹Recall that $[G, G]$ is the $\subseteq$ -minimum of all $N \trianglelefteq G$ such that H/N is abelian.

Problem 2.5

Let G be a finite group and let $K \trianglelefteq H \trianglelefteq G$. If $\gcd\{|K|, |H/K|\} = 1$, prove that $K \trianglelefteq G$.

Proof. For every $g \in G$, we shall prove $K = g^{-1}Kg$. Clearly, $|K| = |g^{-1}Kg|$.¹⁰ It suffices to prove $g^{-1}Kg \subseteq K$.

For every $g^{-1}kg \in g^{-1}Kg$, there exists $h \in H$ such that $kg = gh$ since $k \in H \trianglelefteq G$. So $g^{-1}kg = g^{-1}gh = h \in H$, which implies $g^{-1}Kg \leq H$.

Furthermore, for every $h \in H$, there exists $h' \in H$ such that $gh = h'g$, so $h^{-1}g^{-1}Kgh = (gh)^{-1}K(gh) = (h'g)^{-1}Kh'g = g^{-1}h'^{-1}Kh'g = g^{-1}Kg$, which implies $g^{-1}Kg \trianglelefteq H$.

Therefore, $K(g^{-1}Kg)$ is normal in H , and K is normal in $K(g^{-1}Kg)$.¹¹ So we have

$$|K(g^{-1}Kg)| \mid |H| \Rightarrow \frac{|K(g^{-1}Kg)|}{|K|} \mid \frac{|H|}{|K|}.$$

On the other hand,

$$|K(g^{-1}Kg)| = \frac{|K| \cdot |g^{-1}Kg|}{|K \cap g^{-1}Kg|} = \frac{|K|^2}{|K \cap g^{-1}Kg|},$$

thus

$$\frac{|K(g^{-1}Kg)|}{|K|} = \frac{|K|}{|K \cap g^{-1}Kg|} \Rightarrow \frac{|K(g^{-1}Kg)|}{|K|} \mid |K|.$$

So $\frac{|K(g^{-1}Kg)|}{|K|}$ is a common divisor of $|K|$ and $\frac{|H|}{|K|}$. Given

$$\gcd\left\{|K|, \frac{|H|}{|K|}\right\} = \gcd\{|K|, |H/K|\} = 1,$$

then $|K(g^{-1}Kg)| = |K|$, hence $K = K(g^{-1}Kg)$ because $K \subseteq K(g^{-1}Kg)$, which implies $g^{-1}Kg \subseteq K$. ■

⚠ Caution

One may want to do something with the normality of $K \cap (g^{-1}Kg)$, but the division

$$\frac{|K \cap (g^{-1}Kg)|}{|K|} \mid \frac{|H|}{|K|}$$

is invalid.

Problem 2.6

Prove the following statements.

- (a) For every positive integer n , $\langle \frac{1}{n} + \mathbb{Z} \rangle$ is the unique subgroup of $\mathbb{Q}/\mathbb{Z}$ of order n .

¹⁰One can consider the bijection $\varphi : k \mapsto g^{-1}kg$.

¹¹Recall that if $H \trianglelefteq G$ and $K \leq G$, then $H \trianglelefteq HK \leq G$; When $K \trianglelefteq G$, HK is also normal in G .

(b) Every subgroup of $\mathbb{Q}/\mathbb{Z}$ generated by finitely many elements is cyclic.

(a) *Proof.* Let G be a subgroup of $\mathbb{Q}/\mathbb{Z}$ of order n . For each $\bar{q} \in G$, if $q = 0$, then $\bar{q} \in \langle \frac{1}{n} + \mathbb{Z} \rangle$. Otherwise, write $q = \frac{a}{b} \neq 0$ with $a \in \mathbb{Z}^*$, $b \in \mathbb{N}^+$. Since $o(\bar{q}) \mid n$,

$$n\bar{q} = \overline{\left(\frac{na}{b}\right)} = \bar{0} \Rightarrow \frac{na}{b} \in \mathbb{Z}.$$

Thus

$$\bar{q} = \overline{\left(\frac{1}{n}\right)} \cdot \overline{\left(\frac{na}{b}\right)} = \overline{\left(\frac{na}{b}\right)} \overline{\left(\frac{1}{n}\right)} \in \langle \frac{1}{n} + \mathbb{Z} \rangle,$$

Hence $G \leq \langle \frac{1}{n} + \mathbb{Z} \rangle$ and furthermore $G = \langle \frac{1}{n} + \mathbb{Z} \rangle$ because $|G| = |\langle \frac{1}{n} + \mathbb{Z} \rangle| = n$. ■

(b) *Proof.* Let $G = \langle \bar{q}_1, \dots, \bar{q}_n \rangle$, $q_i \in \mathbb{Q}$. Write $q_i = \frac{a_i}{b_i}$, $a_i \in \mathbb{Z}$, $b_i \in \mathbb{N}^+$.

Let $m = \text{lcm}\{b_1, \dots, b_n\} \in \mathbb{N}^+$, then

$$\bar{q}_i = \overline{\left(\frac{a_i m}{b_i m}\right)} = \overline{\left(\frac{a_i m}{b_i}\right)} \overline{\left(\frac{1}{m}\right)} \in \langle \frac{1}{m} + \mathbb{Z} \rangle,$$

so $G \leq \langle \frac{1}{m} + \mathbb{Z} \rangle$ is cyclic.¹² ■

Problem 2.7

Let G be a finite group and let H be a proper subgroup of G . Subgroups of the form gHg^{-1} ($g \in G$) are called conjugates of H . Prove the following statements.

- (a) H has $[G : N_G(H)]$ conjugates.
- (b) The set of all conjugates of H cannot cover the whole group G .

(a) *Proof.* Let $x, y \in G$. Note that

$$\begin{aligned} xHx^{-1} = yHy^{-1} &\Leftrightarrow H = (y^{-1}x)^{-1}H(y^{-1}x) \\ &\Leftrightarrow y^{-1}x \in N_G(H) \\ &\Leftrightarrow xN_G(H) = yN_G(H). \end{aligned}$$

¹³ By the definition of group index, H has $[G : N_G(H)]$ distinct conjugates. ■

(b) *Proof.* If $N_G(H) = G$, H itself is the only conjugate of H , and it does not cover G because H is a proper subgroup.

Otherwise, $N_G(H)$ is a proper subgroup of G , so $|N_G(H)| < |G|$. Let S denote the set of representatives for the left cosets of $N_G(H)$ in G , then

$$K = \{gHg^{-1} \mid g \in S\}$$

is the set of conjugates of H . We shall prove $|\bigcup K| < |G|$.

Since $|gHg^{-1}| = |H|$ and each conjugate contains the identity:

¹²Recall that all subgroups of a cyclic group is cyclic.

¹³Recall that two cosets xH and yH are either disjoint or equal, and $xH = yH \Leftrightarrow xy^{-1} \in H$.

$$\begin{aligned}
 |\bigcup K| &= \left| \bigcup \left\{ e, \bigcup_{g \in S} (gHg^{-1} \setminus \{e\}) \right\} \right| \\
 &\leq 1 + \sum_{g \in S} (|gHg^{-1}| - 1) \\
 &= 1 + |S| \cdot (|H| - 1) \\
 &= 1 + \frac{|G| \cdot (|H| - 1)}{|N_G(H)|} \\
 &< \frac{|G|}{|N_G(H)|} + \frac{|G| \cdot (|H| - 1)}{|N_G(H)|} \\
 &= \frac{|G| \cdot |H|}{|N_G(H)|} \\
 &\leq |G|.
 \end{aligned}$$

■

Problem 2.8

Let G be a finite group and let H, K be subgroups of G . If

$$\gcd\{[G : H], [G : K]\} = 1,$$

prove that $G = HK$.

Proof. Recall that

$$|H \cap K| = \frac{|H| \cdot |K|}{|HK|},$$

then

$$\frac{|G|}{|H \cap K|} = \frac{|G|^2}{|H| \cdot |K|} \cdot \frac{|HK|}{|G|}.$$

Since $H \cap K \leq H \leq G$,

$$|H \cap K| \mid |H|, |H| \mid |G|,$$

so

$$\frac{|G|}{|H|} \mid \frac{|G|}{|H \cap K|}.$$

Similarly,

$$\frac{|G|}{|K|} \mid \frac{|G|}{|H \cap K|}.$$

Given

$$\gcd\{[G : H], [G : K]\} = \gcd\left\{\frac{|G|}{|H|}, \frac{|G|}{|K|}\right\} = 1,$$

we have

$$\frac{|G|^2}{|H| \cdot |K|} \mid \frac{|G|}{|H \cap K|}.$$

Hence

$$\frac{|G|}{|H \cap K|} \mid \frac{|G|^2}{|H| \cdot |K|} = \frac{|HK|}{|G|} \in \mathbb{Z} \Rightarrow |G| \mid |HK|,$$

which implies $G = HK$ because $HK \subseteq G$. ■

⚠ Caution

Recall that HK is not necessarily a subgroup, do not claim something like $H \leq HK \leq G$.

Problem 2.9

Let G be a subgroup of S_{2024} , and G contains an n -cycle, where $n \geq 4$ is even. Prove that G is not simple.

Proof. Consider the intersection $H = G \cap A_{2024} \trianglelefteq G$.¹⁴

Let $\sigma \in G$ be an n -cycle with $n \geq 4$ even, then H is proper because σ is odd, so $\sigma \notin H$. H is also nontrivial because σ^2 is even.¹⁵ ■

Problem 2.10

Find the structure of the following two subgroups of S_5 :

- (a) $\langle (12)(34), (12345) \rangle$;
- (b) $\langle (12)(35), (12345) \rangle$.

(a) *Solution.* Let $H = \langle (12)(34), (12345) \rangle$. Note that $H \leq A_5$,¹⁶ so $|H| \mid |A_5| = 60$.

Since

$$(12)(34) \in H, (12345) \in H, (12)(34)(12345) = (245) \in H,$$

we have

$$\text{lcm}\{o((12)(34)), o((12345)), o((245))\} = 30 \mid |H|.$$

Thus $|H| = 30$ or $|H| = 60$. Index 2 would force $H \trianglelefteq A_5$, impossible. Hence $H = A_5$.

(b) *Solution.* Let

$$s = (12)(35), r = (12345), G = \langle r, s \rangle.$$

Note that

$$s^2 = r^5 = rsrs = e,$$

¹⁴Normality is ensured by the isomorphic theorems.

¹⁵ $\sigma^2 \neq e$ is a product of two $\frac{n}{2}$ cycles, so it can be expressed as a product of $2 \cdot (\frac{n}{2} - 1)$ transpositions.

¹⁶The generators $(12)(34)$ and (12345) are both even.

so $G \cong D_5$.

Problem 2.11

Let $A_\infty = \bigcup_{n \geq 2} A_n$. Prove the following statements.

- (a) A_∞ has a natural group structure such that $A_n < A_\infty$ for every $n \geq 2$.
- (b) A_∞ is simple.

- (a) *Proof.* For every $x \in A_\infty$, let N_x denote the nonempty set $\{n \in \mathbb{N}^+ \mid x \in A_n\}$ because x belongs to at least one A_n , and let $n(x) = \min N_x$. Define the inverse of x to be x^{-1} in $A_{n(x)}$.

For every $x, y \in A_\infty$, define the product $x \cdot y$ to be xy in $A_{\max\{n(x), n(y)\}}$.

Clearly, A_∞ forms a group under these operations with identity (1). And there is an infinite chain of proper subgroups:

$$A_2 < A_3 < \cdots < A_n < \cdots < A_\infty. \quad \blacksquare$$

- (b) *Proof.* Let N be a normal subgroup of A_∞ . We shall prove $N = \{e\}$ or $N = A_\infty$.

For each $n \geq 5$, consider the intersection $N \cap A_n \trianglelefteq A_n$.¹⁷ Because of the simplicity of A_n , either $N \cap A_n = \{e\}$ or $N \cap A_n = A_n$.

If $N \cap A_5 = \{e\}$, we actually have

$$N \cap A_n = \{e\} \text{ for each } n \geq 5,$$

¹⁸ so

$$N = N \cap A_\infty = N \cap \left(\bigcup_{n=5}^{\infty} A_n \right) = \bigcup_{n=5}^{\infty} (N \cap A_n) = \{e\}.$$

Similarly, if $N \cap A_5 = A_5$, we have

$$N \cap A_n = A_n \text{ for each } n \geq 5,$$

so

$$N = N \cap A_\infty = N \cap \left(\bigcup_{n=5}^{\infty} A_n \right) = \bigcup_{n=5}^{\infty} (N \cap A_n) = \bigcup_{n=5}^{\infty} A_n = A_\infty. \quad \blacksquare$$

Problem 2.12

Let $n \geq 2$ be a positive integer.

- (a) Let $G_n = [S_n, S_n]$. Prove that $G_n = A_n$ for $n \geq 3$.
- (b) Find $[A_n, A_n]$.

- (a) *Proof.* Since $S_n/A_n \cong C_2$ is abelian, $G_n = [S_n, S_n] \subseteq A_n$. For each $3 \leq i \leq n$,

$$[(12), (1i)] = (12)^{-1}(1i)^{-1}(12)(1i) = (12i) \in G_n,$$

¹⁷ $N \trianglelefteq A_\infty$ and $A_n \leq A_\infty$.

¹⁸ If there exists $n > 5$ such that $N \cap A_n = A_n$, then $A_5 \subseteq A_n \subseteq N$, contradicting to $N \cap A_5 = \{e\}$.

so G_n contains all the generators of A_n ¹⁹, then $A_n \subseteq G_n$. Hence $G_n = A_n$. ■

(b) *Solution.*

(i) If $n \leq 3$, A_n is abelian, then $[A_n, A_n] = \{e\}$.

(ii) If $n \geq 5$, A_n is simple, so $[A_n, A_n] = \{e\}$ or $[A_n, A_n] = A_n$. Compute

$$[(123), (124)] = (123)^{-1}(124)^{-1}(123)(124) = (12)(34) \in [A_n, A_n],$$

so $[A_n, A_n] = A_n$.

(iii) If $n = 4$, V_4 is normal in A_4 and $A_4/V_4 \cong C_3$ is abelian, so $[A_4, A_4] \subseteq V_4$.²⁰

Also compute $[(123), (134)] = (14)(23) \in [A_4, A_4]$, so $V_4 = \langle (12)(34), (14)(23) \rangle \subseteq [A_4, A_4]$.

Therefore, $[A_4, A_4] = V_4$.

¹⁹Recall that $A_n = \langle (123), (124), \dots, (12n) \rangle$.

²⁰Recall that $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ which is isomorphic to $\langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle$.

3 Normal Subgroups and Automorphisms

Problem 3.1

- (a) Let N be a normal subgroup of A_4 that contains a 3-cycle. Prove that $N = A_4$.
 (b) Find all normal subgroups of A_4 .

(a) *Proof.* Since $3 \mid |N|$ and $|N| \mid |A_4| = 12$, $|N| \in \{3, 6, 12\}$.

- (i) If $|N| = 12$, we are done.
 (ii) If $|N| = 3$, $N = \langle \sigma \rangle$ where $\sigma = (abc)$. Let $\{d\} = \{1, 2, 3, 4\} \setminus \{a, b, c\}$ and let $\tau = (adb) \in A_4$. Compute

$$\tau\sigma\tau^{-1} = (\tau(a)\tau(b)\tau(c)) = (dac) \notin N,$$

contradicting the normality of N .

- (iii) If $|N| = 6$, $A_4/N \cong C_2$ is abelian, so $V_4 = [A_4, A_4] \leq N$. But $|V_4| = 4 \nmid 6$, contradiction. ■

(b) *Solution.* Let $N \trianglelefteq A_4$, then $|N| \in \{1, 2, 3, 6, 12\}$. $|N| = 1$ and $|N| = 12$ are trivial cases, and we have proved $|N| = 3$ and $|N| = 6$ are impossible.

- (i) If $|N| = 2$, then $N = \langle (ab)(cd) \rangle$, but

$$(abc)(ab)(cd)(abc)^{-1} = (ad)(bc) \notin N,$$

contradiction.

- (ii) If $|N| = 4$, $A_4/N \cong C_3$ is abelian, so $V_4 = [A_4, A_4] \leq N$, which implies $N = V_4$.

In conclusion, normal subgroups of A_4 are $\{e\}$, V_4 , A_4 .

Problem 3.2

Find all normal subgroups of S_n ($n \geq 1$).

Lemma 3.3

If G is a group with trivial center, then it cannot have a normal subgroup of order 2.

Proof. Let $N \trianglelefteq G$ and $|N| = 2$, then $N = \{e, x\}$ with $x^2 = e$.

For every $g \in G$,

$$gNg^{-1} = \{e, gxg^{-1}\} = N = \{e, x\} \Rightarrow gxg^{-1} = x$$

by the normality of N .

This implies

$$x \in Z(G) \Rightarrow x = e \Rightarrow N = \{e\},$$

contradiction. ■

Solution of Problem 3.2.

- (i) $n = 1$: $\{e\}$.

3 Normal Subgroups and Automorphisms

- (ii) $n = 2$: $\{e\}, S_2$.
 - (iii) $n = 3$: $\{e\}, A_3, S_3$.
 - (iv) $n = 4$: $\{e\}, V_4, A_4, S_4$.
 - (v) $n \geq 5$: Let $N \leq S_n$. Consider the intersection $H = N \cap A_n \trianglelefteq A_n$, then $H = \{e\}$ or $H = A_n$ since A_n is simple.
- (1) $H = \{e\}$ implies every nontrivial permutation in N is odd. Let $\varphi : N \rightarrow S_n/A_n$ defined as $g \mapsto gA_n$, $\text{Ker } \varphi = N \cap A_n = \{e\}$, so

$$|N| = |\text{Im}(\varphi)| \leq |S_n/A_n| = 2.$$

Recall that S_n has trivial center when $n \geq 3$. By [Lemma 3.3](#), $N = \{e\}$.

- (2) $H = A_n$ implies $A_n \leq N$. But A_n is already the maximal proper subgroup of S_n , so $N = A_n$ or $N = S_n$.

Hence there are three normal subgroups: $\{e\}, A_n, S_n$.

Problem 3.4

For $n \geq 2$, determine all integers i with $2 \leq i \leq n$ such that $S_n = \langle (1i), (12\cdots n) \rangle$.

Solution. The indices in our solution should wrap around 1 and n .

Note that

$$(12\cdots n)^k (1i) (12\cdots n)^{-k} = (1+k, 1+k+i-1),$$

so we can get transpositions of the form $(a, a+i-1)$ by conjugations of the two generators.

Let $G = (V, E)$ be an undirected graph with $V = \{1, 2, \dots, n\}$ and $E = \{(a, a+i-1) \mid 1 \leq a \leq n\}$. The connected components of G are cosets of $\langle i-1 \rangle$ in $\mathbb{Z}/n\mathbb{Z}$, hence

$$\begin{aligned} (1i) \text{ and } (12\cdots n) \text{ generates } S_n &\Leftrightarrow G \text{ is connected} \\ &\Leftrightarrow \langle i-1 \rangle = \mathbb{Z}/n\mathbb{Z} \\ &\Leftrightarrow \gcd\{n, i-1\} = 1. \end{aligned}$$

Problem 3.5

Let n be a positive integer. Prove that $\sigma, \tau \in S_n$ are conjugate if and only if they have the same type.

Proof. Recall that

$$g(a_1 a_2 \cdots a_k) g^{-1} = (g(a_1) g(a_2) \cdots g(a_k)), \forall g \in S_n,$$

so conjugation of permutations preserves the cycle type. It remains to prove the converse.

Let $\sigma, \tau \in S_n$ with the same type. Decompose them into disjoint cycles (including trivial ones):

$$\sigma = \prod_{i=1}^k \sigma_i = \prod_{i=1}^k (a_{i1} a_{i2} \cdots a_{ir_i}), \tau = \prod_{i=1}^k \tau_i = \prod_{i=1}^k (b_{i1} b_{i2} \cdots b_{ir_i}).$$

Define $\pi : a_{ij} \mapsto b_{ij}$, then $\pi \in S_n$ and $\pi \sigma \pi^{-1} = \tau$. ■

Problem 3.6

Let $f : G \rightarrow H$ be a group homomorphism and let $a \in G$ be an element of finite order. Prove that the order of $f(a)$ divides the order of a .

Proof.

$$(f(a))^{o(a)} = f(a^{o(a)}) = f(e) = e \Rightarrow o(f(a)) \mid o(a). \quad \blacksquare$$

Problem 3.7

Let G be a group and define $f : G \rightarrow G$ to be the map $x \mapsto x^{-1}$.

- (a) Give a necessary and sufficient condition for f to be a group homomorphism.
- (b) If G is finite and $|\text{Aut}(G)| = 1$, prove that $|G| \leq 2$.

(a) *Solution.*

$$\begin{aligned} f \text{ is a group homomorphism} &\Leftrightarrow \forall a, b \in G, f(a)f(b) = f(ab) \\ &\Leftrightarrow \forall a, b \in G, a^{-1}b^{-1} = (ab)^{-1} = b^{-1}a^{-1} \\ &\Leftrightarrow G \text{ is abelian, equivalently } Z(G) = G. \end{aligned}$$

(b) *Proof.* Since $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$ and $|\text{Aut}(G)| = 1$, $|\text{Inn}(G)| = 1$.

Consider the homomorphism $\varphi : g \mapsto \theta_g = (x \mapsto gxg^{-1})$, then²¹

$$G/Z(G) \cong \text{Inn}(G) \Rightarrow \frac{|G|}{|Z(G)|} = |\text{Inn}(G)| = 1 \Rightarrow G = Z(G),$$

which makes f a homomorphism. Furthermore, $f \in \text{Aut}(G)$, so $f = \text{id}$. We have

$$x = x^{-1} \text{ for each } x \in G$$

and every element has order at most 2.

If $|G| > 2$, then $G \cong (\mathbb{Z}/2\mathbb{Z})^d$, $d \geq 2$. Clearly, such a group has nontrivial automorphisms,²² contradiction. ■

Problem 3.8

Let G be a group with trivial center, prove that $\text{Aut}(G)$ also has trivial center.

Proof. For every $\sigma \in Z(\text{Aut}(G))$ and $x \in G$, let $\theta_x \in \text{Aut}(G)$ denote the conjugation induced by x , i.e. $\theta_x : g \mapsto xgx^{-1}$.

Note that $\sigma\theta_x = \theta_{\sigma(x)}\sigma$, we have

$$\sigma\theta_x = \theta_{\sigma(x)}\sigma = \theta_x\sigma \Rightarrow \theta_x = \theta_{\sigma(x)}$$

since σ commutes with θ_x .

By injectivity of $g \mapsto \theta_g$,²³

²¹Recall that $\text{Ker } \varphi = Z(G)$ and $\text{Im } \varphi = \text{Inn}(G)$.

²²e.g. swap two basis vectors.

$$\theta_x = \theta_{\sigma(x)} \Rightarrow \sigma(x) = x \Rightarrow \sigma = \text{id}.$$

Hence $\text{Aut}(G)$ has trivial center. ■

Problem 3.9

Let G be a finite group such that $|G| = p_1 p_2 \cdots p_s$, where the p_i are distinct primes. If G has n normal subgroups, prove that $n \leq 2^s$.

Note that $|G|$ has exactly 2^s positive divisors, so there would be two distinct normal subgroups sharing the same order if $n > 2^s$. If we can prove “identical orders imply identical groups”, then we are done.

Lemma 3.10

Let G be a finite group such that $|G| = p_1 p_2 \cdots p_s$, where the p_i are distinct primes. If N_1 and N_2 are normal subgroups of G with the same order m , then $N_1 = N_2$.

Proof. By induction on s . When $s = 1$, G is cyclic with prime order, so either $N_1 = N_2 = \{e\}$ or $N_1 = N_2 = G$.

Next, we assume the lemma holds for $1, 2, \dots, s - 1$.

- (i) If $m = 1$, $N_1 = N_2 = \{e\}$.
- (ii) If $m \geq 2$ and $N_1 N_2 = G$, we have

$$|G| = |N_1 N_2| = \frac{|N_1| |N_2|}{|N_1 \cap N_2|} = \frac{m^2}{|N_1 \cap N_2|}$$

which forces $|N_1 \cap N_2| = m$ because $|G|$ is squarefree. Thus $N_1 \cap N_2 = N_1 = N_2$.

- (iii) If $m \geq 2$ and $N_1 N_2 < G$, since N_1 and N_2 normal in $N_1 N_2$ with the same order, and $|N_1 N_2|$ is a product of k distinct primes ($1 \leq k \leq s - 1$), we have $N_1 = N_2$ by the induction hypothesis. ■

Problem 3.11

For $n \geq 3$, find $|\text{Aut}(D_n)|$.

Problem 3.12

Let $\varphi : S_n \rightarrow S_n$ be an automorphism of the symmetric group S_n , and suppose $n \neq 6$. Prove the following.

- (a) φ sends transpositions in S_n to transpositions.
- (b) $\text{Aut}(S_n) \cong S_n$.

²³The kernel $Z(G)$ is trivial.

Problem 3.13

Let G be a finite group and let $f : G \rightarrow G$ be a group homomorphism. Prove that there exists a positive integer N such that $G = \text{Ker}(f^N) \cup \text{Im}(f^N)$ and $\text{Ker}(f^N) \cap \text{Im}(f^N) = \{e\}$.

Problem 3.14

Let G and H be finite groups. Solve the following problems.

(a) For every $N \trianglelefteq G$, if $G/N \cong H$, prove that there are exactly $|\text{Aut}(H)|$ surjective homomorphisms $f : G \twoheadrightarrow H$ satisfying $\text{Ker } f = N$.

(b) Hence prove that $|\{f : G \twoheadrightarrow H \mid f \text{ is a group homomorphism}\}| = |\text{Aut}(H)| \cdot |\{N \trianglelefteq G \mid G/N \cong H\}|$.

4 Direct Products, Free Products, and Semidirect Products

Problem 4.1

Let $n > 1$. If n is odd, prove that $D_{2n} \cong D_n \times \mathbb{Z}_2$. Show that this conclusion fails when n is even.

Problem 4.2

Determine whether each of the following statements is true, and explain your reasoning.

- $D_n \cong \mathbb{Z}_n \times \mathbb{Z}_2$.
- $S_n \cong A_n \times \mathbb{Z}_2$.
- $\text{GL}_2(\mathbb{R}) \cong \text{SL}_2(\mathbb{R}) \times \mathbb{R}^*$.

Problem 4.3

Let G_1 and G_2 be finite groups such that $\gcd(|G_1|, |G_2|) = 1$. Prove that $\text{Aut}(G_1 \times G_2) \cong \text{Aut}(G_1) \times \text{Aut}(G_2)$.

Problem 4.4

Solve the following problems.

- (a) Give an example of $H < G_1 \times G_2$ such that H cannot be written as the direct product of a subgroup $H_1 < G_1$ and a subgroup $H_2 < G_2$.
- (b) Let G_1 and G_2 be groups. Prove that every subgroup of $G_1 \times G_2$ has the form $H_1 \times H_2$, where $H_i < G_i$ for $i = 1, 2$, if and only if for every $g_1 \in G_1$ and $g_2 \in G_2$, both g_1 and g_2 have finite order and $\gcd(o(g_1), o(g_2)) = 1$.

Problem 4.5

Let G be a group satisfying $x^2 = e$ for every $x \in G$.

- (a) Prove that G is abelian.
- (b) If G is finite, prove that there exists a nonnegative integer n such that $G \cong \oplus_n \mathbb{Z}_2$, the direct sum of n copies of $\mathbb{Z}_2$.

Problem 4.6

Let G_1 and G_2 be groups. Prove that

- $C(G_1 \times G_2) = C(G_1) \times C(G_2)$;
- $[G_1 \times G_2, G_1 \times G_2] = [G_1, G_1] \times [G_2, G_2]$.

Problem 4.7

Solve the following problems.

- (a) Let $G = G_1 \times \cdots \times G_n$ be a direct product of groups, let $p_i : G \rightarrow G_i$ be the projection onto the i -th component, and let $\varphi_i : S \rightarrow G_i$ be group homomorphisms for $i = 1, \dots, n$. Prove that there exists a unique group homomorphism $\varphi : S \rightarrow G$ such that $p_i \circ \varphi = \varphi_i$ for every $i = 1, \dots, n$.
- (b) Let $G = G_1 \times \cdots \times G_n$, let $j_i : G_i \rightarrow G$ be the natural homomorphisms, and let $\psi_i : G_i \rightarrow S$ be group homomorphisms for $i = 1, \dots, n$. Give an example showing that there need not exist a unique group homomorphism $\psi : G \rightarrow S$ such that $\psi \circ j_i = \psi_i$ for every $i = 1, \dots, n$.

Problem 4.8

Let G be a group and let H, K be subgroups of G . Suppose that

- $G = HK$,
- $H \cap K = \{e\}$,
- $hk = kh$ for every $h \in H$ and $k \in K$.

Prove that the map $H \times K \rightarrow G, (h, k) \mapsto hk$, is a group isomorphism, and that $G/H \cong K$ and $G/K \cong H$.

Problem 4.9

Let $\{G_\alpha\}_{\alpha \in I}$ be a family of groups indexed by I . For a positive integer n , call an n -tuple $a = (x_1, x_2, \dots, x_n)$ a word of length n over $\{G_\alpha\}$, where $x_i \in \bigsqcup_{\alpha \in I} G_\alpha$ (the symbol $\bigsqcup$ denotes disjoint union). Also define the empty word e of length 0.

(a) Define an equivalence relation $\sim$ on the set of all words over $\{G_\alpha\}$ as follows.

(a1) If e_α denotes the identity element of G_α , then $(x_1, \dots, x_{i-1}, e_\alpha, x_{i+1}, \dots, x_n) \sim (x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$.

(a2) If x_i and x_{i+1} both belong to some G_α , then $(x_1, \dots, x_i, x_{i+1}, \dots, x_n) \sim (x_1, \dots, x_i x_{i+1}, \dots, x_n)$.

Denote the equivalence class of a word a by $[a]$. For words $a = (x_1, \dots, x_n)$ and $b = (y_1, \dots, y_m)$, define their product by $ab = (x_1, \dots, x_n, y_1, \dots, y_m)$. Let $*_{\alpha \in I} G_\alpha$ denote the set of all equivalence classes of words over $\{G_\alpha\}$. Prove that multiplication $[a][b] = [ab]$ is well-defined on $*_{\alpha \in I} G_\alpha$ and makes it a group. This group is called the free product of $\{G_\alpha\}_{\alpha \in I}$.

(b) Let $G = G_1 * \cdots * G_n$ be a free product of groups, let $q_i : G_i \rightarrow G$ send x_i to $[(x_i)]$, and let $\psi_i : G_i \rightarrow S$ be group homomorphisms for $i = 1, \dots, n$. Prove that there exists a unique group homomorphism $\psi : G \rightarrow S$ such that $\psi \circ q_i = \psi_i$ for every $i = 1, \dots, n$.

Problem 4.10

Let S be a nonempty set. For $\alpha \in S$, let $G_\alpha = \{\dots, \alpha^{-1}, e_\alpha = \alpha^0, \alpha = \alpha^1, \alpha^2, \dots\}$ be the infinite cyclic group generated by α . The free product $*_{\alpha \in S} G_\alpha$ is called the free group generated by S and is denoted by $F(S)$. Let R be a subset of $F(S)$, let N be the smallest normal subgroup of $F(S)$ containing R , and put $G = F(S)/N$. Then G is called the group generated by the set of generators S with the set of relations R , also written $G = \langle S \mid R \rangle$. If $S = \{s_1, \dots, s_n\}$ and $R = \{r_1, \dots, r_m\}$, this may be written in more detail as $\langle s_1, \dots, s_n \mid r_1 = \cdots = r_m = e \rangle$. In particular, when $r_i = \alpha^{-i} \beta^j$, the relation $r_i = e$ may also be written $\alpha^i = \beta^j$.

- (a) Determine the structure of the groups $\langle r, s \mid r^n = s^2 = e, s^{-1}rs = r^{-1} \rangle$ and $\langle i, j \mid i^4 = e, i^2 = j^2, j^{-1}ij = i^{-1} \rangle$.
- (b) Write down one possible set of generators and relations for $\mathbb{Z} \times \mathbb{Z}$ and for S_4 .

Problem 4.11

Given groups H and K and a group homomorphism $\varphi : K \rightarrow \text{Aut}(H)$, one can define the semidirect product $H \rtimes_{\varphi} K$. As a set, $H \rtimes_{\varphi} K = \{(h, k) \mid h \in H, k \in K\}$, and the group operation is defined by $(h, k)(h', k') := (h\varphi_k(h'), kk')$, where $\varphi_k := \varphi(k)$, and the identity element is $(1_H, 1_K)$.

- Verify that $H \rtimes_{\varphi} K$ is a group.
- Explain that the external direct product is a special case of the semidirect product.
- Verify the group isomorphisms $H \cong H \times 1_K = \{(h, 1_K) \mid h \in H\}$, $h \mapsto (h, 1_K)$, $K \cong 1_H \times K = \{(1_H, k) \mid k \in K\}$, $k \mapsto (1_H, k)$. Also prove that $H \cong H \times 1_K$ is a normal subgroup of $H \rtimes_{\varphi} K$.
- Prove that $K \cong 1_H \times K$ is a normal subgroup of $H \rtimes_{\varphi} K$ if and only if $\varphi : K \rightarrow \text{Aut}(H)$ is trivial, in which case $H \rtimes_{\varphi} K = H \times K$.
- Let H and K be subgroups of a group G satisfying
 - $G = HK$,
 - $H \cap K = \{1\}$,
 - $H \trianglelefteq G$.

Consider the group homomorphism $\varphi : K \rightarrow \text{Aut}(H)$, $\varphi_k(h) = khk^{-1}$ for every $h \in H$. Prove that the map $f : H \rtimes_{\varphi} K \rightarrow G$, $(h, k) \mapsto hk$, is a group isomorphism, and that $G/H \cong K$.

- Prove the following semidirect product decompositions.
 - $D_n \cong \langle r \rangle \rtimes \{1, s\} \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$.
 - $S_n \cong A_n \rtimes \langle \tau \rangle \cong A_n \rtimes \mathbb{Z}_2$, where $\tau \in S_n$ is any transposition.
 - $\text{GL}_2(\mathbb{R}) \cong \text{SL}_2(\mathbb{R}) \rtimes K \cong \text{SL}_2(\mathbb{R}) \rtimes \mathbb{R}^*$, where $K = \{\text{diag}(a, 1) \mid a \in \mathbb{R}^*\}$.
- For a fixed odd integer $n > 1$, prove that the direct product $\text{SL}_n(\mathbb{R}) \times \mathbb{R}^*$ can be realized as a nontrivial semidirect product $\text{SL}_n(\mathbb{R}) \rtimes \mathbb{R}^*$.

5 Group Actions and the Sylow Theorems

Problem 5.1

Let the group $\text{GL}_3(\mathbb{R})$ act on the column-vector space $\mathbb{R}^3$, regarded as a set, by matrix multiplication. Solve the following problems.

- (a) Prove that the column vectors $(1, 0, 0)^t$ and $(0, 1, 0)^t$ lie in the same orbit.
- (b) Is this group action transitive? Explain why.
- (c) Find the stabilizer subgroup $H = \text{Stab}((0, 0, 1)^t)$.

Problem 5.2

Let G be a group of order n . Let p be the smallest prime divisor of n , and let H be a subgroup of G of index p . Prove that H is a normal subgroup of G .

Problem 5.3

Let a group G act on a set X . The action of G on X is called faithful if, for every $g \in G$ satisfying $gx = x$ for all $x \in X$, one has $g = e$. It is called free if, for every $x \in X$ and $g \in G$ satisfying $gx = x$, one always has $g = e$. Determine whether each of the following group actions is faithful and whether it is free.

- (a) The conjugation action of the dihedral group D_4 on itself.
- (b) The action of $\text{SO}_n(\mathbb{R})$ on $\mathbb{R}^n \setminus \{0\}$, where $n \geq 2$.

Problem 5.4

Let U_n denote the group of all $n \times n$ unitary matrices under matrix multiplication, and let S^{2n-1} denote the unit sphere in $\mathbb{C}^n$. Let U_n act naturally on S^{2n-1} , where $n \geq 2$.

- (a) Prove that this action is transitive.
- (b) Fix a point on S^{2n-1} . Prove that its stabilizer subgroup is isomorphic to U_{n-1} .

Problem 5.5

Let $O_n(\mathbb{R}) := \{M \in M_n(\mathbb{R}) \mid M^t M = I\}$ denote the set of all $n \times n$ real orthogonal matrices. It is a group under matrix multiplication and is called the orthogonal group of order n . Let $\text{SO}_n(\mathbb{R}) := \{M \in O_n(\mathbb{R}) \mid \det M = 1\}$. It is also a group under matrix multiplication and is called the special orthogonal group of order n .

- (a) Prove that $\text{SO}_n(\mathbb{R}) \trianglelefteq O_n(\mathbb{R})$ and $[O_n(\mathbb{R}) : \text{SO}_n(\mathbb{R})] = 2$.

The group of all automorphisms of a regular n -hedron in $\mathbb{R}^3$ under composition is called the symmetry group of the regular n -hedron and is denoted by E_n , where $n = 4, 6, 8, 12, 20$. Regard E_n as a subgroup of the orthogonal group $O_3(\mathbb{R})$. The group $E_n \cap \text{SO}_3(\mathbb{R})$ is called the rotation group of the regular n -hedron and is denoted by F_n , where $n = 4, 6, 8, 12, 20$.

- (b) For $n = 4, 6, 8, 12, 20$, find the orders of E_n and F_n .
- (c) Prove that $F_4 \cong A_4$.

(d) Prove that $F_6 \cong F_8 \cong S_4$.

(e) Prove that $F_{12} \cong F_{20} \cong A_5$.

Problem 5.6

Prove that a group of order 56 and a group of order pqr , where $p < q < r$ are primes, are not simple.

Problem 5.7

Let H be a Sylow p -subgroup of a finite group G . Let $L < G$ and suppose $p \mid |L|$. Prove that there exists $g \in G$ such that $gHg^{-1} \cap L$ is a Sylow p -subgroup of L .

Problem 5.8

Let G be a group of order p^2q , where p and q are primes and $p < q$. Prove that either G has a normal Sylow q -subgroup or $G \cong A_4$.

Problem 5.9

Let G be a simple group of order 60. Prove that G is isomorphic to A_5 . (Hint: You may assume that G is not isomorphic to A_5 and prove that there exist two distinct Sylow 2-subgroups P and Q of G satisfying $|N_G(P \cap Q)| \geq 12$, thereby obtaining a contradiction.)

Problem 5.10

Let G be a simple group of order 360. We will use proof by contradiction to determine the number of Sylow 3-subgroups of G .

(a) Assume that G has 40 Sylow 3-subgroups. Prove that there exist two Sylow 3-subgroups $P \neq Q$ such that $|P \cap Q| > 1$.

(b) Under the assumption in (a), let $H = P \cap Q$. Prove that $C_G(H)/H \cong A_4$, and that $C_G(H)$ has a normal Sylow 2-subgroup K , where $C_G(H) = \{g \in G \mid \forall h \in H, hg = gh\}$ is the centralizer of H in G .

(c) Under the assumption in (a), prove that $|N_G(K)| \geq 72$, and derive a contradiction.

(d) Find the number of Sylow 3-subgroups of G .

6 Rings, Ideals, and Nilpotent Elements

Problem 6.1

Let R be a ring such that $a^2 = a$ for every $a \in R$. Prove the following.

- (a) For every $a \in R$, $2a = a + a = 0$.
- (b) R is commutative.

Problem 6.2

Solve the following problems.

- (a) If R is a commutative ring and $a, b \in R$ are nilpotent, prove that $a + b$ is nilpotent.
- (b) Give an example showing that, in a noncommutative ring, the sum of two nonzero nilpotent elements need not be nilpotent.

Problem 6.3

Let $A = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subset \mathbb{R}$. For $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, define $N(x) = a^2 - 2b^2$. Prove the following.

- (a) A is a subring of the field $\mathbb{R}$.
- (b) $x \in \mathbb{Z}[\sqrt{2}]^*$ if and only if $N(x) = \pm 1$.
- (c) The group of units $\mathbb{Z}[\sqrt{2}]^*$ is infinite.

Problem 6.4

Let F be a field and let $T_2(F)$ denote the set of all matrices $T_2(F) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in F \right\}$.

- (a) Find all invertible elements of $T_2(F)$.
- (b) Prove that $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in F \right\}$ is an ideal satisfying $I^2 = 0$, and prove that $T_2(F)/I \cong F \times F$.
- (c) Find the center of $T_2(F)$.

Problem 6.5

Let R and S be unital rings. Prove that every ideal of $R \times S$ can be written uniquely in the form $I \times J$, where $I \trianglelefteq R$ and $J \trianglelefteq S$. Now suppose in addition that R and S are nonzero unital commutative rings. Prove the following.

- (a) The prime ideals of $R \times S$ are exactly $P \times S$ and $R \times Q$, where P and Q are prime ideals of R and S , respectively.
- (b) The same conclusion about prime ideals also holds for maximal ideals.

Problem 6.6

Let $n \geq 2$ be a positive integer and let $R = M_n(\mathbb{C})$ be the ring of $n \times n$ complex matrices. If I is an ideal of R , prove that $I = 0$ or $I = R$.

Problem 6.7

Let R be a commutative ring and let $I \subset R$ be an ideal. Define $\sqrt{I} = \{r \in R \mid \text{there exists a positive integer } n \text{ such that } r^n \in I\}$. Verify that $\sqrt{I}$ is an ideal.

Problem 6.8

Give an example of a maximal ideal I in a noncommutative ring R such that I is not a prime ideal of R .

Problem 6.9

Let R be a ring and let $\text{Nil}(R) = \{a \in R \mid a \text{ is nilpotent}\}$.

- (a) Suppose R satisfies the property that if $a^2 = 0$, then $a = 0$. Prove that $\text{Nil}(R) = \{0\}$.
- (b) If R is commutative, prove that $\text{Nil}(R)$ is an ideal.
- (c) Give an example showing that, in a noncommutative ring, $\text{Nil}(R)$ need not be an ideal.

Problem 6.10

Let R be a unital ring. Let $\{I_i\}_{i \in \Lambda}$ be a family of ideals of R , where Λ is a nonempty index set. If for every $i, j \in \Lambda$ one has $I_i \subseteq I_j$ or $I_j \subseteq I_i$, prove that $\bigcup_{i \in \Lambda} I_i$ is an ideal of R .

7 Ring Homomorphisms, Polynomial Rings, and Ideals

Problem 7.1

Let R be a unital commutative ring and let I_1, I_2, I_3 be ideals of R .

- (a) If I_1 and I_2 are comaximal, prove that $I_1 I_2 = I_1 \cap I_2$.
- (b) If I_1 and I_3 are comaximal, and I_2 and I_3 are comaximal, prove that $I_1 I_2$ and I_3 are comaximal.
- (c) Prove Theorem 4.7.

Problem 7.2

Let R and S be unital rings and let $f : R \rightarrow S$ be a nonzero ring homomorphism. Solve the following problems.

- (a) If I is a prime ideal of S , prove that $f^{-1}(I)$ is a prime ideal of R .
- (b) If J is a prime ideal of R , must $f(J)$ be a prime ideal of S ? Explain why.
- (c) If I is a maximal ideal of S , must $f^{-1}(I)$ be a maximal ideal of R ? Explain why.
- (d) If J is a maximal ideal of R , must $f(J)$ be a maximal ideal of S ? Explain why.

Problem 7.3

Let $A = \mathbb{Z} \times \mathbb{Z}$ be an abelian group and define $\text{End}(A) := \{f : A \rightarrow A \mid f \text{ is a group homomorphism}\}$.

- (a) Prove that $\text{End}(A)$ has a natural ring structure. State its addition and multiplication operations, and find the zero element and the multiplicative identity of $\text{End}(A)$.
- (b) Prove that $\text{End}(A)$ is isomorphic to the ring of 2×2 integer matrices.

Problem 7.4

Let $f : R \rightarrow S$ be a ring homomorphism, let I and J be ideals of R and S , respectively, and suppose $f(I) \subseteq J$. Define $\bar{f} : R/I \rightarrow S/J, a + I \mapsto f(a) + J$.

- (a) Prove that $\bar{f}$ is well-defined and is a ring homomorphism.
- (b) Prove that $\bar{f}$ is a ring isomorphism if and only if $f(R) + J = S$ and $f^{-1}(J) = I$.

Problem 7.5

Let R be a unital ring and let $M_n(R)$ be the ring of $n \times n$ matrices over R . If I is an ideal of R , let $M_n(I)$ denote the set of all $n \times n$ matrices whose entries all belong to I . Prove the following.

- (a) $M_n(I)$ is an ideal of $M_n(R)$.
- (b) Every ideal of $M_n(R)$ has the form $M_n(J)$, where J is some ideal of R .
- (c) There is a ring isomorphism $M_n(R)/M_n(I) \cong M_n(R/I)$.

Problem 7.6

Solve the following problems.

- (a) Prove that $\mathbb{R}[x]/(x^2 + 1)$ is isomorphic to the field of complex numbers $\mathbb{C}$.
- (b) Prove that the quotient ring $\mathbb{Z}[x]/(x^2 + 1)$ is isomorphic to the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

Problem 7.7

Let $f(x) = x^4 + 1$. Discuss separately whether $f(x)$ is irreducible in $\mathbb{Q}[x]$ and whether it is irreducible in $\mathbb{R}[x]$, and explain your reasoning.

Problem 7.8

Let $A = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.

- (a) Let $I = (x^2) \subseteq A[x]$ be the ideal generated by x^2 . Is the quotient ring $A[x]/I$ an integral domain? Explain why.
- (b) Is the ideal $J = (4, x)$ of $A[x]$ principal? Explain why.

Problem 7.9

Let F be a field. Prove that $F[x]$ contains infinitely many monic irreducible polynomials.

Problem 7.10

Let R be a unital commutative ring and let $R[x]$ be the polynomial ring in one indeterminate over R . Let $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$, where $a_i \in R$ for $0 \leq i \leq n$ and $a_n \neq 0$. Prove the following.

- (a) f is a unit in $R[x]$ if and only if $a_0 \in R$ is a unit and $a_1, \dots, a_n$ are nilpotent elements of R .
- (b) f is nilpotent in $R[x]$ if and only if $a_0, a_1, \dots, a_n$ are all nilpotent.
- (c) f is a zero divisor in $R[x]$ if and only if there exists $a \in R \setminus \{0\}$ such that $af = 0$.

Problem 7.11

Let $\varphi : \mathbb{Z}[x] \rightarrow \mathbb{Z}[x]$ be a nonzero ring homomorphism. Determine all such ring homomorphisms, and in each case determine when the homomorphism is injective, when it is surjective, and when it is a ring automorphism.

Problem 7.12

Let R be a unital commutative ring and let $a_1, \dots, a_n \in R$, where $n \geq 1$. Define the map $\Phi : R[x] \rightarrow R^n$, $f(x) \mapsto (f(a_1), \dots, f(a_n))$. Solve the following problems.

- (a) Prove that Φ is surjective if and only if $a_i - a_j \in R^*$ for every $i \neq j$.

- (b) Under the equivalent condition above, prove that $\text{Ker } \Phi = \left(\prod_{i=1}^n (x - a_i) \right)$, and hence prove that $R[x] / \left(\prod_{i=1}^n (x - a_i) \right) \cong R^n$.
- (c) Under the equivalent condition above, prove that for every $b_1, \dots, b_n \in R$, there exists a unique polynomial $f(x) \in R[x]$ of degree less than n such that $f(a_i) = b_i$ for all $1 \leq i \leq n$, and write down such a polynomial $f(x)$.

8 Domains, Fields of Fractions, and Factorization

Problem 8.1

Let R be an integral domain and let F be a field. Let $i : R \rightarrow K(R)$, $i(a) = \frac{a}{1}$ for all $a \in R$, be the natural embedding, and let $f : R \rightarrow F$ be an injective ring homomorphism. Prove that there exists a unique ring homomorphism $\bar{f} : K(R) \rightarrow F$ such that $\bar{f} \circ i = f$.

Problem 8.2

Let p be a prime and let F be a finite field of characteristic p . Define a map $f : F \rightarrow F$ by $f(a) = a^p$ for all $a \in F$. Prove that f is a field isomorphism.

Problem 8.3

Let R be a unital commutative ring. Consider the ring homomorphism $f : \mathbb{Z} \rightarrow R$, $f(n) = n \cdot 1$. If $\text{Ker } f = m\mathbb{Z}$, where m is a nonnegative integer, then m is called the characteristic of R .

- (a) If R is an integral domain, prove that the characteristic of R is either a prime or 0.
- (b) If R is a unital commutative ring of prime characteristic p , prove that for every $a, b \in R$ and every positive integer n , $(a + b)^{p^n} = a^{p^n} + b^{p^n}$.

Problem 8.4

Let p be a prime and let x be an indeterminate. Put $A = \left\{ \sum_{i=0}^n a_i x^{p^i} \mid n \in \mathbb{Z}_{\geq 0}, a_i \in \mathbb{F}_p \right\} \subseteq \mathbb{F}_{p[x]}$. Use the usual polynomial addition on A , and define multiplication by $f * g = f \circ g = f(g(x))$. Solve the following problems.

- (a) Prove that A is a unital commutative ring under the above addition and multiplication.
- (b) Construct a ring isomorphism $\mathbb{F}_{p[t]} \cong A$, where t is an indeterminate.

Problem 8.5

Let (R, φ) be a Euclidean domain that is not a field. Let R_0 be the set of all nonzero nonunit elements of R , and let $a \in R_0$ satisfy $\varphi(a) = \min_{b \in R_0} \varphi(b)$. Prove that the quotient ring $R/(a) = \{r + (a) \mid r \in R^* \cup \{0\}\}$. In particular, $R/(a)$ is a field.

Problem 8.6

Give detailed proofs of Example 6 in this section.

- (a) In the ring $\mathbb{Z}[\sqrt{-5}]$, the ideal $(2, 1 + \sqrt{-5})$ is not principal.
- (b) In the ring $\mathbb{Z}[x]$, the ideal $(2, x)$ is not principal.

Problem 8.7

Let F be a field. Let $F[[x]] = \left\{ \sum_{n=0}^{\infty} a_n x^n \mid a_n \in F \right\}$ be the set of all formal power series over F .

- (a) For $f = \sum_{n=0}^{\infty} a_n x^n$ and $g = \sum_{n=0}^{\infty} b_n x^n$ in $F[[x]]$, define $f + g = \sum_{n=0}^{\infty} (a_n + b_n) x^n$ and $fg = \sum_{n=0}^{\infty} \left(\sum_{i=0}^n a_i b_{n-i} \right) x^n$. Verify that $F[[x]]$ is a unital commutative ring under these addition and multiplication operations.
- (b) Find the group of units of $F[[x]]$.
- (c) Find all ideals of $F[[x]]$. Which of them are prime ideals and which are maximal ideals? Prove that $F[[x]]$ is a PID.
- (d) Find the field of fractions $K(F[[x]])$.

Problem 8.8

Let $R = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{ a + b\left(\frac{1+\sqrt{-19}}{2}\right) \mid a, b \in \mathbb{Z} \right\} \subset \mathbb{C}$. Prove that R is not a Euclidean domain by completing the following steps.

- (a) Assume that R is a Euclidean domain. Then there is a function $\varphi : R \setminus \{0\} \rightarrow \mathbb{N}_0$ satisfying the conditions in the definition of a Euclidean domain. Let R_0 be the set of all nonzero nonunit elements of R , and let $a \in R_0$ satisfy $\varphi(a) = \min_{b \in R_0} \varphi(b)$. Prove that $|R/(a)| \leq 3$.
- (b) Verify that $f(x) = x^2 - x + 5 \in R[x]$ has a root in R , but that $\bar{f}(x) \in (R/(a))[x]$ has no root in $R/(a)$. Derive a contradiction.
- (c) Verify that $\mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right]$, $\mathbb{Z}\left[\frac{1+\sqrt{-67}}{2}\right]$, and $\mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$ are all not Euclidean domains.

Problem 8.9

Let F be a field and let t be an indeterminate. Put $R = F[t^2, t^3] \subseteq F[t]$. Solve the following problems.

- (a) Prove that $K(R) = F(t)$.
- (b) Let $I = (t^2, t^3)$ be the ideal of R . Prove that I is not principal, and hence prove that R is not a PID.

Problem 8.10

Let F be a field. Let $F[x, y_1, y_2, \dots]$ be the polynomial ring over F in the indeterminates $x, y_1, y_2, \dots$, where each polynomial involves only finitely many indeterminates. Let $R = F[x, y_1, y_2, \dots]/(x - y_1^2, y_1 - y_2^2, y_2 - y_3^2, \dots)$. Continue to denote the images of $x, y_1, y_2, \dots$ in the quotient ring R by the same symbols. For every positive integer n , let $R_n = F[y_n] \subseteq R$. Solve the following problems.

- (a) Prove that $R_1 \subseteq R_2 \subseteq \dots$, $R = \bigcup_{n \geq 1} R_n$, and that every R_n is isomorphic to the polynomial ring in one variable $F[t]$. Hence prove that every R_n is a PID.
- (b) Prove that every finitely generated ideal of R is principal.
- (c) Let $I = (y_1, y_2, y_3, \dots)$. Prove that I is not finitely generated. Hence prove that R is not a PID.

Problem 8.11

Consider the subring $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ of the complex numbers. For $x = a + b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$, put $N(x) = a^2 + 3b^2$.

- (a) Prove that the multiplicative group $\mathbb{Z}[\sqrt{-3}]^* = \{x \in \mathbb{Z}[\sqrt{-3}] \mid N(x) = 1\} = \{1, -1\}$.
- (b) Prove that 2 , $1 + \sqrt{-3}$, and $1 - \sqrt{-3}$ are pairwise nonassociate irreducible elements of $\mathbb{Z}[\sqrt{-3}]$.
- (c) Prove that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.
- (d) Let $x = 4$ and $y = 2(1 + \sqrt{-3})$. Prove that x and y have no greatest common divisor in $\mathbb{Z}[\sqrt{-3}]$.
- (e) Let $I = (2, 1 + \sqrt{-3})$. Prove that I is not a principal ideal of $\mathbb{Z}[\sqrt{-3}]$.

Problem 8.12

Let R be an integral domain and let $a, b \in R$ be nonzero elements.

- (a) If $d \in R$ is a greatest common divisor of a and b , and $c \in R$ is a least common multiple of a and b , prove that ab is associate to cd .
- (b) If $\text{lcm}(a, b)$ exists, prove that $\text{gcd}(a, b)$ also exists.

Problem 8.13

Determine whether each of the following statements is true. Give a proof or a counterexample.

- (a) If I is a nonzero prime ideal of $\mathbb{Q}[X]$, then $\mathbb{Q}[X]/I$ is a unique factorization domain.
- (b) If I is a nonzero prime ideal of $\mathbb{Z}[X]$, then $\mathbb{Z}[X]/I$ is a unique factorization domain.

Problem 8.14

If R is a UFD, prove that R is a PID if and only if for any two principal ideals (a) and (b) of R , their sum $(a) + (b)$ is also principal.

9 Eisenstein's Criterion, Modules, and Finite Abelian Groups

Problem 9.1

(Eisenstein's criterion) Let R be a UFD and let F be the field of fractions of R . Let $f(x) \in R[x]$ be a primitive polynomial and let p be an irreducible element of R . Write $f(x) = a_n x^n + \cdots + a_1 x + a_0$. If $p \nmid a_n$, $p \mid a_i$ for $0 \leq i \leq n-1$, and $p^2 \nmid a_0$, prove that $f(x)$ is irreducible in $F[x]$.

Problem 9.2

Let p be an odd prime and let $n \geq 1$. Prove that the polynomial $x^n - p$ is irreducible in $\mathbb{Z}[i][x]$.

Problem 9.3

Let R be an integral domain and let $p \in R \setminus \{0\}$. If the principal ideal (p) generated by p is a prime ideal, then p is called a prime element.

- (a) Prove that p is a prime element if and only if, for every $a, b \in R$, $p \mid ab$ implies $p \mid a$ or $p \mid b$.
- (b) Prove that every prime element is irreducible.
- (c) Must every irreducible element be prime? Explain why.

Problem 9.4

Let F be a field and let $f(x, y, z) = xz - y^2 \in F[x, y, z]$. Let I be the principal ideal generated by f .

- (a) Prove that the quotient ring $F[x, y, z]/I$ is an integral domain.
- (b) Is $F[x, y, z]/I$ a UFD? Explain why.

Problem 9.5

Let $I \subset \mathbb{Z}[x]$ be a prime ideal. Prove that I has at most two generators. Furthermore, find all prime ideals of $\mathbb{Z}[x]$.

Problem 9.6

Let $R = \mathbb{C}[t]$, and let S be a subring of R that contains $\mathbb{C}$ but is not equal to $\mathbb{C}$. Prove that R is a finitely generated S -module.

Problem 9.7

Let R be a unital ring, let M be a finitely generated R -module, and let N be a submodule of M . Explain whether M/N and N are also finitely generated.

Problem 9.8

Let R be a PID. Prove that every submodule of a finitely generated free R -module is again free.

Problem 9.9

Let K be a field and let $K[x]$ be the polynomial ring in one indeterminate over K . Let $A = \{M \mid M \text{ is a } K[x] \text{-module}\}$ and $B = \{(V, \alpha) \mid V \text{ is a } K \text{-vector space, } \alpha \in \text{End}_K(V)\}$. Prove that there is a natural bijection between A and B .

Problem 9.10

Let G be a finite abelian group of order 100. Find all isomorphism classes of G .

Problem 9.11

Let G be a finite abelian group of order n . Let m be a positive integer such that $m \mid n$. Prove that G has a subgroup of order m .

10 Field Extensions and Algebraic Elements

Problem 10.1

Let $(\mathbb{Q}^*, \times)$ be the multiplicative group of nonzero rational numbers. Is it a finitely generated abelian group? Is it a free abelian group? Explain why.

Problem 10.2

Let F be a field, let $F^* = F \setminus \{0\}$ be its multiplicative group, and let G be a finite subgroup of F^* . Prove that G is cyclic.

Problem 10.3

Prove that there is no 3×3 matrix A over $\mathbb{Q}$ such that $A^8 = I$ but $A^4 \neq I$. Here I denotes the identity matrix.

Problem 10.4

Let $\mathbb{C}$ be the field of complex numbers and let $f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$, where $n \geq 2$ and $\deg f \geq 1$. Prove that the zero set $V(f)$ of $f(x_1, \dots, x_n)$ is infinite.

Problem 10.5

Prove that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ are isomorphic as $\mathbb{Q}$ -vector spaces, but are not isomorphic as fields.

Problem 10.6

Let L be a finite extension of K . Prove that the rational function field $L(x)$ is also a finite extension of $K(x)$, and that $[L(x) : K(x)] = [L : K]$.

Problem 10.7

Prove that the field of real numbers $\mathbb{R}$ has no proper subfield isomorphic to itself. Does the field of complex numbers $\mathbb{C}$ have a proper subfield isomorphic to itself?

Problem 10.8

Solve the following problems.

(a) Suppose K/F is an algebraic extension of fields. Let R be a subring of K containing F . Prove that R is a subfield of K .

(b) Suppose K/F is a field extension, and every subring R of K containing F is a field. Prove that K/F is an algebraic extension.

Problem 10.9

Let E/F be a field extension of degree m , and let $f(x)$ be an irreducible polynomial of degree n over F . If m and n are coprime, prove that $f(x)$ is irreducible over E .

Problem 10.10

Let $\alpha = \sqrt{2} + \sqrt{3}$.

- (a) Find the minimal polynomial of α over $\mathbb{Q}$.
- (b) Prove that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
- (c) Find the extension degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, and give a set of elements that are linearly independent over $\mathbb{Q}$ and generate $\mathbb{Q}(\alpha)$.

Problem 10.11

Let F be a field contained in the ring $M_n(\mathbb{Q})$ of $n \times n$ matrices over $\mathbb{Q}$. Prove that $[F : \mathbb{Q}] \leq n$.

11 Splitting Fields and Embeddings

Problem 11.1

For each of the following fields F and polynomials $f(x) \in F[x]$, find the splitting field of f over F .

- (a) $F = \mathbb{Q}$, $f(x) = x^4 - 2$.
- (b) $F = \mathbb{Q}$, $f(x) = x^4 + x^2 + 1$.

Problem 11.2

Let p be an odd prime and consider $f(x) = x^p - 2$. Let L be the splitting field of $f(x)$ over $\mathbb{Q}$. Prove that $[L : \mathbb{Q}] = p(p-1)$.

Problem 11.3

The irreducibility of the cyclotomic polynomial $\Phi_n(x)$ in $\mathbb{Q}[x]$ can be proved by the following steps.

- (a) Let $g(x) \in \mathbb{F}_{p[x]}$ and let $h(x) = g(x^p)$. Prove that $h(x) = g(x)^p$.
- (b) Let $f(x) \in \mathbb{Z}[x]$ be monic and irreducible, and suppose $f(x) \mid \Phi_n(x)$. Let $\zeta \in \mathbb{C}$ be a primitive n -th root of unity such that $f(\zeta) = 0$. Let p be a prime relatively prime to n . Prove that $f(\zeta^p) = 0$. (Hint: Use the quotient map $\mathbb{Z}[x] \rightarrow \mathbb{F}_{p[x]}$ and the fact that $x^n - 1 \in \mathbb{F}_{p[x]}$ has no repeated roots in $\mathbb{F}_p$.)
- (c) Prove that $\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$, and deduce that $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.

Problem 11.4

Consider the polynomial $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$ and let $\alpha = \sqrt{2 + \sqrt{2}}$.

- (a) Prove that $f(x)$ is irreducible in $\mathbb{Q}[x]$.
- (b) Prove that $\mathbb{Q}(\alpha)$ already contains every root of $f(x)$, and hence is the splitting field of $f(x)$.
- (c) Find $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ and write down all $\mathbb{Q}$ -embeddings of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$.

Problem 11.5

Determine whether $\mathbb{C}(x)$ and $\mathbb{C}((x))$ are algebraically closed fields, and give proofs. Here $\mathbb{C}(x)$ is the field of rational functions over the complex numbers, and $\mathbb{C}((x))$ is the field of fractions of the formal power series ring $\mathbb{C}[[x]]$.

Problem 11.6

Compute $\text{Emb}(\mathbb{Q}(\sqrt[4]{2}, \sqrt{-1})/\mathbb{Q})$ and $\text{Emb}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$.

Problem 11.7

Give all field embeddings of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ into $\mathbb{C}$.

Problem 11.8

Prove that $\overline{\mathbb{Q}}(x)$ cannot be embedded into $\overline{\mathbb{Q}}$. What if $\overline{\mathbb{Q}}$ is replaced by the field of complex numbers $\mathbb{C}$?

Problem 11.9

- (a) Prove that every finite extension of $\mathbb{Q}$ can be embedded into the field extension $\mathbb{C}/\mathbb{Q}$.
- (b) Prove that every finitely generated extension of $\mathbb{Q}$ can be embedded into the field extension $\mathbb{C}/\mathbb{Q}$.

Problem 11.10

Let F be a field and let $f(x) \in F[x]$ be irreducible. Let K be the splitting field of $f(x)$ over F , and suppose that there exists an element $\alpha \in K$ such that both α and $\alpha + 1$ are roots of $f(x)$.

- (a) Prove that $\text{char}(F) > 0$.
- (b) Prove that $\text{char}(F)$ divides $|\text{Aut}(K/F)|$.

12 Normal and Separable Extensions

Problem 12.1

For each of the following field extensions E/F , determine whether it is normal and whether it is separable.

- $F = \mathbb{Q}$, $E = \mathbb{Q}(2^{\frac{1}{4}})$.
- $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \dots, \sqrt{n}, \dots)$.
- p is a prime, $F = \mathbb{F}_{p(t^p)}$, $E = \mathbb{F}_{p(t)}$.
- $F = \mathbb{Q}(x)$, $E = \mathbb{Q}(x)[t]/(t^2 - x)$.

Problem 12.2

For a given prime p , find the normal closure of the field extension $\mathbb{Q}(2^{\frac{1}{p}})/\mathbb{Q}$.

Problem 12.3

Give an example of field extensions $F \subseteq K \subseteq L$ such that both K/F and L/K are normal extensions, but L/F is not.

Problem 12.4

Let $E = \mathbb{C}(t)$ be the field of rational functions and let $F = \mathbb{C}(t^n + t^{-n})$. Prove that E/F is a normal extension.

Problem 12.5

For every prime p , prove that $E = \mathbb{F}_{p[x]}/(x^p - x + 1)$ is a normal extension of $\mathbb{F}_p$.

Problem 12.6

Let $E/\mathbb{Q}$ be a finite normal extension of odd degree. Prove that $E \subseteq \mathbb{R}$.

Problem 12.7

Let E/F be a field extension and let $\alpha, \beta \in E$. If $F(\alpha)/F$ is a normal extension and $F(\alpha) \cap F(\beta) = F$, prove that $[F(\alpha, \beta) : F] = [F(\alpha) : F][F(\beta) : F]$.

Problem 12.8

In $\mathbb{C}$, let $\alpha = \sqrt[3]{2}$, let ζ_3 be a primitive third root of unity, and put $K = \mathbb{Q}(\alpha)$ and $M = \mathbb{Q}(\zeta_3\alpha)$.

- Prove that both $K/\mathbb{Q}$ and $M/\mathbb{Q}$ are separable, nonnormal extensions of degree 3.
- Prove that $K \neq M$, and hence prove that $K \cap M = \mathbb{Q}$.
- Prove that $KM = \mathbb{Q}(\alpha, \zeta_3)$ is the splitting field of $x^3 - 2$, and find its degree.

Problem 12.9

Let u be an indeterminate and let $F = \mathbb{Q}(u)$. Let $\alpha^3 = u$ and put $E = F(\alpha)$.

- (a) Prove that $x^3 - u$ is irreducible in $F[x]$, and find $[E : F]$.
- (b) Prove that E/F is separable but not normal.
- (c) Let ζ_3 be a primitive third root of unity. Prove that $L = F(\alpha, \zeta_3)$ is the normal closure of E/F , and find $[L : F]$.
- (d) Prove that $\mathbb{C}(u, \alpha)/\mathbb{C}(u)$ is a normal extension.

Problem 12.10

Verify that the polynomial $f(x) = x^p - t$ in Example 2 is irreducible in $F[x]$.

13 Galois Theory and the Fundamental Theorem

Problem 13.1

Prove that the extension $E \supseteq F$ is Galois, determine the Galois group $\text{Gal}(E/F)$, all of its subgroups, and the corresponding intermediate fields between F and E .

- (a) $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt[4]{2}, i)$.
- (b) $F = \mathbb{R}(x + \frac{1}{x})$, $E = \mathbb{R}(x)$.
- (c) $F = \mathbb{R}(x^2 + y^2, xy)$, $E = \mathbb{R}(x, y)$.

Problem 13.2

Compute the Galois group of $x^5 - 2$ over $\mathbb{Q}$ and over $\mathbb{F}_3$, respectively.

Problem 13.3

Let E/F be a field extension, let $G = \text{Aut}(E/F)$, let $H < G$, and put $K = E^H$. Prove that for every $\eta \in G$, $E^{\eta H \eta^{-1}} = \eta(K)$.

Problem 13.4

If $E/\mathbb{Q}$ is a Galois extension and $\text{Gal}(E/\mathbb{Q}) \cong S_5$, prove that E is the splitting field of a polynomial of degree 5.

Problem 13.5

Let E/F be a separable extension of degree d , and let N be the number of intermediate fields.

- (a) Prove that $N \leq 2^{d!}$.
- (b) Prove that $N \leq 2^d$.

Problem 13.6

Prove that every finite group can be realized as the Galois group of a Galois extension.

Problem 13.7

Suppose E/F is a Galois extension of degree p^n , where p is a prime and n is a positive integer. Prove that E contains Galois extensions of F of degree p and of degree p^{n-1} .

Problem 13.8

Let $f(x) \in F[x]$ be an irreducible separable polynomial, and let E be the splitting field of $f(x)$. If $\text{Gal}(E/F)$ is abelian, prove that $[E : F] = \deg f(x)$.

Problem 13.9

Let p be a prime. Suppose that the degree of every finite extension of a field F is divisible by p .

- (a) Prove that the degree of every finite separable extension of F is a power of p .
- (b) Prove that the degree of every finite extension of F is a power of p .

Problem 13.10

Let k be a field, let $n \geq 2$, and let $E = k(x_1, \dots, x_n)$ be the field of rational functions in n variables over k . Let S_n act on E so that every $\sigma \in S_n$ fixes every element of k and satisfies $\sigma(x_i) = x_{\sigma(i)}$ for $1 \leq i \leq n$. For $1 \leq r \leq n$, put $e_r = \sum_{1 \leq i_1 < \dots < i_r \leq n} x_{i_1} \cdots x_{i_r}$, and let $F = k(e_1, \dots, e_n)$. Solve the following problems.

- (a) Prove that $F \subseteq E^{S_n}$, and prove that E/F is a finite extension with $[E : F] \leq n!$.
- (b) Prove that E/F is a Galois extension, determine its Galois group, and thereby prove that $E^{S_n} = F$.
- (c) Assume $\text{char } k \neq 2$ and put $\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)$. Prove that every element of A_n fixes Δ , while every odd permutation sends Δ to $-\Delta$. Hence prove that $E^{A_n} = F(\Delta)$.

14 Möbius Inversion and Finite Fields

Problem 14.1

Define the Möbius function $\mu : \mathbb{N} \rightarrow \mathbb{Z}$ as follows: $\mu(d) =$

$$\begin{cases} 1 & \text{if } d=1 \\ (-1)^k & \text{if } d=p_1 \cdots p_k \text{ is the product of } k \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

Let $f, g : \mathbb{N} \rightarrow \mathbb{N}$ be nonzero functions. If $f(n) = \sum_{d|n} g(d)$, prove that $g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$, and use this to complete the calculation in Example 4.

Problem 14.2

Let α be a root in $\overline{\mathbb{F}_3}$ of the polynomial $x^2 + 2x + 2$ over $\mathbb{F}_3$, and put $E = \mathbb{F}_3[\alpha]$. Find the following.

- (a) The degree $n = [E : \mathbb{F}_3]$ of the field extension.
- (b) The inverse of $\beta = \alpha^2 + 1$ in E , expressed as an $\mathbb{F}_3$ -linear combination of $1, \alpha, \dots, \alpha^{n-1}$.

Problem 14.3

Find the splitting field of $x^8 - 1 \in \mathbb{F}_3[x]$.

Problem 14.4

Find the greatest common divisor of the polynomials $f(x) = x^6 + x^4 + x + 1 \in \mathbb{F}_2[x]$ and $g(x) = x^8 - x \in \mathbb{F}_2[x]$ over $\mathbb{F}_2$. Use this to explain why $f(x)$ has exactly four roots in $\mathbb{F}_8$.

Problem 14.5

Find the order of the special linear group $\text{SL}_m(\mathbb{F}_q)$ over the finite field $\mathbb{F}_q$.

Problem 14.6

Prove that every element of a finite field can be written as the sum of two squares.

Problem 14.7

For a prime p and a positive integer n , prove that $x^{p^n} - x + 1$ is irreducible over $\mathbb{F}_p$ if and only if $n = 1$ or $n = p = 2$.

Problem 14.8

Let q be a prime power, let $f(x) \in \mathbb{F}_{q^m}[x]$ be a monic irreducible polynomial of degree n , and let m be a positive integer. Prove that $f(x)$ factors in $\mathbb{F}_{q^m}[x]$ into exactly $\gcd(m, n)$ pairwise distinct monic irreducible factors, and that each irreducible factor has degree $n / \gcd(m, n)$. In particular, prove that $f(x)$ is irreducible in $\mathbb{F}_{q^m}[x]$ if and only if $\gcd(m, n) = 1$.

Problem 14.9

Let K be a finite field and let $\overline{K}$ be an algebraic closure of K . Solve the following problems.

- (a) Prove that $\text{Aut}(\overline{K}/K)$ is an abelian group.
- (b) Let $\sigma \in \text{Aut}(\overline{K}/K)$. Prove that if there is a positive integer m such that $\sigma^m = \text{id}_{\overline{K}}$, then $\sigma = \text{id}_{\overline{K}}$. Hence prove that every nonidentity element of $\text{Aut}(\overline{K}/K)$ has infinite order.

Problem 14.10

Let F be a field of characteristic $p > 0$, let $a \in F$, and suppose that $f(x) = x^p - x - a \in F[x]$ is irreducible. If α is a root of $f(x)$, put $E = F(\alpha)$. Solve the following problems.

- (a) Prove that all roots of $f(x)$ are exactly $\alpha + c$, where $c \in \mathbb{F}_p$.
- (b) Prove that E/F is a Galois extension of degree p .
- (c) For every $c \in \mathbb{F}_p$, prove that there exists a unique $\sigma_c \in \text{Aut}(E/F)$ such that $\sigma_c(\alpha) = \alpha + c$. Prove that $\text{Aut}(E/F) = \{\sigma_c \mid c \in \mathbb{F}_p\}$, and hence prove that $\text{Aut}(E/F) \cong (\mathbb{F}_p, +)$.

Problem 14.11

Let k be a finite field of characteristic $p > 0$, let $F = k(t)$ be the field of rational functions in one variable over k , and let E be any finite extension of F . Prove the following.

- (a) If E/F is inseparable, then $k\left(t^{\frac{1}{p}}\right) \subseteq E$.
- (b) E/F is a simple extension.