ABSTRACT ALGEBRA

JACOB REINHOLD

Contents

1. Introduction

These are transcribed notes (with additional information) for a class at The University of Texas at Austin called Algebraic Structures I (M373K) taught by Giang Tran [1]. This course uses the textbooks "Topics in Algebra" by Herstein [2] and "Abstract Algebra" by Dummit and Foote [3].

Given that two books are used there is some inconsistency in notation; however, I have tried (and often failed) to point out when notation may be inconsistent. I have also included worked problems, for each section, that were given in class. The problems are from Herstein, Dummit and Foote, and a variety of other sources. I give no guarantee on the correctness of the solutions. Some of the problems would be more appropriately labeled theorems or propositions.

I occasionally use the symbol: [✓] when I am too lazy to finish typing a claim or statement.

2. Preliminaries

In this section, it would be standard to introduce basic set theory, define functions, and talk about relations and equivalence classes; however, I will assume the reader has familiarity with these topics. Instead, I will talk about properties of integers and the integers modulo n, i.e., $\mathbb{Z}/n\mathbb{Z}$.

Remark 2.1. One fact to note about equivalence classes which will be used and is not obvious is that equivalence classes partition a set.

2.1. Properties of the Integers.

Definition 2.2. If $a, b \in \mathbb{Z}\backslash\{0\}$, there is a unique positive integer d, called the *greatest common divisor* (gcd) of a and b, such that $d \mid a$, $d \mid b$, and if $e \mid a$ and $e \mid b$, then $e \mid d$.

The gcd of a and b is often noted (a, b). If $(a, b) = 1$, then a and b are *relatively prime*.

Definition 2.3. The *division algorithm* is defined as follows: for $a, b \in \mathbb{Z}\backslash\{0\}$, then there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad \text{and} \quad 0 \leqslant r < |b|$$

where q is the quotient and r the remainder.

2.2. Integers Modulo n.

Proposition 2.4. *The congruence relation, $a \equiv b \pmod{n}$, for $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}\backslash\{0\}$ is an equivalence relation.*

Proof.

(i) $a \equiv a \pmod{n}$ since $a - a = n \cdot 0$.

(ii) If $a \equiv b \pmod{n}$ then by definition of the relation, $a - b = nk$ for $k \in \mathbb{Z}$ which implies $b - a = n(-k)$. So $b \equiv a \pmod{n}$.

(iii) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a - b = nk$ and $b - c = nm$ for $k, m \in \mathbb{Z}$. So $a - c = n(k + m)$, i.e., $a \equiv c \pmod{n}$.

□

Since the congruence relation is an equivalence relation, the congruence classes partition the set of integers. For $\mathbb{Z}/n\mathbb{Z}$, there are n distinct equivalence classes mod n, denoted by $\bar{0}, \bar{1}, \ldots, \overline{n-1}$.

The operations of multiplication and addition on these classes are defined as expected,

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{and} \quad \bar{a} \cdot \bar{b} = \overline{ab}.$$

Note that these operations are well-defined, which means they do not depend on the choice of representatives for the classes involved. More precisely, if $a_1, a_2 \in \mathbb{Z}$ and $b_1, b_2 \in \mathbb{Z}$ with $\overline{a_1} = \overline{b_1}$ and $\overline{a_2} = \overline{b_2}$, then $\overline{a_1 + a_2} = \overline{b_1 + b_2}$ and $\overline{a_1 a_2} = \overline{b_1 b_2}$.

In general, to show that an operation [or map], say $\star$ on a set X, is well-defined, we need to show that for $x_1, x_2, y_1, y_2 \in X$ where $x_1 = x_2$ and $y_1 = y_2$, then $x_1 \star y_1 = x_2 \star y_2$ [$\star(x_1) = \star(x_2)$].

An important subset of $\mathbb{Z}/n\mathbb{Z}$ consists of the congruence classes which have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{there exist } \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \bar{a} \cdot \bar{c} = \bar{1}\}.$$

Remark 2.5. $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$.

2.3. **Worked Problems.** Here are some worked problems related to this section.

Problem 2.6. Find all integer solutions for $63x + 36y = -18$

Proof. First, let us simplify using basic algebra.

$$63x + 36y = -18 \implies 7x + 4y = -2$$

From this we get: $x \in \{-a \mid a \bmod 4 = 2, a \in \mathbb{Z}^{\geqslant 0}\}$, and $y \in \{b \mid b \bmod 7 = 3, b \in \mathbb{Z}^{\geqslant 0}\}$. Reverse the signs for a, b below zero in both cases so that all integers are covered. □

Problem 2.7. Let $a, b, c \in \mathbb{Z}$. Show that $(a, b) = (a, c)$ if $b \equiv c (\bmod\, a)$.

Proof. Suppose $b \equiv c (\bmod\, a)$. Then there exists $m, n \in \mathbb{Z}$ such that $b = ma + r$ and $c = na + r$, where $r \in \mathbb{Z}$ and $0 \leqslant r \leqslant a-1$. If $r \neq 0$, then b and c only share 1 as a common divisor; in this case 1 is the greatest common divisor. If $r = 0$, then $b = ma$ and $c = na$; so a divides both b and c. Now either a is the greatest common divisor for b and c, or the greatest common divisor of m and n is the greatest common divisor for b and c. □

Problem 2.8. If $(a, n) = 1$, prove that one can find $b \in \mathbb{Z}/n\mathbb{Z}$ such that $\overline{a}\overline{b} = \overline{1}$.

Proof. If $a, n \in \mathbb{Z}$ and $(a, n) = 1$, then a and n are coprime. Thus there exists $b, x \in \mathbb{Z}$ such that $ab + nx = 1$. Then $ab \equiv 1 \pmod{n}$, so $n \mid ab - 1$. Then for some integer x, $nx = ab - 1$. Fix x to be that integer. If we substitute this into $ab + nx = 1$ we get $2ab = 2$, so $ab = 1$. Since b is an integer, it exists in $\mathbb{Z}/n\mathbb{Z}$ as an equivalence class; say $\overline{b}$. Thus we have shown that there is some integer b such that $\overline{a}\overline{b} = \overline{1}$. □

Problem 2.9. Show that $(a + b)^p \equiv a^p + b^p (\bmod\, p)$ if p is prime.

Proof. Since all prime numbers are integers,

$$(a+b)^p = \binom{p}{0}a^p b^0 + \binom{p}{1}a^{p-1}b^1 + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}a^1 b^{p-1} + \binom{p}{p}a^0 b^p,$$

where $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. From this we see that $\binom{p}{k}$ is a multiple of p when $k \neq p$; the numerator will be the product of p and other terms, and p cannot be divided by $k!$ or $(p-k)!$ since p is prime and all terms are less than p. Then if we divide all terms by p, there will only be a nonzero remainder in the first and

last terms, i.e., $\binom{p}{0}a^p b^0$ and $\binom{p}{p}a^0 b^p$. So the total remainder will be the sum of those terms: $a^p + b^p$. Thus $(a+b)^p \equiv a^p + b^p \pmod{p}$.

□

3. Group Theory

Definition 3.1. Given a set G, a binary operation $\cdot$ on G,

$$G \times G \to G$$
$$(x, y) \mapsto x \cdot y$$

G is called a group if

(i) $(ab)c = a(bc)$, i.e., $\cdot$ is associative.
(ii) There exists an identity element, denoted $e \in G$ such that $ae = ea = a$, for all $a \in G$.
(iii) For all $a \in G$, there is a $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.

Here are some other properties of a group, say G. Let $a \in G$.

(1) The identity element is unique.
(2) Each inverse element a^{-1} is unique with respect to a.
(3) G is closed under $\cdot$.

Definition 3.2. A group G is abelian if $ab = ba$ for all $a, b \in G$. In this case, we denote the operation as +, and the identity as 0, and the inverse of a is $-a$.

Here are some more properties of groups. Let $x, y \in G$ a group.

(1) Cancellation law, $xy = xz \implies y = z$.
(2) $(xy)^{-1} = y^{-1}x^{-1}$.
(3) $(x^{-1})^{-1} = x$.

Problem 3.3. Given a set S. Denote $\Sigma = \{f : S \to S \text{ bijective}\}$. Then $(\Sigma, \circ)$ is a group called the symmetry group of S, where $\circ$ is function composition. If$|S| = n$, then $\Sigma = S_n$.

Here are properties of the symmetry group:

(1) $|S_n| = n!$
(2) S_n is not abelian for $n \geqslant 3$.

Proof.

(1) Every bijection from $S \to S$ is a permutation of S, and by simple combinatorics, the number of permutations of $S = n!$.
(2) [✓]

□

Definition 3.4. Given a group G and $a \in G$, $n \in \mathbb{Z}^+$,

$$a^n = \underbrace{a \cdot a \cdots a}_{n \text{ times}}$$
$$a^0 = e$$
$$a^{-n} = (a^{-1})^n$$

Other basic exponent properties hold. This is not too surprising.

Definition 3.5. Let G be a group, and $a \in G$. If for every $x \in G$, there is an $n \in \mathbb{Z}$ such that $a^n = x$, then a is the *generator* of G. This is denoted by $G = \langle a \rangle$.

Definition 3.6. A group G is cyclic if, and only if, there is a generator for G in G.

Definition 3.7. Given a group G, $a \in G$. The order of a is the smallest positive integer n such that $a^n = e_G$ (where e_G is the identity of G). We denote the order of a as $o(a)$ or $|a|$ (I will switch between both. I tend to use $o(\cdot)$ when we are talking about divisibility, since the vertical bars next to the vertical bar that represents "divides" looks awkward).

Proposition 3.8. *Let $a \in G$. If $a^k = e_G$ for some $k \in \mathbb{Z}^+$, then $o(a) \mid k$.*

Proof. Since $a^k = e_G$, then $o(a)$ is finite and positive. Let $o(a) = n$. We will use the division algorithm,

$$k = o(a) \cdot q + r, \qquad 0 \leqslant r < o(a)$$
$$a^k = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = a^r = e$$

Since $o(a)$ is the smallest positive integer: $a^n = e$, then r must equal 0. Which proves the claim. □

Corollary 3.9. *$a \in G$ a cyclic group, $a^k = a^m \implies m \equiv k \pmod{o(a)}$.*

3.1. **Subgroups.** Given a group G, let $H \subset G$.

Definition 3.10. H is called a subgroup of G if under the multiplication in G, H is a group. We denote this with $H \leqslant G$ (or $H < G$ if H is a proper subgroup).

Lemma 3.11. *Given a group G and $H \subset G$, and $H \neq \varnothing$. $H \leqslant G$ if, and only if, H is closed under multiplication and inverses.*

Proof. The forward direction is obvious. For the backward direction, we need to show H is closed under multiplication, multiplication is associative, H contains the identity, and is closed under inverse. By supposition, we only need to show H is associative and contains the identity. Note that H inherits associativity from G. Since H is closed under inverses and multiplication, then for $a \in H$, $a^{-1} \in H$ and $aa^{-1} = e \in H$. □

Lemma 3.12. *Given a group G, $H \subset G$ a finite nonempty subset. If H is closed under multiplication, then H is a subgroup of G.*

Proof. [✓] □

Definition 3.13. Given group G and $a \in G$. Define $H = \{a^n \mid n \in \mathbb{Z}\}$, then H is a subgroup of G generated by a. This is denoted by $\langle a \rangle$ (the same as before except $\langle a \rangle = H \leqslant G$).

Lemma 3.14. *If the order of a is finite, then $o(H) = o(a)$ (and H is the smallest group that contains a).*

Proof. Let $a^n, a^m \in H$ for some $n, m \in \mathbb{Z}$. Then $a^n a^m = a^{n+m} \in H$ so H is closed under multiplication. Further, $a^n \in H$, so $(a^n)^{-1} = a^{-n} \in H$. Thus $H \leqslant G$. □

Definition 3.15. Let G be a group and $a, b \in G$. a and b are called conjugate if there exists an element G in G such that $gag^{-1} = b$. Note that conjugacy is an equivalence relation, we denote the conjugacy classes as $\mathrm{cl}(x) = \{gxg^{-1} \mid g \in G\}$ for some x in a group (or set, which will be talked about in the group action section).

3.2. **Left and Right Cosets.**

Definition 3.16. Given a group G, $H \leqslant G$ a nonempty subgroup. Let $a \in G$. Then $aH = \{a \cdot x \mid x \in H\}$ is a *left coset* of H, and $Ha = \{x \cdot a \mid x \in H\}$ is a *right coset* of H.

Definition 3.17. If for every $a \in G$, $aH = Ha$, then H is called a normal subgroup of G and is denoted by $H \trianglelefteq G$ (or $H \lhd G$ for a normal proper subgroup).

Definition 3.18. If a group G has no nontrivial normal subgroup, then G is a simple group.

Remark 3.19. In general, a left coset does not equal the right coset.

Lemma 3.20. *Let $H \leqslant G$. Then $aH = H$ if, and only if, $a \in H$. Likewise, $Ha = H$ if, and only if, $a \in H$.*

Proof. We will only show this for the left cosets. The argument for the right cosets is exactly the same.

In the forward direction, $aH = H$, then $ah \in H$ for some $h \in H$. Let $k = ah$. Then $a = kh^{-1} \in H$.

Conversely, let $a \in H$. Then $aH \subset H$. Since $a^{-1} \in H$, $a^{-1} \subset H$. $H = eH = (aa^{-1})H = a(a^{-1}H) \subset aH$. Thus $aH = H$. □

Proposition 3.21. *Let $H \leqslant G$ a group.*

(1) $G = \bigcup_{a \in G} aH = \bigcup_{a \in G} Ha$.
(2) $aH = bH$ if, and only if, $a^{-1}b \in H$.
(3) Given $a, b \in G$, $aH \cap bH = \varnothing$ or $aH = bH$.

Proof.

(1) Let $a \in G$ such that $aH \subset G$, then $\bigcup_{a \in G} aH \subset G$. Note that $a \in G$ implies $a = ae \in aH$, and $G = \bigcup_{a \in G} a \subset \bigcup_{a \in G} aH$. All this together implies that $G = \bigcup_{a \in G} aH$.

(2)

$$\begin{aligned} aH = bH &\iff a^{-1}(aH) = a^{-1}(bH) \\ &\iff (a^{-1}a)H = (a^{-1}b)H \\ &\iff H = (a^{-1}b)H. \end{aligned}$$

This only happens if, and only if, $a^{-1}b \in H$.

(3) If $aH \cap bH = \varnothing$, we are done. If $aH \cap bH \neq \varnothing$ we need to show $aH = bH$. Let $x \in G$ such that $x \in aH \cap bH$. Then $x = ah_1 = bh_2$ for $h_1, h_2 \in H$. So $h_1 = a^{-1}bh_2$. Notice that $a^{-1}b = h_1h_2^{-1} \in H$, so $aH = bH$.

□

Definition 3.22. The number of left cosets of H in G is called the *index* of H in G, which we denote by $i_G(H)$ (or more commonly: $[G : H]$).

Theorem 3.23. *(Lagrange's Theorem) Let G be a finite group and $H \leqslant G$, then $|G| = |H| \cdot i_G(H)$.*

Proof. Let $T = \{aH \mid a \in G\}$ be the set of all left cosets of H in G. Since G is finite, T is finite (there is an injection $a \mapsto aH$ [✓]). Let $V = \{$all mutually disjoint left cosets of H in $G\}$. Then $|V| = i_G(H)$, and $G = \bigcup_{aH \in V} aH$, so $|G| = \sum_{aH \in V} |aH|$.

It suffices to show $|aH| = |H|$ (proof of this not shown here). Then

$$|G| = \sum_{aH \in V} |H| = |H| \cdot i_G(H).$$

□

Remark 3.24. If G is finite and $H \leqslant G$, then $|H|$ divides $|G|$.

Corollary 3.25. *Let G be a finite group, $a \in G$. Then $o(a) \mid o(G)$.*

Proof. Let $H = \langle a \rangle \leqslant G$, and $o(H) \mid o(G)$ and $o(H) = o(a) \mid o(G)$. □

Corollary 3.26. *G is a finite group, $a \in G$ implies $a^{|G|} = e$.*

Proof. $|G| = k \cdot |a|$ for $k \in \mathbb{Z}^+$. So $a^{|G|} = (a^{|a|})^k = e^k = e$. □

Definition 3.27. *Euler's totient function*, denoted by $\phi(n)$, counts the positive integers up to a given integer n that are relatively prime to n.

Corollary 3.28. *(Fermat's little theorem) Let p be a prime. Then $\phi(p) = p - 1$ which implies $a^{p-1} \equiv 1 \pmod{p}$ if $(a, p) = 1$. Or $a^p \equiv a \pmod{p}$ for every $a \in \mathbb{Z}$.*

Proof. `Click here` for a website with lots of proofs. □

Corollary 3.29. *A group of prime order is cyclic.*

Proof. Let G be a group with $o(G) = p$ a prime. Let $a \in G \backslash \{e\}$, $H = \langle a \rangle \leqslant G$. But $o(H) \mid o(G) = p$, which can only happen when $o(H) = 1$ or p. Since $H \neq \{e\}$ we get $o(H) = p = o(G)$ which means $H = G = \langle a \rangle$. □

3.3. **Normal Subgroups and Quotient Groups.**

Proposition 3.30. *The following three definitions are equivalent.*

1. *If $aH = Ha$, for all $a \in G$, then H is called a normal subgroup of G.*
2. *H is called a normal subgroup of G if $ghg^{-1} \in H$ for every $g \in G$, $h \in H$.*
3. *H is called a normal subgroup of G if $gHg^{-1} = H$ for all $g \in G$.*

Proof. We will show that definition 1 is equivalent to definition 2.

In the forward direction, $aH = Ha$, for all $a \in G$. Let $g \in G$, $x \in H$. Then $gH = Hg$ so $gx = h'g$ for some $h' \in H$. Then $gxg^{-1} = h'gg^{-1} = h'e = h' \in H$.

In the reverse direction, $ghg^{-1} \in H$, for all $g \in G$, $h \in H$. Fix g. Then $ghg^{-1} \in H$ implies $gh \in Hg$ for all $h \in H$. So $gH \subset Hg$. Similarly $gH \supset Hg$, so $gH = Hg$.

[✓] □

Definition 3.31. Given a group G, let $N \trianglelefteq G$. Then G/N is a group under the following operation. Let $aN, bN \in G/N$. Then the product of aN and bN is $(aN)(bN)$.

$$(aN)(bN) = a(Nb)N = a(bN)N = abN$$

Remark 3.32. $G/N := \{aN \mid a \in G\}$ is called the quotient group of G by N.

Lemma 3.33. *G is a finite group. $N \trianglelefteq G$. Then $|G/N| = i_G(N) = |G|/|N|$.*

3.4. **A Counting Principle.**

Definition 3.34. Let $H, K \leqslant G$. Define $HK = \{xy \mid x \in H, y \in K\} \supset He, eK$. In general, $HK \neq KH$ and $HK \nleqslant G$ (e.g. $G = S_3$).

Proposition 3.35. $|HK| = \frac{|H||K|}{|H \cap K|}$. *[✓]*

Lemma 3.36. *HK is a subgroup of G if, and only if, $HK = KH$. [✓]*

3.5. **Homomorphism.**

Definition 3.37. Let G, H be groups. A map $f : G \to H$ is a homomorphism if $f(xy) = f(x)f(y)$ for all $x, y \in G$.

Definition 3.38. For $f : G \to H$ a homomorphism, f is an isomorphism if f is a bijection. If there exists such a map, then we say G and H are isomorphic which we denote by: $G \cong H$.

Here are some properties of homomorphisms.

Proposition 3.39. *Let $f : G \to H$ be a homomorphism.*

(1) $f(e_G) = e_H$.
(2) $f(x^{-1}) = (f(x))^{-1}$.

Proof.

(1) $f(e_G e_G) = f(e_G)f(e_G)$ and $f(e_G e_G) = f(e_G) = f(e_G)e_H$ so, by the cancellation law, $f(e_G) = e_H$.
(2) $f(x)f(x^{-1}) = f(xx^{-1}) = f(e_G) = e_H$ which implies $f(x^{-1}) = (f(x))^{-1}$.

□

Lemma 3.40.

(1) Let $f : G \to G$ with $x \mapsto x$. Then f is an isomorphism to itself (also called an automorphism), sometimes denoted by id_G.
(2) If $f : G \to H$ is an isomorphism, then $f^{-1} : H \to G$ is an isomorphism.
(3) If $f : G \to H$ is an isomorphism and $g : H \to K$ is an isomorphism, then $g \circ f : G \to K$ is an isomorphism.

Thus isomorphism between groups defines an equivalence relation, i.e., if $S = \{\text{all groups}\}$ and $G, H \in S$, then $G \sim H$ if $G \cong H$ (there exists some isomorphism $f : G \to H$).

Theorem 3.41. *Every cyclic group is isomorphic to either $(\mathbb{Z}, +)$ or $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Proof. Let $G = \langle a \rangle$.

Case 1:

The order of a is n; $a^n = e$. Let $f : G \to \mathbb{Z}/n\mathbb{Z}$, $f(a^m) = \bar{m} = m + n\mathbb{Z}$. Now we will check f is a well-defined, bijective homomorphism.

First let's verify that f is well-defined. Note $a^{m_1} = a^{m_2} \implies \bar{m}_1 = \bar{m}_2$, and $m_1 \equiv m_2 \pmod{n}$ so $\bar{m}_1 = \bar{m}_2$.

Now let's check f is bijective. Let $a^{m_1} \neq a^{m_2}$ but $f(a^{m_1}) = \bar{m}_1 = f(a^{m_2}) = \bar{m}_2$. Then $m_1 = m_2 + nq$ for $q \in \mathbb{Z}$. $a^{m_1} = a^{m_2+nq} = a^{m_2}(a^n)^q = a^{m_2}$. But this is a contradiction, so f is injective. f is surjective clearly, so f is a bijection.

Finally, let's check f is a homomorphism. $f(a^m) + f(a^k) = (m + n\mathbb{Z}) + (k + n\mathbb{Z}) = (m + k) + n\mathbb{Z}$. And $f(a^m a^k) = f(a^{m+k}) = (m + k) + n\mathbb{Z}$. Since these two quantities are equal, f is a homomorphism. Which proves the claim.

Case 2:

Let $|a| = \infty$, so $a^n \neq e$ for all $n \in \mathbb{Z}\backslash\{0\}$. Let $f : G \to \mathbb{Z}$ and $f(a^m) = m$. [✓] □

Definition 3.42. Let $f : G \to H$ be a group homomorphism. Then the Im $f = \{f(x) \mid x \in G\}$ and ker $f = \{x \in G \mid f(x) = e_H\}$.

Lemma 3.43.

(1) Im f *is a subgroup of* H.
(2) ker f *is a normal subgroup of* G.
(3) f *is surjective if, and only if,* Im $f = H$.
(4) f *is injective if, and only if,* ker $f = \{e_G\}$.

Theorem 3.44. *(Three isomorphism theorems)*

(1) Let $f : G \to H$ be a group homomorphism, then $G/\ker f \cong \text{Im } f$.
(2) (Diamond isomorphism) Let G be a group, $K \leqslant G$ and $N \trianglelefteq G$. Then $KN/N \cong K/K \cap N$.
(3) Let G be a group, $H \subset K \trianglelefteq G$ implies $H \lhd K$.

Proof. [✓] □

Theorem 3.45. *(Cayley's theorem) Every group $G \cong$ subgroup of $\Sigma(G) = \{h : G \to G \text{ bijective}\}$. An alternate way of stating this is: every group G is isomorphic to a subgroup of the symmetric group acting on G (the definition of which will be explained shortly).*

Proof. [✓] □

Theorem 3.46. *Let $\phi : G \to H$ be a group homomorphism. Then* ker $\phi \trianglelefteq G$.

Proof. Note that ker $\phi \leqslant G$ [✓]. Let $k \in \ker \phi$, $x \in G$. Then

$$\begin{aligned}\phi(xkx^{-1}) &= \phi(x)\phi(k)(\phi(x))^{-1} \\ &= \phi(x)(\phi(x))^{-1} \\ &= e_H\end{aligned}$$

Thus $xkx^{-1} \in \ker \phi$, which proves the claim. □

Remark 3.47. Let G be a group, $H \leqslant G$, and S be the collection of all left cosets of H on G. Let $\Sigma(S)$ be the set of all bijections from S to S. Then $|\Sigma(S)| = (i_G(H))!$.

Let $\tau \in \Sigma(S)$. If $o(G) \nmid (i_G(H))!$, then ker $\tau \neq \{e\}$.

3.6. **Group Action.** The several next definitions are almost directly lifted from Dummit and Foote who seemed to best write about the topic [3].

Definition 3.48. A *group action* of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$), for all $g \in G$ and $a \in A$) satisfying the following properties:

(1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G$, $a \in A$;
(2) $e_G \cdot a = a$ for all $a \in A$.

We say that G is a group acting on a set A.

Intuitively, a group action of G on a set A means that every element g in G acts as a permutation on A in a manner consistent with the group operations in G. There is also a notion of *left* action (which we have shown) and *right* action.

For the following three defintions, let G be a group, and $A \subset G$, for $A \neq \varnothing$.

Remark 3.49. The below several definitions are pulled from both Dummit and Foote and Herstein, so there is some overlap.

Definition 3.50. Define $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the centralizer of A in G. Since $gag^{-1} = a$ if, and only if, $ga = ag$, $C_G(A)$ is the set of elements of G which commute with every element of A.

Definition 3.51. Define $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$, the set of elements commuting with all elements of G. This is called the *center* of G.

Definition 3.52. Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. Define the *normalizer* of A in G to be the set $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$.

Definition 3.53. Given a group G, set X, an a group action of G on X. Let $x_1, x_2 \in X$. Define $x_1 \sim x_2$ if, and only if, there is a $g \in G$ such that $gx_1 = x_2$. Note that this is an equivalence relation.

Definition 3.54. Let G act on a set X and let x be some fixed element of X. Define the *stabilizer* of x in G to be $G_x = \{g \in G \mid g \cdot x = x\}$. This is sometimes denoted as $N(x)$ as well.

Define the set of all fixed points to be $X^G = \{x \in X \mid gx = g, \forall g \in G\}$.

Definition 3.55. Let G be a group that acts on a set X. Define the *orbit* of a group element x as $G(x) = \{g \cdot x \in X \mid g \in G\}$.

For the next following sections, let $\mathrm{cl}(x) = \{gxg^{-1} \mid g \in G\}$ for some set X on which the group G acts.

Theorem 3.56. *If G is finite, $|\mathrm{cl}(x)| = |G|/|G_x|$.*

Proof. Let $f : G/G_x \to \mathrm{cl}(x)$. Then $f(g \cdot G_x) = g \cdot x$. First we show that f is well-defined. If $g_1 \cdot G_x = g_2 G_x$ then $g_1^{-1} g_2 \in G_x$. So $g_1^{-1} g_2 x = x$. Then $g_1 \underbrace{(g_1^{-1} g_2 x)}_{=g_2 x} = g_1 x$. So $f(g_1 G_x) = f(g_2 G_x)$. So f is well-defined.

f is injective. If $g_1 H \neq g_2 H$ for some $H \leqslant G$, then $g_1 x \neq g_2 x$.
f is surjective. Let $x' \in \mathrm{cl}(x)$. Then $x' = gx$ for some $g \in G$. Then $f(gG_x) = gx = x'$.
So $|G|/|G_x| = [G : G_x] = |G/G_x| = |\mathrm{cl}(x)|$. □

Definition 3.57. Consider the following group action: $G \times G \to G$, and $(g, x) \mapsto gxg^{-1}$. Then $G = \bigcup_{\text{disjoint}} \mathrm{cl}(x)$ and $|G| = \sum_{\text{disjoint}} |\mathrm{cl}(x)|$. Let G be a finite group, $Z(G)$ be its center. Then we have $|G| = |Z(G)| + \sum_{\text{disjoint } G_x} \frac{|G|}{|G_x|}$. This is called the *class equation*.

Corollary 3.58. *If $|G| = p^n$, for $n \geqslant 1$ and p prime, then $Z(G) \neq \{e\}$.*

Proof. nah. [✓] □

Proposition 3.59. *Let $X^G = \{x \in X \mid gx = g, \forall g \in G\}$. If G is a p-group, i.e., $|G| = p^n$, then $|x| \equiv |x^G| + \sum_{G_x \neq G, \text{disjoint classes}} \frac{|G|}{|G_x|}$. This is an extension of the class equation.*

Theorem 3.60. *(Cauchy's Theorem) If G is a group, p prime, $p \mid o(G)$, then G has an element of order p.*

Remark 3.61. There are too many "Cauchy's theorems".

Proof. [✓] □

Corollary 3.62.

(1) If $p \mid o(G)$, p prime, then G has subgroup of order p.
(2) If $o(G) = p^2$, then G is abelian.

Examples 3.63. Here are some examples of group action (besides the last) that we talked about in the review for the final (so some of these may be slightly out of place).

(1) Left translation: $G \times G \to G$, $(g, x) \mapsto gx$.
(2) Left translation: $G \times G/H \to G/H$, $(g, xH) \mapsto gxH$, where $H \leqslant G$.
(3) $G \times \mathrm{Aut}(G) \to \mathrm{Aut}(G)$, $(g, \sigma) \mapsto g \cdot \sigma : G \to G$, $a \mapsto g \cdot \sigma(a)$.
(4) Conjugation: $G \times G \to G$, $(g, x) \mapsto g \cdot x := gxg^{-1}$.
(5) Let $\mathcal{G} = \{\text{all subgroups of } G\}$. $G \times \mathcal{G} \to \mathcal{G}$, $(g, H) \mapsto gHg^{-1}$.
(6) Let $\mathcal{P} = \{\text{all } p\text{-Sylow subgroups of } G\}$. $G \times \mathcal{P} \to \mathcal{P}$, $(g, P) \mapsto gPg^{-1}$.
(7) If $(g, x) \mapsto xg$, then $(g_1g_2) \cdot x = xg_1g_2 \neq g_1 \cdot (g_2 \cdot x) = g \cdot (xg_2) = xg_2g_1$. So this is not a group action.

3.7. **Sylow Theorems.** Sylow theorems are an important finding in the subject of finite group theory. They generalize Cauchy's theorem and are important in the classification of finite simple groups. The following is (almost) taken directly from Dummit and Foote.

Definition 3.64. Let G be a group and let p be prime.

(1) A group of order p^α for some $\alpha \in \mathbb{Z}_+$ is called a p-group. Subgroups of G which are p-groups are p-subgroups.
(2) If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a Sylow p-subgroup of G.
(3) The set of Sylow p-subgroups of G will be denoted by $Syl_p(G)$ and the number of Sylow p-subgroups of G will be denoted by $n_p(G)$ (or just n_p when G is clear from context).

Theorem 3.65. *(Sylow theorems) Let G be a group of order $p^\alpha m$, where p is prime and does not divide m.*

(1) Sylow p-subgroups of G exist.
(2) If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leqslant gPg^{-1}$, i.e., Q is contained in some conjugate of P. In particular, any two Sylow p-subgroups of G are conjugate in G.
(3) The number of Sylow p-subgroups of G is of the form 1 + kp, i.e.,

$$n_p \equiv 1 \pmod{p}.$$

Further, n_p is the index in G of the normalizer $N_G(P)$ for any Sylow p-subgroup P, hence n_p divides m.

Lemma 3.66. *Let H be a p-subgroup of the finite group G, then $[N(H) : H] \equiv [G : H] \pmod{p}$.*

Proof. [✓] □

Proof. This proof is very long. If you are interested, then there are proofs available online or in Dummit and Foote/Herstein. [✓] □

Remark 3.67. Let G be a finite group. The follow statements are equivalent. Trust me.

(1) Every Sylow p-subgroup of G is a normal subgroup in G.
(2) There exists a Sylow p-subgroup H of G such that $H \lhd G$.
(3) There is only one Sylow p-subgroup of G.

3.8. **Group Product.** In this section we will talk about external and internal direct products of groups and their applications.

Definition 3.68. Let $G_1, G_2, \ldots, G_n$ be groups. $G := G_1 \times G_2 \times \cdots G_n$ is a group called the *external direct product* of G_i.

G has elements $(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n)$ and multiplication of these two elements equals $(x_1y_1, x_2y_2, \ldots, x_ny_n)$.

Definition 3.69. Let $H_1, H_2, \ldots, H_n$ be normal subgroups of G. Then G is called an *internal direct product* of $\{H_i\}$ if and only if, for all $g \in G$, there is a unique way to write $g = h_1h_2 \cdots h_n$ for $h_i \in H$. We say $G = H_1 \cdot H_2 \cdots H_n$.

Remark 3.70. Suppose G is an internal direct product of $H_1, H_2, \ldots, H_n$, then

(1) $H_i \cap H_j = \{e\}, i \neq j$.
(2) For all $x \in H_i$, $y \in H_j$ $xy = yx$ (elementwise commutative)
(3) If $h_1h_2 \cdots h_n = e$, then $h_1 = h_2 = \cdots = h_n = e$.
(4) $G = H_1H_2 \cdots H_n$.
(5) $|G| = |H_1| \cdot |H_2| \cdots |H_n|$.

Remark 3.71. Let $H, K \lhd G$.

(1) $hk = kh$, for all $h \in H$, $k \in K$.
(2) If $hk = e$, then $h = k = e$ if and only if $H \cap K = \{e\}$.
(3) $G = HK$ and $|G| = |H||K|$.

Then G is the internal direct product of H and K and $G \cong H \times K$.

Theorem 3.72.

(1) If group G is an internal direct product of normal groups $H_1, H_2, \ldots, H_n$ then $G \cong H_1 \times H_2 \times \cdots \times H_n$.
(2) If $G = \times_i G_i$ is an external direct product, then $G = H_1 \cdot H_2 \cdots H_n$ and $H_i \cong G_i$.

Proof. [✓] □

Theorem 3.73. *Let G be a finite group, $o(G) = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $\alpha_i \geqslant 1$ where p_j are distinct primes.*

Let H_i be a Sylow p_i-subgroup of G. Then G is the interal direct product of $\{H_i\}_{i=1}^k$ if and only if $H_i \lhd G$.

Proof. [✓] □

3.9. **Symmetric Groups.** Recall Cayley's theorem, i.e., that every group of order n is isomorphic to a subgroup of $S_n := \{\text{all permutations of } \{1, 2, \ldots, n\}\}$ which is a group with composition ($\circ$) as multiplication, i.e., for $\tau, \sigma \in S_n$, $\tau \circ \sigma(x) = \tau(\sigma(x)) \in S_n$ for all $x \in \{1, 2, \ldots, n\}$.

Here are some properties of symmetric groups:

(1) $|S_n| = n!$.

(2) S_n is non-abelian for $n \geqslant 3$.
(3) Every non-abelian group of order 6 is isomorphic to S_3.
(4) S_n is not simple.

Definition 3.74.

(1) $\sigma \in S_n, \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$
(2) A k-cycle $\sigma \in S_n$, then there exists $a_1, a_2, \ldots, a_k \in \{1, \ldots, n\}$ such that $\sigma(a_1) = a_2, \ldots, \sigma(a_{k-1}) = a_k, \sigma(a_k) = a_1$.
(3) Two cycles $\sigma = (a_1\ a_2\ \cdots\ a_k), \tau = (b_1\ b_2\ \cdots\ b_m)$ are called disjoint if $a_i \neq b_j$ for all i, j. Then $\sigma\tau = \tau\sigma$.

Proposition 3.75. *Every element $\sigma \in S_n$ can be written as the product of disjoint cycles, unique up to permutation of factors.*

Example 3.76. $\sigma \in S_5, \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$. Then $\sigma = (1\ 3)(2\ 4\ 5)$. The type of $\sigma = (2, 3)$.

Definition 3.77. Let $\sigma \in S_n$ be a permutation. The (cycle) type of σ is the data of how many cycles of each length are present in the cycle decomposition of σ.

Proposition 3.78. *The number of conjugation classes* ($\mathrm{cl}(a) = \{b \in G \mid \exists g \in G : b = gag^{-1}\}$) *in S_n is equal to the number of paritions of n.*

Recall: a partition of n is $(n_1, n_2, \ldots, n_k)$, where $1 \leqslant n_1 \leqslant \cdots \leqslant n_k$ for $n_i \in \mathbb{Z}$ and $\sum n_i = n$.

Example 3.79. $n = 3, 3 = 1 + 1 + 1 = 1 + 2$.
$S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.
Type: 1st class - 1, 2nd class - 3, 3rd class - 2 = 6.

Definition 3.80. $\sigma \in S_n$, consider $\Delta = \prod_{i<j}(x_i - x_j)$. Define $\sigma(\Delta) = \prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)})$. Then $\sigma(\Delta)$ will contain $x_i - x_j$ or $x_j - x_i$ for all $i < j$. Define $\mathrm{sgn}(\sigma) = \frac{\sigma(\Delta)}{\Delta} = \pm 1$.

Definition 3.81. $\sigma \in S_n$, $\sigma =$ product of disjoint cycles. $(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_k)(a_1\ a_{k-1}) \cdots (a_1\ a_2)$. Then $\mathrm{sgn}(\sigma) = (-1)^{\#\text{ of 2-cycles in decomposition of } \sigma \text{ in terms of 2-cycles}}$.

Proposition 3.82. $\mathrm{sgn} : S_n \to \{\pm 1\}$ *is a surjective homomorphism and* $S_n/\ker \mathrm{sgn} \cong \mathrm{Im}(\mathrm{sgn})$. *Denote* $A_n = \ker \mathrm{sgn} \lhd S_n$. *Then* $|S_n/A_n| = 2$ *so* $|A_n| = n!/2$. A_n *are all even permutations normal in* S_n.

3.10. **Finite Abelian Groups.**

Theorem 3.83. *For every finite abelian group G*

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

where 1) $n_i \geqslant 2$, 2) $n_{i+1} \mid n_i$, 3) $n = n_1 n_2 \cdots n_k$ and $(n_1, n_2, \ldots, n_k)$ is called the invariant factor of G, 4) n_1 contains all the prime divisors of n, and 5) If n is square free $n = p_1 p_2 \cdots p_k$, for p_i prime and $G \cong \mathbb{Z}/n\mathbb{Z}$ cyclic.

Example 3.84. $n = 180$, classify all finite abelian groups of order n.
Note $180 = 2^2 \cdot 3^2 \cdot 5$, $n_1 = \underbrace{2^2 \cdot 3^2 \cdot 5}_{G \cong \mathbb{Z}/180\mathbb{Z}}$. [✓]

3.11. **Worked Problems.** Here are worked problems relevant to the group theory section.

Problem 3.85. Let G be the set of all 2×2 matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where a, b, c, d are real numbers such that $ad - bc = 1$.

Define the operation $\cdot$ in G as the normal multiplication of matrices. Verify that G is a non-abelian, infinite group.

Proof. First we will show that G is closed under $\cdot$. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad B = \begin{pmatrix} w & x \\ y & z \end{pmatrix},$$

where $ad - bc = 1$ and $wz - xy = 1$. Then $A \cdot B$ is equal to

$$A \cdot B = \begin{pmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{pmatrix}$$

So we must show that $(aw + by)(cx + dz) - (ax + bz)(cw + dy) = 1$. Note that after some basic algebra that $(aw + by)(cx + dz) - (ax + bz)(cw + dy) = (ad - bc)(wz - xy)$, which equals 1. Thus G is closed under $\cdot$.

Next we will show that G is associative. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad B = \begin{pmatrix} w & x \\ y & z \end{pmatrix}, \qquad C = \begin{pmatrix} i & j \\ k & l \end{pmatrix}$$

where $ad - bc = 1$, $wz - xy = 1$, and $il - jk = 1$. We must show that $A \cdot (B \cdot C) = (A \cdot B) \cdot C$. Note

$$A \cdot B = \begin{pmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{pmatrix}$$

so

$$(A \cdot B) \cdot C = \begin{pmatrix} (aw + by)i + (ax + bz)k & (aw + by)j + (ax + bz)l \\ (cw + dy)i + (cx + dz)k & (cw + dy)j + (cx + dz)l \end{pmatrix}.$$

And

$$B \cdot C = \begin{pmatrix} wi + xk & wj + xl \\ yi + zk & yj + zl \end{pmatrix}$$

so

$$A \cdot (B \cdot C) = \begin{pmatrix} a(wi + xk) + b(yi + zk) & a(wj + xl) + b(yj + zl) \\ c(wi + xk) + d(yi + zk) & c(wj + xl) + d(yj + zl) \end{pmatrix}.$$

After some basic algebra we see that both $A \cdot (B \cdot C)$ and $(A \cdot B) \cdot C$ are equal. Thus $\cdot$ is associative.

Now we must show that there exists an identity element $e \in G$. Define e as

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

We can verify that this is the identity element by multiplying it by an arbitrary matrix, say A from before. Then

$$e \cdot A = \begin{pmatrix} 1(a) + 0(c) & 1(b) + 0(d) \\ 0(a) + 1(c) & 0(b) + 1(d) \end{pmatrix} = A, \qquad A \cdot e = \begin{pmatrix} a(1) + c(0) & b(1) + d(0) \\ a(0) + c(1) & b(0) + d(1) \end{pmatrix} = A.$$

Thus G contains an identity element.

Finally we must show that all elements of G have an inverse. From A, defined as before, we now will define $A^{-1} \in G$ as

$$A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Then

$$A^{-1} \cdot A = \begin{pmatrix} d(a) - b(c) & d(b) - b(d) \\ -c(a) + a(c) & -c(b) + a(d) \end{pmatrix} = e, \quad A \cdot A^{-1} = \begin{pmatrix} a(d) - c(b) & b(d) - d(b) \\ a(-c) + c(a) & b(-c) + d(a) \end{pmatrix} = e.$$

Since A and A^{-1} are are defined with arbitrary elements, we see that all elements of G have an inverse.

Since G is closed under multiplication, is associative, contains an identity, and all elements have an inverse, we have shown that G is a group.

Now we must show that G is non-abelian. Define A and B as before. Then

$$A \cdot B = \begin{pmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{pmatrix} \neq B \cdot A = \begin{pmatrix} aw + cx & bw + dx \\ ay + cz & by + dz \end{pmatrix}.$$

Thus $\cdot$ is not commutative, i.e., non-abelian.

Now we must show that G is infinite. Take

$$A = \begin{pmatrix} ka & kb \\ c/k & d/k \end{pmatrix},$$

where $a, b, c, d \in \mathbb{R}$ such that $ad - bc = 1$ and take let k be any non-zero real number. Then $A \in G$, and since k is an arbitrary element of an infinite set, we see that G must also have infinite elements. □

Remark 3.86. The above proof would be greatly simplified using basic knowledge of linear maps.

Problem 3.87. Given a group G and $a, b \in G$ such that $ab = ba$. Prove that $(ab)^n = a^n b^n$, for all $n \in \mathbb{Z}$.

Proof. Note that $(ab)^n$ can be rewritten as: $(ab)(ab) \cdots (ab)$, where there are n multiplications. Since G is a group, multiplication is associative so the order in which we multiply the elements does not matter, so we can remove the parentheses, i.e., we now have: $abab \cdots ab$. Then since we are told that G is abelian, we can switch the order of the elements and group them, like $ab(ba) \cdots ab$, one-by-one into a series of multiplications that looks like: $aa \cdots abb \cdots b$, where there are n multiplications of a and n multiplications of b. This is equivalent to $a^n b^n$. As desired. □

Problem 3.88. Assume $G = \{e, a, b, c\}$ is a group of order 4 with identity e and G has no elements of order 4. Show that there is a unique multiplication table for G.

Proof. We are asked to find a non-cyclic group G of order 4. Recall that for $a \in G$, $o(a)|o(G)$. Thus the only possible orders of elements are 1 and 2 since we are excluding 4 by supposition. Since there are no elements of order 4, all elements must be of order 2; if any element is order 1 that element is the identity.

The Klein four-group satisfies this proposition, and we have shown it is unique up to isomorphism.

TABLE 1. Multiplication table for Klein four-group

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

□

Problem 3.89.

(1) Show that if $a^2 = e$ for all elements of a group G, where e is the identity of G, then G is abelian.
(2) Prove that if G is a finite group of even order, then G contains an element of a of order 2.
(3) Show that every subgroup of index 2 is normal.

Proof.

(1) Let $a, b \in G$. Then $ab \in G$. By our supposition $(a \cdot b)^2 = (ab)(ab) = e$. Our supposition also implies that $a = a^{-1}$, and $b = b^{-1}$. Thus $(b^{-1}a^{-1})(ab)(ab) = b^{-1}a^{-1} \implies ab = ba$.
(2) Pair every element of $G\backslash\{e\}$ with its inverse. This pairing is an equivalence relation that partitions $G\backslash\{e\}$. Since there are an even number of elements in G, if all pairs consist of different elements, then there would be an even number of pairings for $G\backslash\{e\}$. Thus there must exist some $a \in G$ such that $a = a^{-1}$ and $a \neq e$, i.e., a is of order 2.
(3) Let $H \leqslant G$ where G is a group, and let H be of index 2. Then H has 2 left and right cosets: for $g \in H$ and for $g \notin H$. For $g \in H$, $gH = H = Hg$, i.e., normal. For $g \notin H$, $gH = G\backslash H$ since there are only 2 cosets (which partition G). Likewise, $Hg = G\backslash H$. Since those two quantites are equal, and in both cases $gH = Hg$, we see H is normal.

□

Lemma 3.90. *A subgroup of a cyclic group is cyclic.*

Proof. Let $H \leqslant \langle a \rangle$. Let m be the smallest positive integer such that $a^m \in H$. Let $a^x \in H$. By the division algorithm we can write $x = mq + r$, for some $q \in \mathbb{Z}$ and $0 \leqslant r < m$. So

$$a^x = a^{mq+r} = (a^m)^q a^r.$$

Thus $(a^m)^{-q} \in H$, since $a^{-m} \in H$. We see that $a^x \cdot (a^m)^{-q} = a^r$. But this must equal e, since an $r < m$ such that $a^r \in H$ contradicts our assumption that m was the minimal integer, thus a^m generates H. As desired. □

Problem 3.91.

(1) Prove that for any positive integer n, the set of all complex n^{th}-roots of unity

$$G = \{z \in \mathbb{C} \mid z^n = 1\}$$

forms a group with respect to complex multiplication. Show that this group is cyclic.
(2) Show that if G is a cyclic group of order n and $k|n$, then G has exactly one subgroup of order k.

Proof.

(1) The complex n^{th}-roots of unity are complex numbers of unit-length, that sit on the unit circle in the complex plane. For example, the 5^{th}-roots of unity have 5 principal roots on the unit circle that are spaced apart equally, starting at 1 on the real line. Note that unit-length complex multiplication is a rotation in the complex plane. Thus for the n^{th}-roots of unity, we need to find a complex number which rotates 1 around the unit circle making n distinct points. Note that any number $z \in \mathbb{C}$ can be rewritten as $re^{i\theta}$, where r is the radius away from the origin and θ is the angle counter-clockwise from the real axis. Since we are unit-length, $r = 1$ for all our solutions, so we must only increment θ by a fixed value at integer multiples. Thus our solution must be of the form: $e^{2\pi ik/n}$, for $k \in \mathbb{Z}$.

So $G = \{e^{2\pi ik/n} \mid k \in \mathbb{Z}\}$. Now we must show that G is closed under multiplication. Let $e^{2\pi ix/n}, e^{2\pi iy/n} \in G$. Then $e^{2\pi ix/n} \cdot e^{2\pi iy/n} = e^{2\pi i(x+y)/n} \in G$ since $x + y \in \mathbb{Z}$. Thus G is closed under multiplication.

Now we will show multiplication on G is associative. Let $e^{2\pi ix/n}, e^{2\pi iy/n}, e^{2\pi iz/n} \in G$. Then $(e^{2\pi ix/n} \cdot e^{2\pi iy/n}) \cdot e^{2\pi iz/n} = e^{2\pi i(x+y)/n} \cdot e^{2\pi iz/n} = e^{2\pi i(x+y+z)/n}$. Also $e^{2\pi ix/n} \cdot (e^{2\pi iy/n} \cdot e^{2\pi iz/n}) = e^{2\pi ix/n} \cdot e^{2\pi i(y+z)/n} = e^{2\pi i(x+y+z)/n}$. Since these two quantities are equal, $\cdot$ on G is associative.

Now we must show that there exists an identity element in G. That element is $e^{2\pi i0/n} = 1$. Since 1 times any complex number is that complex number, there exists an identity element.

Now we will show that there exists inverse elements in G. Let $e^{2\pi ix/n} \in G$. Then $e^{2\pi i(-x/n)} \in G$ and $e^{2\pi ix/n} \cdot e^{2\pi i(-x/n)} = e^{2\pi i(x-x)/n} = 1$. Thus all elements in G have an inverse element.

Since G is closed under multiplication, associative, has an identity, and has inverses, G is a group.

To show G is cyclic we must only notice that $\cdots = e^{2\pi i(-n/n)} = e^{2\pi i0/n} = e^{2\pi i(n/n)} = e^{2\pi i(2n/n)} = \cdots$, by Euler's identity. Thus $e^{2\pi i/n}$ is the generator for the group, since, as explained before, that is the element of unit-length multiplication that rotates 1 around the unit-circle $n - 1$ times, for n distinct elements. However, as that generator is multiplied more than n times, it will only continue around the circle hitting the same spots as it hit before.

(2) Let $G = \langle a \rangle$ be a cyclic group of order n, and let $\langle a^x \rangle = H \leqslant G$, $\langle a^y \rangle = K \leqslant G$ be subgroups of order k, where $k|n$. Let $x = n/k$. Notice $(a^y)^k$ must equal e, so for some $q \in \mathbb{Z}$, $qn = yk$. However, this implies $y = q \cdot (n/k) = qx$. Since they are of the same order, q must equal 1. Thus $H = K$.

□

Problem 3.92. Show that if H and K are subgroups of G, then $H \cap K$ is also a subgroup of G. Moreover, if H and K are finite of relatively prime orders, then show that $H \cap K = \{e\}$.

Proof. Let $H, K \leqslant G$. Then $x \in H \cap K$ implies $x \in H$ and $x \in K$. Fix $x, y \in H \cap K$. We see that $x \cdot y \in H$ and $x \cdot y \in K$, thus $x \cdot y \in H \cap K$. Next, we know that H and K both inherit associativity, so $H \cap K$ is associative. e is in both H and K, so e is in $H \cap K$. $x^{-1} \in H$ and $x^{-1} \in K$, so $x^{-1} \in H \cap K$. Thus $H \cap K$ is a subgroup of G. □

Lemma 3.93. *An infinite cyclic group has infinitely many subgroups.*

Proof. Let G be an infinite cyclic group. Let $\langle g^n \rangle \leqslant G$ for $n \in \mathbb{Z}^{\geqslant 0}$. Notice that for $n < m$, $g^n \in \langle g^n \rangle$ but $g^n \notin \langle g^m \rangle$. Thus $\langle g^n \rangle \neq \langle g^m \rangle$, as desired. □

Problem 3.94. Show that if G has only a finite number of subgroups, then G is finite.

Proof. Define $\langle g \rangle$ as the (cyclic) subgroup generated by $g \in G$, a group that has only a finite number of subgroups. Note that all $\langle g \rangle$ must be finite, because an infinite cyclic group has infinitely many subgroups. So we can write $G = \bigcup_{g \in G} \langle g \rangle$, i.e., the finite union of sets with finite elements. Hence G is finite. □

Problem 3.95. Denote $(\mathbb{Z}/n\mathbb{Z})^* = \{cl(a) \mid (a, n) = 1\}$. Show that $(\mathbb{Z}/9\mathbb{Z})^*$ is a cyclic group. Find all its generators.

Proof. Note that $(\mathbb{Z}/9\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$. This is closed under multiplication since if $(a, n) = 1$ and $(b, n) = 1$ then $(ab, n) = 1$. Since this is finite and closed under multiplication, this is a group. Notice that $\bar{2} \cdot \bar{2} = \bar{4}, \bar{4} \cdot \bar{2} = \bar{8}, \bar{8} \cdot \bar{2} = \bar{16} = \bar{7}, \bar{7} \cdot \bar{2} = \bar{14} = \bar{5}$, and $\bar{5} \cdot \bar{2} = \bar{10} = \bar{1}$. Thus $\bar{2}$ is a generator of $(\mathbb{Z}/9\mathbb{Z})^*$, so $(\mathbb{Z}/9\mathbb{Z})^*$ is cyclic.

Note $\bar{5} \cdot \bar{5} = \bar{25} = \bar{7}, \bar{7} \cdot \bar{5} = \bar{35} = \bar{8}, \bar{8} \cdot \bar{5} = \bar{40} = \bar{4}, \bar{4} \cdot \bar{5} = \bar{20} = \bar{2}$, and $\bar{2} \cdot \bar{5} = \bar{10} = \bar{1}$. Thus $\bar{5}$ is another generator for $(\mathbb{Z}/9\mathbb{Z})$ (and is the only other one). □

Lemma 3.96. *Every group of prime order is cyclic.*

Proof. Let $o(G) = p$ for p prime. Let $a \in G$ such that $a \neq e$. Then $\langle a \rangle \leqslant G$. So by Lagrange's Theorem we get $o(\langle a \rangle) \mid o(G)$. Since the only number that can divide p is 1 and p, and we have stated that a is not order 1, we see $o(\langle a \rangle) = p$. Since there is an element in G which generates all other elements of G, G is cyclic. □

Problem 3.97. Find the non-cyclic group of smallest order.

Proof. The smallest order of a non-cyclic group must be 4 since every group of prime order is cyclic, and the trivial group is cyclic. The name of this group is the Klein four-group and its multiplication table is in the proof of example 3.88. □

Problem 3.98. Let H be a subgroup of a group G. Show that there is a bijection between the set of left cosets of H in G and the set of right cosets of H in G.

Proof. Consider the map ϕ which takes gH to Hg^{-1}, for $g \in G$. We will first show ϕ is well-defined. Let $a, b \in G$. Notice $aH = bH$ if and only if $a^{-1}b \in H$. Then $(a^{-1}b)^{-1} = b^{-1}a \in H$. Thus $b^{-1}(a^{-1})^{-1} \in H$, which implies $Ha^{-1} = Hb^{-1}$. So ϕ is well-defined.

Now we will show ϕ is injective. Let $a, b \in G$ such that $\phi(aH) = \phi(bH)$. Then $Ha^{-1} = Hb^{-1}$, which implies $a^{-1} = e_G a^{-1} = hb^{-1}$ for $h \in H$. It follows that $a^{-1}b = h$, so $ab^{-1} = h^{-1}$. Thus $b^{-1}a \in H$, which means $aH = bH$. So ϕ is injective.

Now we will show ϕ is surjective. Let $g \in G$. Note $g = (g^{-1})^{-1}$, so $Hg = \phi(g^{-1}H)$. Thus ϕ is surjective.

Since ϕ is a well-defined, injective, and surjective map, ϕ is a bijection. □

Problem 3.99. Let H be a subgroup of a group G. Suppose that for any $a \in G$, there exists $b \in G$ such that $aH = Hb$. Show that H is a normal subgroup of G.

Proof. Note that $a = ae \in aH$, which, by assumption, means $a \in Hb$. Further notice $a = ea \in Ha$, so $a \in Ha \cap Hb$, i.e., $Ha \cap Hb \neq \varnothing$. Thus $Hb = Ha = aH$. As desired. □

Problem 3.100. If H is a subgroup of G, let $N(H) = \{g \in G \mid gHg^{-1} = H\}$. Prove that

(1) $N(H)$ is a subgroup of G.
(2) H is normal in G if and only if $N(H) = G$.

Proof.

(1) Let $a, b \in N(H)$. Then $aHa^{-1} = H$ and $bHb^{-1} = H$, so $abH(ab)^{-1} = a(bHb^{-1})a^{-1} = aHa^{-1} = H$. Thus $ab \in N(H)$ which implies $N(H)$ is closed under multiplication.
(2) If $H \lhd G$, then $g \in G$ implies $gHg^{-1} = H$. Thus $G \leqslant N(H)$. Since $N(H) \leqslant G$, by definition, we get $N(H) = G$. Conversely, if $G = N(H)$, then $g \in G$ implies $gHg^{-1} = H$ by definition, i.e., $H \lhd G$.

□

Problem 3.101. Let G be a finite abelian group and suppose $n \in \mathbb{Z}$ is relatively prime to the order of G. Prove that every $g \in G$ can be written as $g = x^n$, with $x \in G$. (Hint: consider the mapping $\psi : G \to G$ defined by $\psi(a) = a^n$, and prove this mapping is an isomorphism).

Proof. Consider $\psi : G \to G$ defined by $\psi(x) = x^n$ for $x \in G$. First we will show that ψ is well-defined. Let $a, b \in G$ where $a = b$. Then $\psi(a) = a^n$ and $\psi(b) = b^n$, and if $a = b$ then $a^n = b^n$. Thus ψ is well-defined.

Next we will show that ψ is a homomorphism, i.e., that $\psi(xy) = \psi(x)\psi(y)$ for $x, y \in G$. Notice that $\psi(xy) = (xy)^n$; however, since we are working with an abelian group, we get $(xy)^n = x^n y^n = \psi(x)\psi(y)$. As desired.

Recall that a if a homomorphism f has $\ker f = \langle e \rangle$, then f is injective. If $x \in \ker \psi$ then $\psi(x) = x^n = e$. Since G is finite, $x^{o(G)} = e$. Note that $o(G)$ is coprime with n, so there are integers a, b such that $ao(G)+bn = 1$. Then we get, $x = x^{ao(G)+bn} = (x^{o(G)})^a (x^n)^b = e$, so the only element in $\ker \psi$ is e, i.e., ψ is injective.

Since G is finite and ψ is injective, we get ψ is surjective.

Thus ψ is an isomorphism. □

Problem 3.102. Let G be a non-abelian group of order 6. Prove the following:

(1) G has a subgroup H of order 2.
(2) H is not a normal subgroup of G.
(3) G is isomorphic to the symmetry group S_3.

Lemma 3.103. *The center $Z(G)$ of a group G is a normal subgroup.*

Proof. Let $g \in G$ and $x \in Z(G)$. By definition, $gx = xg$. Then $gZ(G) = Z(G)g$. Thus $Z(G) \lhd G$. □

Proof.

(1) Note that $o(G) = 6 = 2 \cdot 3$, i.e., the product of primes 2 and 3. Thus by Cauchy's theorem, G has a subgroup of order 2.
(2) Let $a \in G$ such that $o(a) = 2$ and let $H = \langle a \rangle$. If H were normal, then for any $g \in G$, $gag^{-1} = a$. Thus $ga = ag$ for all $g \in G$. This means $a \in Z(G)$. However, if this is the case, $o(G/Z(G)) = 1$ or 3, which implies G is cyclic and therefore abelian (by the next example). A contradiction.
(3) First, note that $|S_3| = 3! = 6$, and no element of G can be order 6. Let $a, b \in G$ where $o(a) = 2$ and $o(b) = 3$. Let $H = \langle a \rangle$ and $K = \langle b \rangle$. Then $H, K < G$. Note that K is normal in G since $i_G H = 2$ (since every subgroup of index 2 is normal). Thus $aba^{-1} \in K = \{e, b, b^2\}$. If $aba^{-1} = e$, then $b = e$ which contradicts our assumption that $o(b) = 3$. If $aba^{-1} = b$, then $ab = ba$ which contradicts our assumption that G is abelian. Thus $aba^{-1} = b^2$ and
$$G = \{e, b, b^2, a, ab, ab^2 \mid a^2 = b^3 = e, ab = b^2 a\} \cong S_3.$$

□

Problem 3.104. Let G be a group, $Z(G)$ be its center. Prove that if $G/Z(G)$ is cyclic, then G must be abelian.

Proof. Let $G/Z(G)$ be cyclic. Then there is some $x \in G/Z(G)$ such that $G/Z(G) = \langle xZ(G)\rangle$. Let $g \in G$. We get $gZ(G) = x^m Z(G)$ for some $m \in \mathbb{Z}$. Then $x^{-m}g = z$ for some $z \in Z(G)$, so $g = zx^m$.

Let $g_1 = x^a z_1$ and let $g_2 = x^b z_2$, for $x \in G/Z(G)$, $g_1, g_2 \in G$, and $a, b \in \mathbb{Z}$. Note that x commutes with itself. Then we see that

$$\begin{aligned} g_1 g_2 &= (x^a z_1)(x^b z_2) = x^a(z_1 x^b)z_2 = x^a(x^b z_1)z_2 = (x^a x^b)(z_1 z_2) \\ &= (x^b x^a)(z_2 z_1) = x^b(x^a z_2)z_1 = x^b(z_2 x^a)z_1 = (x^b z_2)(x^a z_1) = g_2 g_1. \end{aligned}$$

Thus G is abelian. (Furthermore $G/Z(G)$ cannot be a cyclic group which is non-trivial.) □

Lemma 3.105. *Let G be a group where $o(G) = pq$, for p, q prime and $p < q$. Then there is only one subgroup of G with size q.*

Proof. By Cauchy's theorem, there exists $H \leqslant G$ such that $|H| = q$. Since H is of prime order, it is cyclic. Let $H = \langle a\rangle$ for $a \in G$, where $o(a) = q$.

Suppose that $\langle a\rangle$ is not unique. Then there is some $b \in G$ which has order q and $b \notin \langle a\rangle$. Note that b^0 is the only multiple of b that is in $\langle a\rangle$. If $b^m = a^n$ for $m, n \in \mathbb{Z}$ and $m \not\equiv 0 \pmod q$, then $b^{m-m+1} = b = a^{n-m+1}$, i.e., b is a power of a which contradicts our assumption. Thus if $b^m \in \langle a\rangle$, then $m \equiv 0 \pmod q$, and $b^m = e$.

Consider the left cosets of $\langle a\rangle$ of the form $b^i\langle a\rangle$, for $i \in \{0, 1, \ldots, q-1\}$. The total number of left H cosets is $i_G H = pq/q = p$. Since $p < q$, and we have enumerated q cosets, some cosets must be equal. Let $b^j\langle a\rangle = b^k\langle a\rangle$ for $j \neq k$. Then $b^{k-j} \in \langle a\rangle$. Thus there is a power of b other than the identity equal to a power of a. This contradicts what we found in the previous paragraph. Therefore b cannot exist, which means that every element of order q is in $\langle a\rangle$, i.e., $\langle a\rangle$ is unique. □

Lemma 3.106. *Let p, q be primes with $p > q$. If $p \not\equiv 1 \pmod q$, then any group of size pq is cyclic.*

Proof. Let $|G| = pq$. Then by Cauchy's theorem, G has an element of order p and an element of order q. Let $a, b \in G$ be elements of order p and q respectively. Note that bab^{-1} is a conjugate of a which has order p. Then by Lemma 3.105, $bab^{-1} = a^k$ for $k \in \mathbb{Z}$. It follows that $b^n ab^{-n} = a^{k^n}$ for $n \in \mathbb{Z}$ and $n \geqslant 1$. For $n = q$, this statement implies $a = a^{k^q}$.

Since a has order p, we get $k^q \equiv 1 \pmod p$. Then k has order either 1 or q in $(\mathbb{Z}/p\mathbb{Z})^*$ which is a group of size $p-1$ (since the multiplicative group of integers modulo a prime number always has size $n-1$ for n prime). If the order is q, then $q \mid (p-1)$, i.e., $p \equiv 1 \pmod q$. But $p \not\equiv 1 \pmod q$ by supposition. Thus the order of $k \in (\mathbb{Z}/p\mathbb{Z})^*$ is 1, so $k \equiv 1 \pmod p$ and $bab^{-1} = b^k = b^1 = b$ so $ba = ab$. □

Problem 3.107. Let G be a group of order 15. Use Cauchy's theorem to prove that G is cyclic.

Proof. G has an element of order 3 and an element of order 5. By the lemma above, since $3 \nmid (5-1)$, G must be cyclic. □

Lemma 3.108. *Let G be a group. G is abelian if and only if $Z(G) = G$.*

Proof. Let G be an abelian group. Then for all $a, x \in G$, $ax = xa$. Thus for all $a \in G$, $a \in Z(G) = G$.

Let $Z(G) = G$. Then for all $a, x \in G$, $ax = xa$. Thus G is abelian. □

Lemma 3.109. *The center of an abelian group of prime power order is non-trivial.*

Proof. Let G be a group whose order is the power of a prime. Suppose G is abelian. Then from the above lemma, $Z(G) = G$ which by supposition is non-trivial. □

Problem 3.110. Let G be a group of order p^2, where p is prime. Prove the following:

(1) G is abelian.
(2) Show that G is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proof.

(1) Let $Z(G)$ be the center of G. By Lagrange's theorem $\left|Z(G)\right| \mid |G|$, so $\left|Z(G)\right| = 1, p$ or p^2. But we know that $\left|Z(G)\right| \neq 1$ since the center of a group of prime power order is not the identity.

Suppose $\left|Z(G)\right| = p$. Then $\left|G/Z(G)\right| = i_G(G/Z(G)) = |G| / \left|Z(G)\right| = p^2/p = p$. So $G/Z(G)$ is non-trivial and of prime order so it is cyclic.

However, this cannot be the case since $G/Z(G)$ cannot be a cyclic group that is non-trivial by example 3.104. So $\left|Z(G)\right| = p^2$, and thus $Z(G) = G$. Since cyclic groups are always abelian, G is abelian.

(2) If there is an element $g \in G$ of order p^2. Then $G \cong \mathbb{Z}/p^2\mathbb{Z}$ by the isomorphism that takes $g \mapsto 1 \pmod{p^2}$ and $g^a \mapsto a \pmod{p^2}$.

If there is no element of order p^2, then every $g \neq e$ has order p. Then $G \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^2$ by the isomorphism that takes $g_1^{a_1} g_2^{a_2} \mapsto (a_1, a_2)$.

□

Lemma 3.111. *If a group G has only one subgroup of a given order, then that subgroup is normal.*

Proof. Let $H \leqslant G$, where H is the only subgroup of some order. Then for $g \in G$, $gHg^{-1} \leqslant G$, i.e., the conjugate of a subgroup is a subgroup. Note the conjugate of a subgroup has the same order as the subgroup. But any subgroup of order $|H|$ must be H, since H is the only subgroup of G of that order by supposition. Thus $gHg^{-1} = H$, so $H \trianglelefteq G$. □

Problem 3.112. Let G be a group of order 385. Show that G has only one subgroup H of order 11 and one subgroup K of order 7. Also, prove that H is normal and K is in the center of G.

Proof. The prime factorization of $385 = 5 \cdot 7 \cdot 11$. By Cauchy's theorem, there exists a subgroup H of order 11, and there exists a subgroup K of order 7. Let n_p be the number of Sylow p-subgroups of G. By Sylow, $n_{11} \equiv 1 \pmod{11}$ and $n_{11} \mid 35$. So n_{11} must equal 1. The same applies to n_7. By Lemma 3.111, we get H and K are both normal subgroups of G.

Let $g \in G$. Note that g must either be an element of order 5,7, or 11. Let $k \in K$ and $k \neq e$. Since K is normal. $gkg^{-1} = k^n$ for some $n \in \mathbb{Z}$. Then $k = g^{o(g)}kg^{-o(g)} = k^{n^{o(g)}}$, which means $n^{o(g)} \equiv 1 \pmod{7}$. If $o(g) = 5$ or 11, then $n \equiv 1 \pmod{7}$ (otherwise the result would disagree with Fermat's little theorem). Therefore every element of G commutes with k, so K is in the center of G. □

Problem 3.113. If G is of order 108, show that G has either a normal subgroup of order 9 or order 27.

Proof. Note that the prime factorization of $108 = 2^2 \cdot 3^3$. Let H be a Sylow 3-subgroup of G. Then $n_3 = 1$ or 4.

If n_3 is 1, then $|H| = 27$ and it is normal since it is unique.

If $n_3 = 4$, then we have more to show. Let G act on G/H (the set of all left cosets of H). This is a natural group action of G on G/H by left multiplication: $g \cdot (xH) = (gx)H$, i.e., every $g \in G$ induces a permutation of G/H. Note that this defines a homomorphism of G on $\mathrm{Sym}(G/H) \cong S_4$. Let $\phi : G \to S_4$ be this homomorphism. From the first isomorphism theorem and Lagrange's theorem, we get $|G| = |\ker \phi| \left|\phi(G)\right|$.

Thus $o(\phi(G)) \mid |G| = 108$. Notice that $\phi(G) \leqslant S_4$. Recall $|S_4| = 24$. Thus $o(\phi(G)) \mid 24$. Then $\left|\phi(G)\right| \mid (108, 24) = 12$. It follows that $|\ker \phi| \geqslant 108/12 = 9$.

Let $|\ker \phi| = 9$. Recall that the kernel is a normal subgroup of G. Thus $\ker \phi \trianglelefteq G$. □

Problem 3.114. Let G be a non-abelian group of order pq, where $p < q$ are primes. Prove that G has a nonnormal subgroup of index q and there exists an injective homomorphism from G to the symmetry group S_q.

Proof. Note that the Sylow q-subgroup is normal, since for groups of order pq where p, q prime and $p < q$, the q-subgroup is always normal. Let Q be the normal Sylow q-subgroup. By Lemma 3.111, $n_q = 1$.

Suppose G had a normal Sylow p-subgroup. Let P be that subgroup. Then $n_p = 1$. We have stated that $n_q = 1$. Recall that $G = PQ$. Further, recall that the product of cyclic groups of coprime order is cyclic. Thus G is cyclic, and therefore abelian. A contradiction. Thus P must be nonnormal.

Note $\left|G/P\right| = q$. Let G act on G/P. Then every $g \in G$ induces a permutation of G/P. This defines a homomorphism $\phi : G \to S_q$. Note that $\ker \phi \trianglelefteq P$. Since P is prime order, $|\ker \phi| = 1$. Thus $\ker \phi = \{e\}$, and we get ϕ is injective. □

Problem 3.115. Prove that a group of order 1365 is not simple.

Proof. Let G be a group of order 1365. The prime factorization of $1365 = 3 \cdot 5 \cdot 7 \cdot 13$. Suppose G is simple. Then $n_p \neq 1$ for $p = 3, 5, 7, 13$ by Lemma 3.111. By Sylow, $n_3 = 7, 13$, or 91, $n_5 = 21$ or 91, $n_7 = 15$ and $n_{13} = 105$. Since the Sylow p-subgroups have prime order, they are cyclic, which implies their intersection is the identity. Then G has, at minimum, $7 \cdot (3-1) + 21 \cdot (5-1) + 15 \cdot (7-1) + 105 \cdot (15-1) = 1448$ elements (where the minus 1 eliminates recounting the identity element). This contradicts our assumption that G has 1365 elements. Thus G is not simple. □

Problem 3.116. Prove that a group of order p^2q, where p, q are primes, is not simple.

Proof. Let G be a group of order p^2q, for p, q prime, and suppose G is simple. Let n_q and n_p be the number of Sylow q-subgroups and p-subgroups, respectively. Since we suppose G is simple, then n_q and n_p are both greater than 1 by Lemma 3.111.

Let H be a Sylow q-subgroup. Since H is of order q, H is cyclic. Note that the only divisors of q are 1 and q, so any two distinct Sylow q-subgroups have an intersection which only contains the identity. Thus the elements of G of order q equals $n_q(q-1)$. If $n_q = p^2$, then the number of elements that are not of order q is $p^2q - p^2(q-1) = p^2$.

Let K be a Sylow p-subgroup of G. Then $|K| = p^2$, so no element can have order q. Thus K contains all elements that do not have order q. Thus there cannot be another Sylow p-subgroup, which means K is normal, which contradicts our supposition.

Thus n_q must equal p. But by Sylow, $n_q \equiv 1 \pmod q$, so $p \equiv 1 \pmod q$. This implies $p > q$. On the other hand, $n_p \mid q$, so n_p must be q. Then $n_p \equiv 1 \pmod p$, so $q \equiv 1 \pmod p$. This implies $p < q$. A contradiction.

Thus our supposition leads to a contradiction in all cases, so if a group has order p^2q for p, q prime, then it is not simple. □

The next 2 problem solutions are taken directly from Giang Tran's solutions

Problem 3.117. Prove that any subgroup $H \subset A_n$ of index n is isomorphic to A_{n-1}.

Proof. Sketch. Recall $|A_n| = n!/2$. A_n/H is the set $\{\sigma \circ H \mid \sigma \in A_n\}$. Consider the group action of A_n on A_n/H by left translation

$$\begin{aligned} \phi : A_n &\to \Sigma(A_n/H) \\ \sigma \mapsto \phi_\sigma : \qquad & A_n/H \to A_n/H \\ & \phi_\sigma(\tau H) = \sigma\tau H \end{aligned}$$

Step 1: Verify ϕ is a group homomorphism.
Step 2: Note $[A_n : H] = n$ so $|\Sigma(A_n/H)| = |S_n| = n!$ and $\Sigma(A_n/H) \cong S_n$.
Since ϕ is a homomorphism, $A_n/\ker\phi \cong \operatorname{Im}\phi < S_n$.
Case 1: $n \geqslant 5$. Since $n \geqslant 5$, A_n is simple. So $\ker\phi = \{e\}$ or $\ker\phi = A_n$. On the other hand, from Cayley's extension theorem, we know that $\ker\phi$ is a subgroup of $H \subset A_n$. So $\ker\phi = \{e\}$, which means ϕ is injective and $H \cong \phi(H)$, $|\phi(H)| = |H| = (n-1)!/2$
For $\sigma \in H \subset A_n$, $\phi_\sigma(\tau H) = \sigma\tau H$ especially $\phi_\sigma(H) = \sigma H = H$. So

$$\phi_\sigma = \begin{pmatrix} H & a_2H & \cdots & a_nH \\ H & a_2'H & \cdots & a_n'H \end{pmatrix}$$

Thus $|\phi(H)| \leqslant |A_{n-1}| = \frac{(n-1)!}{2}$. So $H \cong \phi(H) \cong A_{n-1}$.
Case 2: [✓] □

Problem 3.118. List all the conjugate classes in S_4 and verify the class equation.

Proof. Note $S_4 : 4 = 4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$. So S_4 has 5 conjugacy classes.
All 4 cycles, $4!/4 = 6$ elements. All 3 cycles, $\binom{4}{3}2 = 8$ elements. All double 2-cycles, i.e., of the form $(a\ b)(c\ d)$, 3 elements. All 2 cycles, $\binom{4}{2} = 6$ elements. All 1 cycles, the identity so 1 element. Thus $4! = 6+8+3+6+1$. As desired. □

Problem 3.119. Describe all abelian groups of order $2^4 \cdot 3^3 \cdot 5$.

Proof. Note $2^4 \cdot 3^3 \cdot 5 = 2160$.

(1) $Z_{2160} \cong Z_{16} \times Z_{27} \times Z_5$
(2) $Z_{1080} \times Z_2 \cong Z_8 \times Z_2 \times Z_{27} \times Z_5$
(3) $Z_{720} \times Z_3 \cong Z_{16} \times Z_9 \times Z_3 \times Z_5$
(4) $Z_{540} \times Z_4 \cong Z_4 \times Z_4 \times Z_{27} \times Z_5$
(5) $Z_{540} \times Z_2 \times Z_2 \cong Z_4 \times Z_2 \times Z_2 \times Z_{27} \times Z_5$
(6) $Z_{360} \times Z_6 \cong Z_8 \times Z_2 \times Z_9 \times Z_3 \times Z_5$
(7) $Z_{270} \times Z_2 \times Z_2 \times Z_2 \cong Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_{27} \times Z_5$
(8) $Z_{240} \times Z_3 \times Z_3 \cong Z_{16} \times Z_3 \times Z_3 \times Z_5$
(9) $Z_{180} \times Z_{12} \cong Z_4 \times Z_4 \times Z_9 \times Z_3 \times Z_5$
(10) $Z_{180} \times Z_6 \times Z_2 \cong Z_4 \times Z_2 \times Z_9 \times Z_3 \times Z_5$
(11) $Z_{120} \times Z_6 \times Z_3 \cong Z_8 \times Z_2 \times Z_3 \times Z_3 \times Z_3 \times Z_5$
(12) $Z_{90} \times Z_6 \times Z_2 \times Z_2 \cong Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_9 \times Z_3 \times Z_5$
(13) $Z_{60} \times Z_{12} \times Z_3 \cong Z_4 \times Z_4 \times Z_3 \times Z_3 \times Z_3 \times Z_5$
(14) $Z_{60} \times Z_6 \times Z_6 \cong Z_4 \times Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_3 \times Z_5$
(15) $Z_{30} \times Z_6 \times Z_6 \times Z_2 \cong Z_2 \times Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_3 \times Z_5$

□

Lemma 3.120. *If $\phi : G \to H$ is an isomorphism, then $o(a) = o(\phi(a))$.*

Proof. Suppose $o(a) = n$ for $n \in \mathbb{Z}_{\geqslant 0}$ and $o(\phi(a)) = \infty$. Then

$$\phi(a)^n = \phi(a^n) = \phi(e_G) = e_H,$$

a contradiction.

Suppose $o(a) = \infty$ and $o(\phi(a)) = n$ for $n \in \mathbb{Z}_{\geqslant 0}$. Then

$$\phi(a^n) = \phi(a)^n = e_H = \phi(e_G).$$

But ϕ is injective, so $a^n = e_G$. A contradiction.

Suppose $o(a) = n$ and $o(\phi(a)) = m$ for $m, n \in \mathbb{Z}_{\geqslant 0}$. Then

$$\phi(a)^n = \phi(a^n) = \phi(e_G) = e_H.$$

So $m \leqslant n$. On the other hand,

$$\phi(e_G) = e_H = \phi(a)^m = \phi(a^m).$$

So $n \leqslant m$. Thus $n = m$, and it follows that $o(a) = o(\phi(a))$. □

Lemma 3.121. *$Z_m \times Z_n$ is cyclic and isomorphic to Z_{mn} if and only if $(m, n) = 1$.*

Proof. Note that this is a restatement of the Chinese remainder theorem. Let $(a, b) \in Z_m \times Z_n$. Then $o(a) \mid m$ and $o(b) \mid n$. Let k be some multiple of $\text{lcm}(m, n)$, then we have $k(a, b) = (0, 0)$. If $\text{lcm}(m, n) \neq mn$, i.e., $\gcd(m, n) \neq 1$, then $Z_m \times Z_n$ cannot be cyclic.

Conversely, let $\gcd(m, n) = 1$. Consider $(1, 1)$. If $k(1, 1) = (0, 0)$, then k is a multiple of m and n such that $\text{lcm}(m, n) \mid k$. Since $\gcd(m, n) = 1$, we get $\text{lcm}(m, n) = mn$. Thus $\left|\langle (1, 1) \rangle\right| = mn = |Z_m \times Z_n|$. Thus $Z_m \times Z_n$ is cyclic and isomorphic to Z_{mn}. □

Problem 3.122. Is the group $(\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z})$ isomorphic to the group $(\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z})$? Verify your answer.

Note: The Lemma 3.120 is not used in this proof. It is only kept for completeness.

Proof. Since $(9, 10) = 1$, $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/90\mathbb{Z}$. Since $(6, 15) = 3$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \ncong \mathbb{Z}/90\mathbb{Z}$. Since isomorphism is an equivalence relation, $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \ncong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$. □

Problem 3.123.

(1) Let G and H are groups, and $(a, b) \in G \times H$ with $o(a) = m, o(b) = n$. Show that the order of (a, b) in the group $G \times H$ is the least common multiple of m and n. Extend the answer for the external direct product of 3 groups.
(2) Denote $Z_n = \mathbb{Z}/n\mathbb{Z}$. Let $A = Z_{12} \times Z_{45} \times Z_{60}$. Find the number of elements of order 2 in A.

Proof.

(1) Let $l = \text{lcm}(m, n)$. By definition, $l = mx = ny$ for some $x, y \in \mathbb{Z}$. Then

$$(a, b)^l = (a^l, b^l) = ((a^m)^x, (b^n)^y) = (e_G^x, e_H^y) = (e_G, e_H).$$

Since l is the *least* common multiple where this occurs, we get that $o((a, b)) = l$.

To extend this to three, simply take some group K, and put $(G \times H) \times K$ and apply the above argument. We can, in fact, do this at least finitely many times.

(2) We want to find all elements $(a, b, c) \in Z_{12} \times Z_{45} \times Z_{60}$ such that $\text{lcm}(|a|, |b|, |c|) = 2$. Then $|a| = 1, 2$, $|b| = 1$, $|c| = 1, 2$, so there are 4 since there are 4 choices.

□

Problem 3.124. Let G be a finite abelian group and H is a subgroup of G of index 2. Define $G^2 = \{g^2 : g \in G\}$.

(1) Show that G^2 is a normal subgroup of G.
(2) Prove that $G^2 \lhd H$ and H/G^2 is a subgroup of G/G^2 of index 2. Deduce that G and G/G^2 have the same number of subgroups of index 2.
(3) Show that every non-identity element in G/G^2 has order 2. Deduce that

$$G/G^2 \cong Z_2 \times Z_2 \times \cdots \times Z_2, \ n \text{ times, for some } n.$$

Proof.

(1) Let $g \in G$ and $h \in G^2$. Let $h' := ghgh = (gh)^2 \in G^2$. Then $ghg = h'h{-}1 \in G^2$. Note $g^{-2} \in G^2$ since $g^{-2} = (g^{-1})^2$. So $(ghg)g^{-2} = ghg^{-1} \in G^2$. As desired.
(2) Recall every subgroup of index 2 is normal. So $H \trianglelefteq G$ and $o(G/H) = 2$. Let $a \in G$. Then $(aH)^2 = H$ and $a^2 \in H$. It follows that $G^2 \leqslant H$. Since $G^2 \trianglelefteq G$, we get $G^2 \trianglelefteq H$. Note $H/G^2 \leqslant G/G^2$ and $[G/G^2 : H/G^2] = [G : H] = 2$.

    Define a map ϕ from all subgroups of G of index 2 to the set of subgroups of G/G^2 of index 2, with $\phi(H) = H/G^2$. Then $\phi^{-1}(H/G^2) := \{a \in G : aH \in H/G^2\}$. Since there exists a bijection, these sets have the same number of elements.
(3) Note that every group where every element squared is the identity is abelian, since 2 is prime and a group of prime order is cyclic and therefore abelian.

    Since $(aG^2)^2 = G^2$ for all $a \in G$, we get G/G^2 is a finite abelian group such that every non-identity element in G/G^2 has order 2. By the Fundamental Theorem of Finite Abelian Groups, we get G/G^2 is isomorphic to a direct product of cyclic groups. Since every non-identity element of G/G^2 has order 2, there is only one direct product decomposition:

$$G/G^2 \cong Z_2 \times Z_2 \times \cdots \times Z_2, \ n \text{ times, for some } n.$$

□

Problem 3.125.

(1) Given $n \in \mathbb{Z}, n \geqslant 1$. Find the number of subgroups of index 2 in $Z_2 \times Z_2 \times \cdots \times Z_2$ (n times).
(2) Find the number of subgroups of index 2 in $Z_{12} \times Z_{45} \times Z_{60}$.

Proof.

(1) From the previous problem, $Z_2^n := Z_2 \times Z_2 \times \cdots \times Z_2 \cong G/G^2$ for some finite abelian group G. Then the subgroups of G/G^2 are of the same number as subgroups of Z_2^n. Again, by the previous problem, the number of subgroups of index 2 in G equals the number of subgroups of index 2 in G/G^2.
(2) Let $H \leqslant G$ with $i_G(H) = 2$. Then there are only two cosets, $\{H, aH\}$ for $a \in G, a \notin H$. Note that $a^2 \in H$, since otherwise, $a^2H = aH$ which means $a \in H$ by the cancellation law.

□

4. Ring Theory

Groups are the foundations of algebra. Now lets build on that and add another operation to a set and call it a ring. Why not?

Definition 4.1.

(1) A ring R is a set together with two binary operations $+$ and $\times$ satisfying the following axioms:

(a) $(R, +)$ is an abelian group,
(b) $\times$ is associative,
(c) the distributive laws hold in R: for all $a, b, c \in R$

$$(a + b) \times c = (a \times c) + (b \times c) \text{ and } a \times (b + c) = (a \times b) + (a \times c).$$

(2) The ring R is commutative if multiplication is commutative.
(3) The ring R is said to have an identity if there is an element $1 \in R$ such that

$$1 \times a = a \times 1 = a, \text{ for all } a \in R.$$

Definition 4.2. A ring R with identity, where $1 \neq 0$, is called a division ring if every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$ such that $ab = ba = 1$. A commutative division ring is called a field.

Proposition 4.3. *Let R be a ring. Then*
(1) $0a = a0 = 0$ for all $a \in R$.
(2) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$.
(3) $(-a)(-b) = ab$ for all $a, b \in R$.
(4) if R has an identity 1, then the identity is unique and $-a = (-1)a$.

Proof. [✓] □

Definition 4.4. Let R be a ring.
(1) A nonzero element $a \in R$ is called a *zero divisor* if there is a nonzero element $b \in R$ such that either $ab = 0$ or $ba = 0$.
(2) Assume R has an identity $1 \neq 0$. An element $u \in R$ is called a *unit* in R if there is some $v \in R$ such that $uv = vu = 1$. The set of units in R is denoted $R^\times$.

Definition 4.5. A commutative ring with identity $1 \neq 0$ is called an *integral domain* if it has no zero divisors.

The abscence of zero divisors in integral domains give these rings a cancellation property.

Proposition 4.6. *Assume $a, b, c \in R$ a ring and a not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$. In particular, if $a, b, c \in R$ an integral domain, and $ab = ac$, then either $a = 0$ or $b = c$.*

Proof. If $ab = ac$ then $a(b - c) = 0$ so either $a = 0$ or $b - c = 0$. The second statement follows from the definition of an integral domain. □

Corollary 4.7. *Any finite integral domain is a field.*

Proof. [✓] □

Proposition 4.8. *$\mathbb{Z}/p\mathbb{Z}$ is a field if and only if p is prime. If p is composite, then there exists a zero-divisor.*

Proof. [✓] □

Remark 4.9. Fields $\subset$ integral domains $\subset$ commutative unital rings.

Definition 4.10. Let R be a ring, if for all $a \in R$, there exists a $m \in \mathbb{Z}_+$ such that $ma = 0$, then R is called a ring of finite characteristic.

Definition 4.11. The characterisitc of a ring R is the smallest number of times one must add 1_R to get 0_R.

4.1. **Ring Homomorphisms and Ideals.**

Definition 4.12. A *subring* of the ring R is a subgroup of R that is closed under multiplication. A more computational definition is: $S \subset R$ a subring if

$$a - b \in S, \forall a, b \in S, \qquad ab \in S, \forall a, b \in S.$$

If R contains 1, then S is a (unital) subring if $1_R \in S$. We assume subrings are unital for the rest of these notes unless otherwise specified.

Definition 4.13. A ring homomorphism between rings R and S is defined as such:

$$f : R \to S, \qquad f(x+y) = f(x) + f(y)$$
$$f(xy) = f(x)f(y).$$

Note that ker f and isomorphism is defined similarly to that of group homomorphisms. Im f is a subring of S and ker f is a subring of R.

An interesting note is that if R and S are unital, then, in general, $f(1_R) \neq 1_S$. [✓]

Definition 4.14. Let R be a ring, let $I \subset R$ and let $r \in R$.

(1) $rI = \{ra \mid a \in I$ and $Ir = \{ar \mid a \in I\}$.
(2) A subset I of R is a *left ideal* of R if
   (a) I is a subring of R,
   (b) I is closed under left multiplication by elements from R. (A right ideal is similarly defined [closed under right multiplication]).
(3) A subset I that is both a left and right ideal is called an ideal of R.

For commutative rings, left, right and ideals coincide.

Definition 4.15.

(1) A left principal ideal of R is a subset of R of the form $Ra = \{ra : r \in R\}$.
(2) A right principal ideal of R is a subset of R of the form $aR = \{ar : r \in R\}$.
(3) A (two-sided) principal ideal of R is a subset of R of the form $RaR = \{r_1as_1 + \cdots + r_nas_n : r_1, s_1, \ldots, r_n, s_n \in R\}$.

The difference between an ideal and a principal ideal is subtle, note that a principal ideal is generated by the multiplication of all elements in the ring with a *single* element of the ring. Here is an example of a principal ideal that is not an ideal:

Example 4.16. Show $(2, x) := \{2f(x) + xg(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$ is an ideal in $\mathbb{Z}[x]$, but $(2, x)$ is not a principal ideal in $\mathbb{Z}[x]$.

Proof. Suppose $(2, x) = \langle h(x) \rangle$. Then $x = h(x)f(x)$, $2 = h(x)g(x)$ for $f, g \in \mathbb{Z}[x]$ and $0 = \deg h + \deg g$ each of which are greater than or equal to 0. But $\deg h = 0$ so $h(x) = a_0 \in \mathbb{Z}$. Thus $x = a_0(b_0 + b_1x + \cdots + b_nx_n)$ for $b_i \in \mathbb{Z}$ and $1 = a_0b_1$ so $a_0 \mid 1$ which means $a_0 = \pm 1$. Therefore $(2, x) = \langle 1 \rangle = \mathbb{Z}[x]$. Now $1 \in \mathbb{Z}[x]$,

$$1 = 2p(x) + xq(x)$$
$$1 = 2(\alpha_0 + \alpha_1x + \cdots + \alpha_mx^m) + x(\beta_0 + \beta_1x + \beta_tx^t)$$
$$1 = 2\alpha_0$$

but $2\alpha_0$ is even, a contradication. □

Remark 4.17. Let I, J be ideals, then $I \cap J$, $I + J$, $IJ = \{\sum_{i=1}^{n} x_i y_i, x_i \in I, y_i \in J\}$ are ideals too. Note that $IJ \subset I \cap J$.

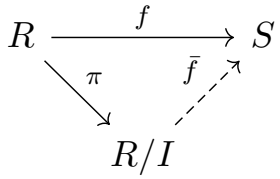
Definition 4.18. Let $I \subset R$ be an ideal. Then

$$R/I = \{x + I \mid x \in R\}$$

and $(x + I) + (y + I) := (x + y) + I$, $(x + I) \cdot (y + I) := xy + I$.

$(R/I, +, \cdot)$ is a ring called a quotient ring.

The mapping $\pi : R \to R/I$, $\pi(x) = x + I$ is a surjective ring homomorphism.



Note that $\bar{f} \circ \pi = f$.

Examples 4.19.

(1) Every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}, n \in \mathbb{Z}$.
(2) $\mathbb{Z}/n\mathbb{Z}$ is a quotient ring.

Definition 4.20. Let $R_1, \ldots, R_n$ be unital rings, then $R_1 \times \cdots \times R_n = \{(x_1, \ldots, x_n) \mid x_i \in R_i\}$ is a ring. This is the direct product of rings (addition and multiplication work as expected).

Remark 4.21. $\ker f = \{0\}$ if and only if f is injective.

4.2. **Chinese Remainder Theorem.**

Theorem 4.22. *(Chinese Remainder Theorem [CRT]) Let $\{m_i\}_{i=1}^{n} \subset \mathbb{Z}$ be a sequence of pairwise coprime integers. Then for all $a_1, \ldots, a_n \in \mathbb{Z}$, there is an $a \in \mathbb{Z}$ such that $a \equiv a_i \pmod{m_i}$, i.e., $a - a_i \in m_i\mathbb{Z}$.*

We can extend the CRT for a general unital ring.

Definition 4.23. Let R be a unital ring, I an ideal in R, and $x, y \in R$. Then $x \equiv y \pmod{I}$ if $x - y \in I$.

Proposition 4.24. *Let $x_1 \equiv y_1 \pmod{I}, x_2 \equiv y_2 \pmod{I}$. Then*

(1) $x_1 + x_2 \equiv y_1 + y_2 \pmod{I}$.
(2) $x_1 x_2 \equiv y_1 y_2 \pmod{I}$.

Theorem 4.25. *(CRT - Ring defintion) Let R be a unital ring, and let $I_1, I_2, \ldots, I_n$ be ideals in R such that $I_i + I_j = R$ for all $i \neq j$. Then for all $a_1, a_2, \ldots, a_n \in R$, there is an $a \in R$ such that $a \equiv a_i \pmod{I_i}$.*

Proof. By induction. [✓] □

Theorem 4.26. *(CRT - Ring 2 - CRT harder) Let R be a unital ring, and let $I_1, I_2, \ldots, I_n$ be ideals in R such that $I_i + I_j = R$ for all $i \neq j$. Then*

$$R/\bigcap_{k=1}^{n} I_k \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n \text{ (ring isomorphism).}$$

Proof. [✓] □

Example 4.27. Let $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, and p_i be distinct primes, $\alpha_i \geqslant 1$. Let $I_k = p_k^{\alpha_k}\mathbb{Z}$, then $I_k + I_l = \mathbb{Z}$ for all $k \neq l$ [✓]. Then $\bigcap_{k=1}^{n} I_k = m\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z} \cong \prod_{k=1}^{n} \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$.

4.3. **Prime and Maximal Ideals.**

Definition 4.28. Let R be a commutative ring,

(1) An ideal $P \subset R$ is called prime if whenever $xy \in P$, either $x \in P$ or $y \in P$.
(2) An ideal $m \subset R$ is called maximal if there is no ideal between M and R, i.e., for ideal U in R and $M \subseteq U \subset R$ implies $U = M$.

Example 4.29. Every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for $n \in \mathbb{Z}$. Then $p\mathbb{Z}$ for p prime is a prime ideal and, notably, $\{0\}$ is a prime ideal. Further $p\mathbb{Z} \subseteq U = n\mathbb{Z} \subset \mathbb{Z}$, and $p \in U$, then $p = nq$ for some $q \in \mathbb{Z}$. But p is prime and $n \neq 1$ so $n = p$. Thus $U = p\mathbb{Z}$. Thus $p\mathbb{Z}$, for p prime, is a maximal ideal in $\mathbb{Z}$. Note that $0 \subset p\mathbb{Z} \subset \mathbb{Z}$, so 0 is not a maximal ideal in $\mathbb{Z}$.

Proposition 4.30.

(1) 0 is a prime ideal in a ring R if and only if R is a integral domain (commutative ring with no zero divisors).
(2) 0 is a maximal ideal in R if and only if R is a field.

Proof. [✓] □

Proposition 4.31. *Let R be a commutative ring, I an ideal in R. Then*

(1) I prime if and only if R/I is an integral domain.
(2) I maximal if and only if R/I is a field.

Corollary 4.32. *Any maximal ideal is prime; I maximal $\iff$ R/I field $\iff$ R/I integral domain $\iff$ I prime.*

This is a little bit of a shift here, but bear with me.

Definition 4.33. A partially ordered set is a set, say X, with a binary relation denoted $\leqslant$, where for every $a, b \in X$, $a \leqslant a$, $a \leqslant b, b \leqslant a \implies a = b$ and $a \leqslant b, b \leqslant c$ implies $a \leqslant c$.

Definition 4.34. Let X be a paritally ordered set. $Y \subset X$ is called a chain if for all $y_1, y_2 \in Y$, we have $y_1 \leqslant y_2$ or $y_2 \leqslant y_1$.

Lemma 4.35. *(Zorn's Lemma) Let X be a partially ordered set. If every chain $Y \subset X$ has an upper bound in X, i.e., there exists $x \in X$ such that $y \leqslant x$ for all $y \in Y$, then X has a maximal element x_0 such that $x \leqslant x_0$ for all $x \in X$.*

Now let's get back to ring theory.

Theorem 4.36. *(Existence of maximal ideal) Every nonzero commutative ring R has a maximal ideal.*

Proof. $X = \{$ all proper ideals of $R\}$, $(X, \subseteq)$ partially ordered set. Let Y be a chain in X. Then $J = \bigcup_{I \in Y} I$ is an ideal in R [✓]. Since Y is a chain, $I_1 \subseteq I_2$ or $I_2 \subseteq I_1$. WLOG, let $I_1 \subseteq I_2$ and $a \in I_1$, $b \in I_2$. Then $a - b \in I_2 \subseteq J$. Let $a \in I_1 \in Y, r \in R$, then $ar = ra \in I_1 \in Y$. So J is an ideal in R. If R has 1, then $J \neq 1$. Thus J is proper. □

4.4. **Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains.**

Definition 4.37. An integral domain R is called a Euclidean domain if there exists a $d : R\backslash\{0\} \to \mathbb{Z}_{\geqslant 0}$ that satisfies: for all $a, b \in R$, $b \neq 0$, there exists $q, r \in R$ such that $a = bq + r$ and $r = 0$ or $d(r) < d(b)$.

Example 4.38.

(1) Consider $\mathbb{Z}$. Let $a, b \in \mathbb{Z}$ and $b \neq 0$. Then $a = bq + r$, $d : \mathbb{Z}\backslash\{0\} \to \mathbb{Z}_{\geqslant 0}$ and $d(x) = |x|$.
(2) Let F be a field. $F[x]$ be the ring of polynomials with elements of F as coefficients. Consider long division. $d : F[x]\backslash\{0\} \to \mathbb{Z}_{\geqslant 0}$ and $d(f(x)) := \deg f$.
(3) Consider $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ where $i^2 = -1$. Then $\mathbb{Z}[i]$ is an integral domain with unit $1 = 1 + 0i$ Then $d : \mathbb{Z}[i]\backslash\{0\} \to \mathbb{Z}_{\geqslant 0}$ under $d(a + bi) = a^2 + b^2$.

Theorem 4.39. *Let R be a Euclidean domain, I an ideal in R. Then there exists $a_0 \in R$ such that $I = Ra_0$, i.e., I is a principal ideal.*

Proof. [✓] □

Definition 4.40. A commutative ring R such that all ideals are principal is called a principal ideal domain (PID).

Proposition 4.41. *Every Euclidean domain is a PID*

Proof. [✓] □

Proposition 4.42. *Every field is a Euclidean domain.*

Proof. [✓] Let $d : R\backslash\{0\} \to \mathbb{Z}_{\geqslant 0}$. Then for all $a, b \in R$, $b \neq 0$, $a = b\underbrace{(b^{-1}a)}_{q}$ and $r = 0$. □

Let's talk about factorization in commutative rings.

Definition 4.43. Given a commutative ring R and $a, b \in R$. We say $b \mid a$ if there exists $c \in R$ such that $a = bc$. We also say a and b are associated if $a \mid b$ and $b \mid a$ which is denoted by $a \sim b$ (an equivalence relation).

Remark 4.44. If a and b are associated, then $a = bn$ for $n \in R^\times = \{v \in R \mid \exists v' : vv' = 1\}$. Then $a = bn = anv \implies a(1 - nv) = 0$ and $b = av$ for some $n, v \in R$.

Lets talk about some properties (that I suppose have to do with the above equivalence relation). Let $a, b, c \in R$ a commutative ring.

(1) $b \mid a_1, b \mid a_2 \implies b \mid (a_1 \pm a_2)$
(2) $b \mid a, c \mid b \implies c \mid a$
(3) $a \mid 0$

(4) $1 \mid a$
(5) $b \mid a \implies b \mid ac$
(6) $b \mid a \iff Ra \subseteq Rb$
(7) $a \sim b \iff Ra = Rb$
(8) If R is an integral domain, then $Ra = Rb \iff b = an$, for some $n \in R^\times$.

Definition 4.45. Let R be an integral domain. $a \in R$ is called irreducible if

(1) $a \neq 0$,
(2) $a \notin R^\times$,
(3) a has a nontrivial factorization, i.e. if $a = bc$ for $b, c \in R$, then $b \in R^\times$ or $c \in R^\times$.

Let's show some more properties of an integral domain given these new definitions. Let R be an integral domain for the next 4 propositions.

Proposition 4.46. *Let $p \neq 0$, p is prime if and only if Rp is prime.*

Proof. [✓] □

Proposition 4.47. *$c \in R$ is irreducible if and only if Rc is a maximal ideal in the set of all principal ideals $X = \{Ra \mid a \in R\}$ if $Rc \subseteq Ra \subseteq R$ then $Ra = Rc$ or $Ra = R$.*

Proof. [✓] □

Proposition 4.48. *Every prime element is irreducible (recall every maximal ideal is a prime ideal).*

Proof. [✓] □

Example 4.49. $a \in \mathbb{Z}$ is irreducible if and only if a is prime and a is a prime number. However, a is not prime [✓].

Proposition 4.50. *If R is a PID, a is irreducible if and only if a is prime.*

Proof. It suffices to show that if a is irreducible, then a is prime (since every prime is irreducible). Note Ra is a maximal ideal in the set of all principal ideals. So Ra is a prime ideal, so a is prime. Every maximal ideal M is a prime ideal. □

Now let's talk about unique factorization domains (UFDs).

Definition 4.51. An integral domain R is called a UFD if for every nonzero, non-unit $a \in R$, i.e., $a \neq 0$ and $a \notin R^\times$, then a can be written as a product of prime (or irreducible) elements, uniquely up to order and units. This is analogous to the fundamental theorem of arithmetic for integers.

Remark 4.52. If $a = c_1 c_2 \cdots c_n$, then $Ra = R(c_1 c_2 \cdots c_n) = Rc_1 Rc_2 \cdots Rc_n$, i.e., every principal ideal can be factorized as a product of maximal ideals in the set of all principal ideals.

Proposition 4.53. *Every PID is a UFD*

Proof. [✓] □

Example 4.54.

(1) $\mathbb{Z}[\sqrt{-2}]$ is a UFD, $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.
(2) $\mathbb{Z}[\sqrt{-5}]$ is a UFD, $2, 3, 1 \pm \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$.
(3) $\mathbb{Z}[x]$ is a UFD but not a PID, see Example 4.16.

4.5. **Polynomial Rings.** Let R be a commutative ring with 1, then

$$R[x] = \{f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R\}.$$

Addition works as follows:

$$f(x) = \sum_{k=0}^{n} a_k x^k,\ g(x) = \sum_{j=0}^{m} b_j x^j, \qquad f(x) + g(x) = \sum_{i=0}^{\max(n,m)} (a_i + b_i)x^i$$

Guess how multiplication works:

$$f(x)g(x) = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k$$

Definition 4.55. $R \subset R[x]$ a subring, $f(x) \in R[x]$, $f(x) = a_n x^n + \cdots + a_1 x + a_0$.

- If $a_n \neq 0$, then $\deg f := n$,
- if $a_n = 1$, then f is a monic polynomial,
- if R is an integral domain, then $f(x)g(x) \in R[x]\backslash\{0\}$, $\deg(fg) = \deg(f) + \deg(g)$.

Remark 4.56. For general commutative rings, $\deg(fg) \leqslant \deg(f) + \deg(g)$.

4.5.1. *Polynomials over a Field.* Let F be a field. Here are some miscellaneous defnitions and propositions (which will go unproved).

Definition 4.57.

(1) $f(x), g(x) \in F[x]\backslash\{0\}$, then $\deg(fg) = \deg(f) + \deg(g)$.
(2) *The division algorithm*, $f(x), g(x) \in F[x]$ and $g(x) \neq 0$, then there exists $q(x), r(x) \in F[x]$, such that
$$f(x) = g(x)q(x) + r(x) \qquad r(x) = 0 \vee \deg(r) < \deg(g).$$
(3) $F[x]$ is a Euclidean domain (degree function).
(4) $F[x]$ is a PID.
(5) $F[x]$ is a UFD.
(6) If R is an integral domain, then $R^\times = R[x]^\times$.
(7) The ideal $(p(x)) := F[x]p(x)$, is a a maximal ideal if and only if $p(x)$ is irreducible.
(8) $F[x]/(p(x))$ is a field if and only if $p(x)$ is irreducible.

4.5.2. *Polynomials over $\mathbb{Z}$.*

Definition 4.58. Let $f = a_0 + a_1 x + \cdots + a_n x^n$, $a_i \in \mathbb{Z}$, $a_n \neq 0$ is said to be *primitive* if

$$\gcd(a_0, a_1, \ldots, a_n) = 1.$$

Remark 4.59. Note

$$\begin{aligned}\gcd(a,b,c) &= \gcd(\gcd(a,b),c)\\ &\Downarrow\\ a &= p_1^{\alpha_1}\cdots p_r^{\alpha_r} \quad \alpha_i \geqslant 0,\\ b &= p_1^{\beta_1}\cdots p_r^{\beta_r} \quad \beta_i \geqslant 0,\\ c &= p_1^{\gamma_1}\cdots p_r^{\gamma_r} \quad \gamma_i \geqslant 0\\ \gcd(a,b,c) &= \prod_{k=1}^{r} p_k^{\min(\alpha_k,\beta_k,\gamma_k)}\end{aligned}$$

for $\alpha_i^2+\beta_i^2+\gamma_i^2>0$. This expands as expected with additional terms in the gcd.

Lemma 4.60. *(Gauss Lemma) If $f,g\in\mathbb{Z}[x]$ are primitive, then so is fg.*

Proof. [✓] □

Corollary 4.61. *(Gauss Lemma 2) If the primative polynomial $f\in\mathbb{Z}[x]$ can be factorized as the product of two polynomials in $\mathbb{Q}[x]$, then f can be factorized as the product of two polynomials in $\mathbb{Z}[x]$.*

Proof. Let $f(x)=g(x)h(x)$ for $g,h\in\mathbb{Q}[x]$. Then there are $g',h'\in\mathbb{Z}[x]$ such that $f(x)=g'(x)h'(x)$. Observe $g(x)\in\mathbb{Q}[x]$, $g(x)=\frac{a}{b}\tilde{g}(x)$ where $\tilde{g}(x)\in\mathbb{Z}[x]$ and $\tilde{g}(x)$ is primitive.

Notice

$$\underbrace{f(x)}_{\text{primitive}} = \frac{a}{b}\,\underbrace{\tilde{g}(x)\tilde{h}(x)}_{\text{also primative}},$$

for $\tilde{g},\tilde{h}\in\mathbb{Z}[x]$ primative and $\gcd(a,b)=1$. Then $bf(x)=a\tilde{g}(x)\tilde{h}(x)$. If $b\neq 1$, there exists prime p, $p\mid b$, $p\nmid a$, $p\mid \text{coef}(\tilde{g}(x)\tilde{h}(x))$ so $\tilde{g}\tilde{h}$ is not primative. A contradiction.

So $b=1$,

$$f(x)=a\,\underbrace{\tilde{g}\tilde{h}}_{\in\mathbb{Z}[x]},$$

and a divides every coefficient of f. Since f is primative, $a=1$ so $f=\tilde{g}\tilde{h}$ primative. □

Proposition 4.62. *If f is a monic polynomial in $\mathbb{Z}[x]$ (so f is primitive) and f can be factorized as a product of 2 polynomials in $\mathbb{Q}[x]$, then f can be written as a product of monic polynomials in $\mathbb{Z}[x]$.*

Proof. From Gauss Lemma, $f=gh$ for $g,h\in\mathbb{Z}[x]$. The leading coefficient is 1 = a_mb_n for $a_m,b_n\in\mathbb{Z}$. Then $a_m=b_n=1$ or $a_m=b_n=-1$. Then $g=a_mx^m+\cdots+a_0$, $h=b_nx^n+\cdots+b_0$. □

Theorem 4.63. *(Eisenstein Criterion) Let $f(x)=a_0+\cdots+a_nx^n\in\mathbb{Z}[x]$. Suppose there is a prime p such that $p\mid a_0,a_1,\ldots,a_{n-1}$ but $p\nmid a_n$ and $p^2\nmid a_0$. then $f(x)$ is irreducible over $\mathbb{Q}[x]$.*

Proof. Assume f reducible over $\mathbb{Q}$, $f=gh$ for $g,h\in\mathbb{Q}[x]$, so $f=\frac{A}{B}\tilde{g}\tilde{h}$ for $\tilde{g},\tilde{h}\in\mathbb{Z}[x]$ primative and $\gcd(A,B)=1$. Then $Bf=A\tilde{g}\tilde{h}$ and $\tilde{g}=b_0+b_1x+\cdots+b_rx^r$ and $\tilde{h}=c_0+c_1x+\cdots+c_sc_sx^s$. Then $p\nmid Ba_0=Ab_0c_0$ and $p\nmid Ba_n=Ab_rc_s$. □

Example 4.64.

(1) $f(x) = x^5 - 4x^4 + 6x^3 - 2x^2 - 8x + 2$, then $p = 2$ so by the Eisenstein criterion $f(x)$ is irreducible.
(2) p prime, $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$ is irreducible over $\mathbb{Q}[x]$. Note

$$\begin{aligned} f(x+1) = \frac{(x+1)^p + 1}{(x+1) - 1} &= \frac{x^p + \binom{p}{1}x^{p-1} + \cdots + px + 1 - 1}{x} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{2}x + p \end{aligned}$$

Apply EC and we get f is irreducible over $\mathbb{Q}[x]$.
(3) *(Lemma)* $f(x) \in \mathbb{Z}[x]$, irreducible and primitive in $\mathbb{Q}[x] \implies f(x)$ irreducible in $\mathbb{Z}[x]$.
Proof. Suppose f is reducible in $\mathbb{Z}$, $f = gh$, $g, h \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$ so g or h should be irreducible in $\mathbb{Q}[x]$, without loss of generality $g \in (\mathbb{Q}[x])^\times = \mathbb{Q}^\times$. So $g = c_0 \neq 0$ for $c_0 \in \mathbb{Z}$. □
(4) $f(x, y) = x^3 + 3x^2y + 3xy^2 - 5 \in \mathbb{Q}[x, y]$, y "prime,"

$$f(x, y) \in \mathbb{Q}[y][x] \subset \underbrace{\mathbb{Q}(y)}_{\text{Quotient field of an integral domain}}[x]$$

Then $f(x, y)$ is irreducible over $\mathbb{Q}[y]$ and it is monic, so it is primative so $f(x, y)$ is irreducible over $\mathbb{Q}[y]$.

4.6. **Worked Problems.**

Problem 4.65. Prove that a finite nonzero ring with no zero divisors is a division ring and a finite integral domain is a field.

Proof. Let R be a finite nonzero ring with no zero divisors. Let $a \in R$ such that $a \neq 0$. Since R is finite, there are only finitely many distinct powers of x. Suppose that $a^m = a^n$ for some $m > n$. Then

$$0 = a^m - a^n = a^n(a^{m-n} - 1).$$

Since R has no zero divisors, one of a^n and $a^{m-n} - 1$ must be zero.

If $a^n = 0$, then a is zero divisor. A contradiction. Thus $a^{m-n} - 1 = 0$. It follows that $a^{m-n} = a \cdot x^{m-n} - 1 = 1$. So a has an inverse in R. Since a is arbitrary (but nonzero) R is a division ring.

Let R be a finite integral domain. Let $a \in R$ such that $a \neq 0$. Define $\phi : R \to R$ and $\phi(x) = ax$. Note that

$$\ker \phi = \{x \in R : ax = 0\}.$$

Since R is an integral domain, it has no proper zero divisors. So $ax = 0$ implies $a = 0$ or $x = 0$. By assumption, we get $x = 0$. Thus $\ker \phi = \{0\}$. Since the kernel of ϕ is trivial, we get ϕ is injective. Since ϕ is an injective map from a finite set to itself, ϕ is surjective.

Since ϕ is sujective and $1 \in R$, there exists an $x \in R$ such that $\phi(x) = ax = 1$. Thus R is a commutative division ring, i.e., a field. □

Problem 4.66. Let R be a commutative ring with 1. Define the set $R[[x]]$ of *formal power series* (the convergence is not considered here) in the indeterminate x with coefficients from R to be all formal infinite sums

$$\sum_{n=0}^{\infty} a_n x^n := a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$$

Define addition and multiplication in $R[[x]]$ as follows:

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n := \sum_{n=0}^{\infty} (a_n + b_n) x^n.$$

$$\sum_{n=0}^{\infty} a_n x^n \times \sum_{n=0}^{\infty} b_n x^n := \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n.$$

(1) Prove that $R[[x]]$ is a commutative ring with 1.
(2) Show that $1 - x$ is invertible in $R[[x]]$. What is $(1 - x)^{-1}$?
(3) Prove that $\sum_{n=0}^{\infty} a_n x^n$ is invertible in $R[[x]]$ iff a_0 is invertible in R.

Proof.

(1) Nope. [✓]
(2) Note $1 - x = \sum_{n \in \mathbb{N}} c_n x^n$ where $c_0 = 1$, $c_1 = -1$, and $c_{\geqslant 2} = 0$.
Suppose $(1 - x)^{-1} = \sum_{n \in \mathbb{N}} x^n$. We get

$$(1 - x)(1 - x)^{-1} = \left(\sum_{n=0}^{\infty} c_n x^n \right) \left(\sum_{n=0}^{\infty} x^n \right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} c_k \right) x^n.$$

Notice that for $n \geqslant 1$, we get $\sum_{k=0}^{n} c_k = 0$, but $c_0 = 1$ so $(1 - x)(1 - x)^{-1} = 1$. As desired.
(3) Let $f(x) = \sum_{n=0}^{\infty} a_n x^n$ and $g(x) = \sum_{n=0}^{\infty} b_n x^n$. We need to show that $f(x)g(x) = 1$. Note $f(x)g(x) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k b_{n-k} \right) x^n$. This will only equal 1 when $a_0 b_0 = 1$ and $\sum_{k=0}^{n} a_k b_{n-k} = 0$. For all $k \geqslant 1$.

If a_0 is not invertible, then $g(x)$ does not exist and $f(x)$ is not invertible in $R[[x]]$. If a_0 is invertible, then $b_0 = a_0^{-1}$. We can then define

$$b_k = -b_0 \sum_{k=0}^{n} a_k b_{n-k}$$

which produces a solution for $g(x)$. Thus $f(x)$ is invertible. As desired.

□

Problem 4.67. Let I and J be two ideals of a ring R. Denote $I + J = \{x + y \mid x \in I, y \in J\}$. Prove that $I + J$ is also an ideal in R and is the smallest ideal containing both I and J.

Proof. To show $I + J$ is an ideal, we must show that $I + J$ is closed under subtraction and two-sided multiplication.

Let $i + j, i' + j' \in I + J$. Then $(i + j) - (i' + j') = (i - i') + (j - j') \in I + J$ since I and J are closed under subtraction.

Let $r \in R$. Then $r(i + j) = ri + rj \in I + J$ and $(i + j)r = ir + jr \in I + J$ since I and J are two-sided ideals. Thus $I + J$ is an ideal of R.

Note that both I and J contain 0. Then $I = I + 0 \subseteq I + J$ and $J = 0 + J \subseteq I + J$. Thus $I, J \subset I + J$.

Let K be an ideal of R and $I \cup J \subseteq K$. Let $i + j \in I + J$. Then $i + j \in K$ since K is closed under addition. Thus $I + J \subseteq K$ which means $I + J$ is the smallest ideal containing both I and J. □

Problem 4.68. Let I and J be ideals of a ring R. Denote IJ the set of all elements that can be written as finite sums of elements of the form xy, where $x \in I$, $y \in J$. Prove that IJ is an ideal of R and $IJ \subset I \cap J$. Find an example that $IJ \neq I \cap J$.

Proof. Let $a = \sum_n x_i y_i \in IJ$ and $b = \sum_m x_i' y_i' \in IJ$ for $x_i, x_i' \in I$, $y_i, y_i' \in J$, and $n, n \in \mathbb{Z}$.

Ideals are closed under subtraction. Since I, J are ideals, $-x_i \in I$ so $-b = \sum_m (-x_i') y_i' \in IJ$. Then, clearly, $a - b \in IJ$.

Let $r \in R$. Since I, J are (two-sided) ideals of R, we have $ra = \sum_n (rx_i) y_i \in IJ$ and $ar = \sum_n x_i (y_i r) \in IJ$. Thus IJ is an ideal of R.

Note every product xy is in both I and J since they are ideals, thus closed under arbitrary multiplication of elements of R. Since I and J are both closed under addition, $I \cap J$ is also closed under addition, so it follows that the sum of products xy must also be in $I \cap J$. Thus $IJ \subseteq I \cap J$.

Here is an example where $IJ \neq I \cap J$. Consider $I = J$ and $I = \langle x \rangle \subset \mathbb{R}[x]$. Then $IJ = I^2 = \langle x^2 \rangle \neq \langle x \rangle = I = I \cap J$. □

Problem 4.69. Prove that $\mathbb{R}[x]/\mathbb{R}[x](x^2 + 1) \cong \mathbb{C}$ (ring isomorphism).

Proof. Let $\phi : \mathbb{R}[x] \to \mathbb{C}$ where x, the variable in the polynomial, maps to i. Let $c = \sum_n a_k x^k \in \mathbb{R}[x]$ and $d = \sum_m b_k x^k \in \mathbb{R}[x]$ for $a_k, b_k \in \mathbb{R}$. Then

$$\phi(c + d) = \sum_n a_k i^k + \sum_m b_k i^k = \phi(c) + \phi(d)$$

and

$$\phi(cd) = \sum_n a_k i^k \sum_m b_k i^k = \phi(c)\phi(d).$$

Also, $1_{\mathbb{R}[x]} \mapsto 1_{\mathbb{C}}$. So ϕ is a ring homomorphism.

Note $\phi(x^2 + 1) = i^2 + 1 = 0$, which implies $\ker \phi = \mathbb{R}[x](x^2 + 1)$. By the first isomorphism theorem, $\mathbb{R}[x]/\mathbb{R}[x](x^2 + 1) \cong \mathbb{C}$. □

Problem 4.70. Ring of integers $\mathbb{Z}$. Prove the following

(1) Every ideal in $\mathbb{Z}$ is of the form $n\mathbb{Z}$, for some n.
(2) $n\mathbb{Z}$ is prime if and only if n is prime or $n = 0$.

Proof.

(1) For $n = 0$, $n\mathbb{Z} = \{0\}$ and $\mathbb{Z}/\{0\} \cong \mathbb{Z}$. This is the zero ideal.

Let I be a non-zero ideal. Then I has a positive integer. Let n be the smallest positive integer in I. If $b \in I$, then $b = qn + r$ for some $q \in \mathbb{Z}$ and $r \in [0, n)$. But $r \in I$, since $r = b - qn$ and $b \in I$ by construction and $qn \in I$ since I is an ideal. However, since n is the smallest positive integer in I and $r \in [0, n)$, we get $r = 0$. So $b = qn$, which means $I = n\mathbb{Z}$. As desired.

(2) Note $a \in n\mathbb{Z}$ if and only if $n \mid a$. If $n = 0$, then we have the zero ideal which is a prime ideal.

Suppose $n\mathbb{Z}$ is not prime. Then for $a, b \in \mathbb{Z}$ where $ab \in n\mathbb{Z}$ and $a, b \notin n\mathbb{Z}$. Then $n \mid ab$ but $n \nmid a$ and $n \nmid b$. If n were prime then n would divide one of a or b, so n cannot be prime if $n\mathbb{Z}$ is not prime.

Conversely, suppose $n > 0$ is not prime. Then there are positive integers $a, b < n$ such that $n = ab$. Then $ab \in n\mathbb{Z}$, but $a \in n\mathbb{Z}$ and $n \mid a$ contradicts the assumption that $a < n$. Similarly, a contradiction is found for b. Thus $n\mathbb{Z}$ must not be prime when n is not prime.

□

Problem 4.71. Let $f : R \to S$ be a ring homomorphism. I, J are ideals in R, S, respectively.

(1) Prove that $f^{-1}(J)$ is an ideal in R containing $\ker f$.
(2) If f is surjective, then $f(I)$ is an ideal in S. Give an example to show that the conclusion is not true if f is not surjective.

Proof.

(1) Let $r, x \in R$ such that $f(x) \in J$. Since f is a ring homomorphism, $f(rx) = f(r)f(x) \in J$, so $rx \in f^{-1}(J)$. Similarly, $xr \in f^{-1}(J)$. Thus $f^{-1}(J)$ is an ideal in R.
(2) Let $x \in f(I), s \in S$. Since f is surjective, there is some $r \in R$ such that $f(r) = s$. So $f^{-1}(sy) = rf^{-1}(f) \in I$. Thus $sy \in f(I)$. Similarly, $ys \in f(I)$ so $f(I)$ is an ideal in R.

Here is a counterexample for f not surjective. Let $f : \mathbb{Z} \to \mathbb{Q}$ where $x \mapsto x$. $\mathbb{Z}$ is a trivial ideal of itself, but not an ideal of $\mathbb{Q}$. Consider $(1/2) \cdot 3 = 3/2 \notin \mathbb{Z}$.

□

Problem 4.72. Find all subrings of $\mathbb{Z}$.

Proof. Let $R \subset \mathbb{Z}$ be a (unital) subring. Then $1 \in R$. Since R is a group under addition we have $1 + 1 + \cdots + 1 = n \in R$, for n additions of 1 and $-n \in R$. Thus the only subring of $\mathbb{Z}$ is itself.

If we are not considering subrings to be unital, then all subrings, by similar reasoning to the above, are of the form $n\mathbb{Z}$ for $n \in \mathbb{Z}$. However, we have only refered to subrings as unital in class. □

Problem 4.73. Let R be an integral domain with unit element such that $R[X]$ is a principle ideal domain. Prove that R is a field.

Proof. An integral domain is a nonzero commutative ring, so we must only show that R is a division ring as well. Let $r \in R$ and $r \neq 0$. Then $(r, X) \subset R[X]$ is an ideal. Thus $(r, X) = (f)$ for some $f \in R[X]$. So there exist $p, q \in R[X]$ such that $fp = r$ and $fq = X$. However, $R[X]$ has the property that $\deg fg = \max(\deg f, \deg g)$ since R is an integral domain. So it follows that $\deg f = 0$ because $\deg r = 0$ by construction, so $f = a$ and $p = b$ for $a, b \in R$. Note that q is of the form $q = c + dX$ for $c, d \in R$. So we have

$$X = fq = a(c + dX) = ac + adX$$

Thus $ad = 1$, so $(f) = (a) = R[X]$. We then see that there exists $\alpha, \beta \in R[X]$ such that

$$\alpha r + \beta X = 1.$$

To account for the degrees of r and X, β must equal 0 which implies $\alpha r = 1$. Then $r = 1/\alpha$. Since r is arbitrary, R is a commutative division ring, i.e., a field. □

Problem 4.74. Let R be a commutative ring with unit element and the ideal J is the intersection all maximal ideals in R. Show that $x \in J$ if and only if $1 - xy \in R^\times$ for all $y \in R$.

Proof. Note that $R^\times = \{x \in R \mid \exists y \in R : xy = yx = 1\}$. Let $x \in J$. Suppose that $1 - xy \notin R^\times$. Then $1 - xy \in M$ for some maximal ideal M. However, since $x \in J \subset M$, we have $xy \in M$. Thus $(1 - xy) + xy = 1 \in M$, a contradication. So every $1 - xy \in R^\times$.

Conversely, suppose $x \notin J$. Then $x \notin M$ for some maximal ideal $M \neq R$. Thus $R = M + Rx$, i.e., $1 = m + xy$ for some $y \in R$ and $m \in M$. So we see that $m = 1 - xy \notin R^\times$ since $M \neq R$. To be clear, we have shown the contrapositive $x \notin J$ implies $1 - xy \notin R^\times$. □

Problem 4.75. Prove that in principal ideal domain R, two ideals (a) and (b) are coprime ($(a)+(b)=R$) if and only if a greatest common divisor of a and b is 1.

Proof. Let $(a)+(b)=R$. Note that $1\in R$, so $(a)+(b)=(a,b)=(1)$. However, the generator for a principal ideal generated by (a) and (b) is a greatest common divisor of a and b. As desired.

Conversely, let 1 be a greatest common divisor of a and b. Then we have the R-linear combination $ax+by=1$ for some elements $x,y\in R$. Thus $1\in(a)+(b)$, and it follows that $(a)+(b)=R$ since an ideal that contains 1 is the whole ring. □

Lemma 4.76. *$2,3,1+\sqrt{-5},1-\sqrt{-5}$ are irreducible elements in $\mathbb{Z}[\sqrt{-5}]$.*

Proof. Define $d:\mathbb{Z}[\sqrt{-5}]\to\mathbb{Z}^+$ with $a+\sqrt{-5}b\mapsto a^2+5b^2$. Then $d(2)=4$, so if 2 factored into a product of non-unit elements each factor would have a norm of 2 which does not exist in R, so 2 is irreducible. Similarly, 3 is irreducible. $1+\sqrt{-5}$ and $1-\sqrt{-5}$ both have $d(\cdot)=6$, but there are still no elements x where $d(x)=2,3$ in $\mathbb{Z}[\sqrt{-5}]$, so these are irreducible as well. □

Lemma 4.77. $(\mathbb{Z}[\sqrt{-5}])^\times=\{\pm1\}$.

Proof. Define $d:\mathbb{Z}[\sqrt{-5}]\to\mathbb{Z}^+$ with $a+\sqrt{-5}b\mapsto a^2+5b^2$. Then $d(xy)=d(x)d(y)$. Let $r\in\mathbb{Z}[\sqrt{-5}]$. Then there is an $a\in\mathbb{Z}[\sqrt{-5}]$ such that $ra=1$. Then $d(ra)=d(r)d(a)=1$. So $d(r)=1$ and if $r=x+y\sqrt{-5}$, we must have $x=\pm1, y=0$ and $r\in\{\pm1\}$. □

Problem 4.78. Show that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Proof. Note that $6=2\cdot3=(1+\sqrt{-5})(1-\sqrt{-5})$. However, $2,3,1+\sqrt{-5}$, and $-\sqrt{-5}$ are irreducible elements. Note that $R^\times=\{\pm1\}$ so these factors are not associates. So we see that 6 has two distinct factorizations which implies that $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain. □

Problem 4.79. Show that $\mathbb{Z}[\sqrt{-2}]$ is a UFD.

Proof. Since every Euclidean domain is a UFD, it is enough to show that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain. Let $d:\mathbb{Z}[\sqrt{-2}]\to\mathbb{Z}^+$ and $a+b\sqrt{-2}\mapsto a^2+2b^2$, i.e., $\left|a+b\sqrt{-2}\right|^2$ for every $a,b\in\mathbb{Z}$. Let d' be a map similarly defined by from $\mathbb{Q}[\sqrt{-2}]\to\mathbb{Z}^+$. Note that $d(xy)=d(x)d(y)$ and $d'(xy)=d'(x)d'(y)$.

Let $x:=a+b\sqrt{-2}, y:=c+d\sqrt{-2}\in\mathbb{Z}[\sqrt{-2}]$ and $y\neq0$. Then

$$\frac{x}{y}=\frac{(a+b\sqrt{-2})\cdot(c-d\sqrt{-2})}{c^2+2d^2}=:e+f\sqrt{-2}\in\mathbb{Q}[\sqrt{-2}].$$

Let $g,h\in\mathbb{Z}$ such that $|e-g|,|f-h|\leqslant1/2$. Furthermore, let $q=g+h\sqrt{-2}$ and $r=x-qy$. Then we have $x=qy+r$ and, by construction,

$$d(r)=d(x-qy)\leqslant\frac{3}{4}d(y)<d(y)$$

Since $d(r)<d(y)$, we get $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain. As desired. □

Lemma 4.80. *Let R be a commutative ring and let I be an ideal of R. Then $R[x]/(I+(x))\cong R/I$.*

Proof. Let $\phi:R[x]\to R/I$ be a map where $\phi(\sum_{i=0}^n a_ix^i)=a_0+I$. Note that ϕ is a surjective ring homomorphism. Then $\ker\phi=I+(x)$; this follows from the fact that if $f(x)=b+xg(x)\in I+(x)$, then $\phi(f)=\phi(b)+\phi(x)\phi(g)=I$. Then $I+(x)\subseteq\ker\phi$. Let $h(x)\in\ker\phi$, where $h(x)=\sum_{i=0}^n a_ix^i$. Then $a_0\in I$, so $h(x)\in I+(x)$. As desired. □

Problem 4.81. Prove that the ideals $(x) := x\mathbb{Q}[x,y]$ and $(x,y) := \{xf(x,y) + yg(x,y) \mid f,g \in \mathbb{Q}[x,y]\}$ are prime ideals in $\mathbb{Q}[x,y]$ but only the latter ideal is a maximal ideal.

Proof. Recall the definitions of a prime ideal and maximal ideal. Let R be a commutative ring. An ideal $P \subset R$ is called prime if whenever $xy \in P$, either $x \in P$ or $y \in P$. An ideal $M \subset R$ is called maximal if there is no ideal between M and R, i.e., for ideal U is R and $M \subseteq U \subset R$ implies $U = M$. Furthermore, An ideal P of a ring R is prime if and only if R/P is an integral domain. Also, note that an ideal M of a ring R is maximal if and only if R/M is a field.

It follows from the above definitions and the first isomorphism theorem for rings that $R[x]/(x) \cong R$. Let $(\mathbb{Q}[y])[x]$ be the polynomial ring with coefficients in $\mathbb{Q}[y]$. Then $(\mathbb{Q}[y])[x]/(x) \cong \mathbb{Q}[y]$. Note that $\mathbb{Q}[y]$ is an integral domain, so (x) is prime. Further note that $\mathbb{Q}[y]$ is not a field since y does not have an inverse. So (x) is not maximal.

By Lemma 4.80, for a commutative ring R, we have $R[x,y]/(x,y) \cong (R[x])[y]/((x)+(y)) \cong R[x]/(x) \cong R$. Therefore $\mathbb{Q}[x,y]/(x,y) \cong \mathbb{Q}$, which is known to be a field. So we have (x,y) is maximal and it follows that it is prime. □

Lemma 4.82. *A polynomial ring over a field is a Euclidean domain.*

Proof. Let $a(x), b(x) \in F[x]$, where F is a field. We must show that if $F[x]$ is a Euclidean domain, that there exists unique $q(x), r(x) \in F[x]$ such that $b(x) = q(x)a(x) + r(x)$ and $r(x) = 0$ or $\deg r(x) < \deg a(x)$. If $b(x) = 0$ we set $q(x) = r(x) = 0$, and if $\deg b(x) < \deg a(x)$ then we set $q(x) = 0$ and $r(x) = b(x)$. Suppose $b(x) \neq 0$ and $\deg b(x) \geqslant \deg a(x)$. Then, by induction on $\deg b(x) = n$. If $n = 0$, then $\deg a(x) = 0$ and the result follows from the fact F is a field. Suppose $\deg r(x) < \deg a(x)$ for $\deg b(x) < n$ and let $b(x) = b_0 + \cdots + b_n x^n$, i.e., $\deg b(x) = n$. Fix $a(x) = a_0 + \cdots + a_k x^k$ where $n \geqslant k$. Now consider the polynomial $c(x) = b(x) - b_n a_k^{-1} x^{n-k} a(x)$. Note $\deg c(x) < n$ so, by the induction hypothesis, there are $q'(x), r(x)$ such that $c(x) = q'(x)a(x) + r(x)$ and $r(x) = 0$ or $\deg r(x) < \deg a(x)$. Now let $q(x) = q'(x) + b_n a_k^{-1} x^{n-k}$; this gives us $b(x) = q(x)a(x) + r(x)$ with $r(x) = 0$ or $\deg r(x) < \deg a(x)$. As desired.

Now we will show that this result is unique. Suppose $q(x)a(x) + r(x) = b(x) = q'(x)a(x) + r'(x)$. Then $a(x)(q(x) - q'(x)) = r'(x) - r(x)$. Since the degree of the right hand side is less than the degree of $a(x)$, $q(x) - q'(x) = 0$. Thus $q(x) = q'(x)$ it follows that $r(x) = r'(x)$. □

Problem 4.83.

(1) Let $f(x) \in F[x]$ be a polynomial of degree $n \geqslant 1$. Prove that for each element $\overline{g(x)} \in F[x]/(f(x))$, there is a unique polynomial $g_0(x)$ of degree $\leqslant n-1$ or $g_0(x) = 0$ such that $\overline{g(x)} = \overline{g_0(x)}$.
(2) Let F be a finite field of q elements and $f(x) \in F[x]$ with $\deg(f) = n \geqslant 1$. Prove that $F[x]/(f(x))$ has q^n elements.

Proof.

(1) By Lemma 4.82, $F[x]$ is a Euclidean domain. By the division algorithm, there exist $h(x)$ and $g_0(x)$ such that $g(x) = h(x)f(x) + g_0(x)$ and $\deg g_0 < n$. Then $\overline{g(x)} = \overline{g_0(x)}$ and g_0 is unique, which follows from Lemma 4.82.
(2) By the previous part, the number of elements of $F[x]/(f(x))$ is the number of polynomials in $F[x]$ with degree less than n. Every polynomial of this type is uniquely determined by its n coefficients, where each coefficient takes one of the q values in F. Thus $F[x]/(f(x))$ contains q^n elements.

□

Lemma 4.84. *Let $f(x)$ be a polynomial in $F[x]$. Then $F[x]/(f(x))$ is a field if $f(x)$ is irreducible.*

Proof. Suppose $f(x)$ is irreducible. Then $f(x)$ is prime, and $(p(x))$ is a prime ideal. Since $F[x]$ is a principal ideal domain, $(p(x))$ is maximal. Then $F[x]/(f(x))$ is a field. □

Problem 4.85. Denote $\mathbb{F}_{11}$ be a finite field of 11 elements. Prove that $K_1 = \mathbb{F}_{11}[x]/(x^2 + 2x + 2)$ and $K_2 = \mathbb{F}_{11}[y]/(y^2 + 1)$ are both fields with 121 elements. Prove that the map which sends the element $p(\bar{x})$ of K_1 to the element $p(\bar{y} - 1)$ of K_2, where p is any polynomial over $\mathbb{F}_{11}$ is well-defined and gives a ring isomorphism from K_1 to K_2.

Proof. Note that $\mathbb{F}_{11} = \mathbb{Z}/11\mathbb{Z}$. So $\mathbb{F}_{11}[x] = \{$the set of all polynomials with coefficients in $\{0, 1, 2, \ldots, 11\}\}$.

We first show that $f(x) = x^2 + 2x + 2$ and $g(y) = y^2 + 1$ are irreducible over $\mathbb{F}_{11}$. We see $f(x), g(y)$ are irreducible since $f(a), g(a) \neq 0$ for each $a \in \mathbb{F}_{11}$, i.e., they have no roots and are not linear in $\mathbb{F}_{11}$. Thus, by Problem 4.832 and Lemma 4.84, $\mathbb{F}_{11}[x]/(x^2 + 2x + 2)$ and $F[y]/(y^2 + 1)$ are finite fields containing 121 elements.

Define $\psi : \mathbb{F}_{11}[x] \to \mathbb{F}_{11}[x]/(x^2 + 2x + 2)$ by $x \mapsto x + 1$. Then $\psi(y^2 + 1) = (x + 1)^2 + 1 = x^2 + 2x + 2 = 0$. So we see that $(x^2 + 1) \subseteq \ker \psi$. By Lemma 4.82, $\mathbb{F}_{11}[x]$ is a Euclidean domain, and since $x^2 + 1$ is irreducible, $x^2 + 1$ is prime and $(x^2 + 1)$ is maximal. Note ψ is nontrivial; consider $\psi(1) = 1$. Thus $\ker \psi = (x^2 + 1)$. By the first ring isomorphism theorem, there is an injective ring homomorphism $\phi : \mathbb{F}_{11}[x]/(x^2 + 1) \to F[y]/(y^2 + 2y + 2)$. Since $\mathbb{F}_{11}[x]/(x^2 + 1)$ and $F[y]/(y^2 + 2y + 2)$ have the same number ofeelements, ϕ is surjective. Thus ϕ is a ring isomorphism between K_1 and K_2. □

Problem 4.86. Find all monic irreducible polynomials of degree $\leqslant 3$ in $\mathbb{F}_3[x]$. Use it to construct a field having 27 elements.

Proof. Note that $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$. So $\mathbb{F}_3[x] = \{$the set of all polynomials with coefficients 0,1,2$\}$.

All monic polynomials of degree 1 are irreducible. For $\mathbb{F}_3[x]$, these are

(1) x, (2) $x + 1$, (3) $x + 2$.

The monic polynomials of degree 2 are:

(1) $x^2 = x \cdot x$,
(2) $f(x) = x^2 + 1$ is irreducible; $f(0) = 1$ and $f(1) = f(2) = 2$,
(3) $x^2 + 2 = (x + 1)(x + 2)$,
(4) $x^2 + x = x(x + 1)$,
(5) $x^2 + 2x = x(x + 2)$,
(6) $x^2 + x + 1 = (x + 2)^2$,
(7) $f(x) = x^2 + x + 2$ is irreducible; $f(0) = f(2) = 2$ and $f(1) = 1$,
(8) $x^2 + 2x + 1 = (x + 1)^2$,
(9) $f(x) = x^2 + 2x + 2$ is irreducible; $f(0) = f(1) = 2$ and $f(2) = 1$.

The monic polynomials of degree 3 are:

(1) $x^3 = x \cdot x \cdot x$,
(2) $x^3 + 1 = (x + 1)^3$,
(3) $x^3 + 2 = (x + 2)^3$,
(4) $x^3 + x = x(x^2 + 1)$,
(5) $x^3 + 2x = x(x + 1)(x + 2)$,
(6) $x^3 + x + 1 = (x + 2)(x^2 + 2x + 2)$,

(7) $x^3 + x + 2 = (x + 1)(x^2 + 2x + 2)$,
(8) $f(x) = x^3 + 2x + 1$ is irreducible; $f(0) = f(1) = f(2) = 1$,
(9) $f(x) = x^3 + 2x + 2$ is irreducible; $f(0) = f(1) = f(2) = 2$,
(10) $x^3 + x^2 = x^2(x + 1)$,
(11) $x^3 + x^2 + 1 = (x + 2)(x^2 + 2x + 2)$,
(12) $f(x) = x^3 + x^2 + 2$ is irreducible; $f(0) = f(2) = 2$ and $f(1) = 1$,
(13) $x^3 + x^2 + x = x(x + 2)^2$,
(14) $x^3 + x^2 + 2x = x(x^2 + x + 2)$,
(15) $x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$,
(16) $f(x) = x^3 + x^2 + x + 2$ is irreducible; $f(0) = f(1) = 2$ and $f(2) = 1$,
(17) $f(x) = x^3 + x^2 + 2x + 1$ is irreducible; $f(0) = 1$ and $f(1) = f(2) = 2$,
(18) $x^3 + x^2 + 2x + 2 = (x + 1)^2(x + 2)$,
(19) $x^3 + 2x^2 = x^2(x + 2)$,
(20) $f(x) = x^3 + 2x^2 + 1$ is irreducible; $f(0) = f(1) = 1$ and $f(2) = 2$,
(21) $x^3 + 2x^2 + 2 = (x + 1)(x^2 + x + 2)$,
(22) $x^3 + 2x^2 + x = x(x + 1)^2$,
(23) $x^3 + 2x^2 + 2x = x(x^2 + 2x + 2)$,
(24) $f(x) = x^3 + 2x^2 + x + 1$ is irreducible; $f(0) = f(2) = 1$ and $f(1) = 2$,
(25) $x^3 + 2x^2 + x + 2 = (x + 2)(x^2 + 1)$,
(26) $x^3 + 2x^2 + 2x + 1 = (x + 1)(x + 2)^2$,
(27) $f(x) = x^3 + 2x^2 + 2x + 2$ is irreducible; $f(0) = 2$ and $f(1) = f(2) = 1$.

All together, the irreducible monic polynomials of $\mathbb{F}_3[x]$ with degree $\leqslant 3$ are:

(1) x,
(2) $x + 1$,
(3) $x + 2$,
(4) $x^2 + 1$,
(5) $x^2 + x + 2$,
(6) $x^2 + 2x + 2$,
(7) $x^3 + 2x + 1$,
(8) $x^3 + x^2 + 2$,
(9) $x^3 + x^2 + x + 2$,
(10) $x^3 + x^2 + 2x + 1$,
(11) $x^3 + 2x^2 + 1$,
(12) $x^3 + 2x^2 + x + 1$,
(13) $x^3 + 2x^2 + 2x + 2$.

Consider: $\mathbb{F}_3[x]/(x^3+2x^2+1)$. By Lemma 4.84, this is a field. By Problem 4.832 this has 27 elements. □

Problem 4.87. Prove that $x^4 + 4x^3 + 6x^2 + 2x + 1$ is irreducible in $\mathbb{Z}[x]$.

Proof. Let us substitute $x = y - 1$ in the polynomial $f(x) := x^4 + 4x^3 + 6x^2 + 2x + 1$. Then we get

$$(y - 1)^4 + 4(y - 1)^3 + 6(y - 1)^2 + 2(y - 1) + 1 = y^4 - 2y + 2.$$

Let $p = 2$. Then we see that $p \mid a_3, a_2, a_1, a_0$, $p \nmid a_4$, and $p^2 \nmid a_0$. Then by Eisenstein's Criterion, we get f is irreducible in $\mathbb{Q}[x]$. It follows that f is irreducible in $\mathbb{Z}[x]$. □

Problem 4.88. Let F be a finite field. Prove that $F[x]$ contains infinitely many prime elements.

Proof. Suppose that $F[x]$ has finitely many primes. Let $p_1, p_2, \ldots, p_n$ be these primes. Let $q = \prod p_i$. By Lemma 4.82, $F[x]$ is a Euclidean domain, and, consequently, a UFD. Note that $\deg p_i \geqslant 1$, since constants in $F[x]$ are units. Then $\deg q + 1 \geqslant 1$, and in particular is not a unit or zero. Thus $q + 1$ can be written as a product of irreducibles in $F[x]$. Since $F[x]$ is a UFD, these elements are the p_i previously mentioned. Suppose $q + 1 = p_j s$ for some p_j in the set of p_i and $s \in F[x]$. Then $1 = p_j s - q$, but note that there must be some $a \in F[x]$ such that $1 = p_j(s - aq)$. Thus p_j is a unit which contradicts our assumption that it is prime. Therefore $F[x]$ contains infinitely many prime elements. □

Problem 4.89. Let F be a field and $f(x) \in F[x]$ and $\deg(f) = n$. The polynomial $g(x) = x^n f(1/x)$ is called the *reverse* of $f(x)$.

(1) Describe the coefficients of g in terms of the coefficients of f.
(2) Prove that f is irreducible if and only if g is irreducible.

Proof.

(1) If $f(x) = \sum_{i=0}^{n} a_i x^i$, then $g(x) = \sum_{i=0}^{n} a_i x^{n-i}$. Thus $g(x) = \sum_{j=0}^{n} a_{n-j} x^j$. So we see that the coefficients of $g(x)$ are those of $f(x)$ in reverse order.
(2) Note that $\deg g \leqslant \deg f$. This inequality is strict when the constant coefficient of f is zero, otherwise $\deg g = \deg f$ and the reverse of $g = f$.

Let $f \in F[x]$ with a nonzero constant coefficient. Suppose $f(x)$ is irreducible and suppose $g(x)$ is reducible. Then we can write $g(x) = a(x)b(x)$ for $a, b \in F[x]$. Since the constant coefficient of $g(x)$ is nonzero and $F[x]$ is an integral domain, the constant coefficients of a and b are nonzero. So the reverse of $a(x)$ and $b(x)$, which we will call $a'(x)$ and $b'(x)$, are nonconstant polynomials with nonzero constant coefficient such that $f(x) = a'(x)b'(x)$; a contradiction.

Therefore if $f(x)$ is irreducible, then $g(x)$ is irreducible. Since the reverse of $g = f$, it follows that, when $f(x)$ has a nonzero constant term, the converse follows. Thus $f(x)$ is irreducible if and only if $g(x)$ is irreducible.

□

5. Field Theory and Galois Theory

This section is very mediocre and possibly non-sensical. I typed this section very quickly. However, this section outlines what we covered in the course.

Definition 5.1. The *characersitic* of a field F, denoted by $\mathrm{ch}(F)$, is defined to be the smallest positive integer p such that $p \cdot 1_F = 0$ if such a p exists and is defined to be 0 otherwise.

Remark 5.2. The characteristic of a field F, $\mathrm{ch}(F)$, is either 0 or prime p. If $\mathrm{ch}(F) = p$ then for any $\alpha \in F$,

$$p \cdot \alpha = \underbrace{\alpha + \alpha + \cdots + \alpha}_{p \text{ times}} = 0.$$

Definition 5.3. Let K be a field, $F \subset K$, a subfield. Then K is a field extension, K is a vector space over F with the same operation as $(\cdot)$. (Recall the definition of a vector space).

Definition 5.4. For $v_1, v_2, \ldots, v_n \in K$, for K/F,

$$a_1 v_1 + \cdots + a_n v_n = 0_K$$

only if $a_1, a_2, \ldots, a_n = 0$, for $a_i \in F$. Then $v_1, v_2, \ldots, v_n$ are linearly independent.

Definition 5.5. The basis $(v_1, \ldots, v_n)$ spans a space K if for any $k \in K$, there are coefficients a_i such that $a_1 v_1 + \cdots + a_n v_n = K$.

Definition 5.6. The *degree* of K over F is the dimension of the vector space K over F, denoted by $[K : F]$.

Example 5.7.

(1) $[\mathbb{R} : \mathbb{R}] = 1$,
(2) $[\mathbb{C} : \mathbb{R}] = 2$,
(3) $[\mathbb{R} : \mathbb{Q}] = \infty$,

(4) $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.

Theorem 5.8. *Let F be a field, $p(x)$ an irreducible polynomial over F. Then there exists a field K containing a field isomorphic to F such that $p(x)$ has a root inside K.*

Proof. [✓] □

Theorem 5.9. *$p(x) \in F[x], \deg p(x) = n$, an irreducible polynomial, $K = F[x]/(p(x))$, then for $\theta \equiv x \pmod{p(x)}$, $1, \theta, \theta^2, \ldots, \theta^{n-1}$ is a basis of K over F.*

$$[K : F] = n, \quad K = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid a_i \in F\}$$

Proof. [✓] □

Example 5.10.

$$\mathbb{R}[x]/(x^2+1) = K, i \in K \mid i^2 + 1 = 0,$$
$$K = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{C}$$
$$(a_1 + b_1 i)(a_2 + b_2 i) = a(x)(x^2+1) + r(x)$$

Given K an extension of F, $\alpha \in K$, define $F(\alpha)$ to be the smallest subfield of K with α and F.

Theorem 5.11. *Let K be an extension of F, $p(x) \in F[x]$, irreducible and let α be a root in K, then*

$$F(\alpha) \cong F[x]/(p(x)).$$

Proof. [✓] Let $\phi : F[x] \to F(\alpha)$ and $f(x) \mapsto f(\alpha)$. We know $p(\alpha) = 0$, so $(p(x)) \mapsto 0$. Suppose $a(x) \in \ker(\phi)$,

$$a(\alpha) = 0$$
$$a(x) = q(x)p(x) + r(x)$$
$$\underbrace{a(\alpha)}_{=0} = \underbrace{q(\alpha)p(\alpha)}_{=0} + r(\alpha).$$

Thus $r(\alpha) = 0$. A contradiction. □

5.1. **Finite Extensions and Algebraic Extensions.**

Theorem 5.12. *Let L be a finite extension of K be a finite extension of F. Where $[L : K] = m < \infty$, $[K : F] = n < \infty$. Then L is a finite extension over F and $[L : F] = [L : K][K : F] = m \cdot n < \infty$.*

Proof. Outline: $[L : K] = m, \{v_1, v_2, \ldots, v_m\} \subset L$ a basis of L over K. For all $v \in L$, $v = \sum_{i=1}^{m} k_i v_i$ for $k_i \in K$ and $v_i \in L$. $[K : F] = n, \{w_1, \ldots, w_n\}$ a basis of K over F. For all $k \in K$, $k = \sum_{j=1}^{n} f_j w_j$ for $f_j \in F$ and $w_j \in K$.

We must hsow that $v = \sum_{i=1}^{m} k_i v_i = \sum_{j=1}^{m}\sum_{i=1}^{n} f_{ji} w_j v_i$, $\{v_i w_j \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}$ spans L over F and is linearly independent. [✓] □

Corollary 5.13. *If $[L : F] < \infty$, $L \supset K \supset F$ fields, then $[L : K] < \infty, [K : F] < \infty$ and $[L : K] \mid [L : F], [K : F] \mid [L : F]$.*

Proof. [✓] □

Definition 5.14. $K/F, \alpha \in K$, then α is called *algebraic* over F if there exists $f(x) \in F[x]$ and $f(x) \neq 0$ such that $f(\alpha) = 0$.

Definition 5.15. K/F is called an *algebraic extension* if for all $\alpha \in K$ is algebraic over F.

Definition 5.16. α is called transendental over F if for all $f(x) \neq 0$, $f(x) \in F[x]$ and $f(\alpha) \neq 0$.

Examples 5.17.

(1) $\mathbb{R}/\mathbb{Q}$, $\sqrt{2} \notin \mathbb{Q}$ is a solution of $x^2 - 2 \in \mathbb{Q}[x]$, $\sqrt{2}$ is an algebraic element over $\mathbb{Q}$. $\mathbb{R}/\mathbb{Q}$ is not an algebraic extension.

(2) $\mathbb{C}/\mathbb{R}$, $\alpha = a + bi$ for $a, b \in \mathbb{R}$.

$$(\alpha - a)^2 = -b^2 \quad a^2 - 2\alpha a + a^2 + b^2 = 0.$$

α is a solution to $x^2 - 2xa + a^2 + b^2 \in \mathbb{R}[x]$ so α is algebraic and $\mathbb{C}/\mathbb{R}$ is an algebraic extension.

Theorem 5.18. *$K/F, \alpha \in K$ algebraic over F,*

(1) There exists a unique monic irreducible polynomial $m_\alpha(x) \in F[x]$ such that $m_\alpha(\alpha) = 0$.
(2) For all $f(x) \in F[x]$ such that $f(\alpha) = 0$ then $m_\alpha(x) \mid f(x)$ in $F[x]$.
(3) $[F(\alpha) : F] = \deg m_\alpha(x)$.

Proof. Too long. [✓] □

Theorem 5.19. *K/F a field extension. Let*

$$E = \{\alpha \in K \mid \alpha \text{ algebraic over } F\}.$$

Then E is a field and is also algebraic.

Remark 5.20. α is algebraic over F if and only if $[F(\alpha) : F] < \infty$.

Proof. $\boxed{\Rightarrow}$ From above theorem.
$\boxed{\Leftarrow}$ Given $[F(\alpha) : F] < \infty$. $\{v_1, v_2, \ldots, v_n\} \subset F(\alpha)$ a basis.

$$v_i = \sum_{j=m_i}^{s_i} a_{ij}\alpha^j \qquad \alpha = \sum_{i=1}^{m} \beta_i v_i = \sum_{i=1}^{n} \beta_i \sum_{j=m_i}^{s_i} a_{ij}a^j.$$

$f(\alpha) = v$, $f(x) \in F[x]$. □

Example 5.21. $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = ?$. Both $\sqrt{2}, \sqrt{3}$ are algebraic over $\mathbb{Q}$.

- $\sqrt{2}$, $x^2 - 2$ irreducible $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$.
- $\sqrt{3}$, $x^2 - 3$ irreducible $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 2$.

Note that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is an extension of $\mathbb{Q}(\sqrt{2})$ which extends $\mathbb{Q}$.

$$[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \leqslant \frac{[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]}{2}$$

But $x^2 - 3$ might not be irreducible over $\mathbb{Q}(\sqrt{2})$ and

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Then we get $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

Proposition 5.22. *$K_1 = F(\alpha_1, \ldots, \alpha_n), K_2 = F(\beta_1, \ldots, \beta_m), \alpha_1, \ldots, \alpha_n$ is a basis for K_1 over F $[K_1 : F] = n, [K_2 : F] = m$. Then*

$$[F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) : F] \leqslant m \cdot n.$$

If $(m, n) = 1$, then $[F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) : F] = m \cdot n$.

Example 5.23. $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, since $\sqrt{2}$ is a root of $x^2 - 2 \in \mathbb{Q}[x]$, $x^2 - 2$ is irreducible over $\mathbb{Q}$ based on Eisenstein's theorem. Note

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\underbrace{1, \sqrt{2}}_{\text{basis}}).$$

5.2. **Splitting Fields.**

Definition 5.24. Let $f(x) \in F[x]$ be a non-constant polynomial, a field extension K/F is called a splitting field of f if

(1) $f(x) = a_n \prod_{k=1}^{n} (x - \alpha_k), \quad \alpha_k \in K, a_n \in F$,
(2) $K = F(\alpha_1, \ldots, \alpha_n)$, the minimal field containing $F, \alpha_1, \ldots, \alpha_n$.

Examples 5.25. Find a splitting field $K/\mathbb{Q}$, $[K : \mathbb{Q}] =$?

(1) $f(x) = x^2 - 2 \in \mathbb{Q}[x]$, $f(x) = (x - \sqrt{2})(x + \sqrt{2})$, then a splitting field of f over $\mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$; $[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.
(2) $f(x) = x^n - 1 \in \mathbb{Q}[x], \xi = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} = e^{i \frac{2\pi}{n}}$. $f(x) = (x-1)(x-\xi)(x-\xi^2) \cdots (x-\xi^{n-1})$. A splitting field of $f(x)$ over $\mathbb{Q} \to \mathbb{Q}(1, \xi, \xi^2, \ldots, \xi^{n-1}) = \mathbb{Q}(\xi)$. $[\mathbb{Q}(\xi) : \mathbb{Q}] \leqslant n$.

Remarks 5.26.

(1) For every $f \in F[x]$, nonconstant, there exist a splitting field of f over F a field.

Proof. Sketch. Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$, let K be an extension of F, $K = F[x]/p(x)F[x]$. There exists an extension of F that contains a root of $f(x)$. In $K[x]$, $f(x) = (x - \alpha)g(x)$, where $g(x) \in K[x]$ and $\deg g = \deg f - 1$. By induction on degree of f, there exists a splitting field L of g, $L(\alpha)$ a splitting field of f. □

(2) If K is a splitting field of a nonconstant polynomial $f(x) \in F[x]$, $\deg f = n$, then $[K : F] \leqslant n!$.

Proof. Explanation: $[F(\alpha) : F] = \deg p \leqslant \deg f = n$; $f(x) = (x - \alpha)g(x)$. □

(3) Uniqueness of a splitting field, $f(x) \in F[x]$ nonconstant. K/F and K'/F are splitting fields over F, then there exists an isomorphism (in fields) $\psi : K \to K'$, $\psi|_F = \mathrm{id}_F$.

$$\begin{array}{ccc} K & \overset{\psi}{\cong} & K' \\ | & & | \\ F & \overset{\phi}{\cong} & F' \end{array}$$

(a) There exists isomorphism $\psi : K \to K'$ and $\psi|_F = \phi$,
(b) $[K : F] = [K' : F']$,
(c) The number of such extensions is at most $[K : F]$.

Application:

$$\begin{array}{ccc} K_1 & \overset{\psi}{\overset{\cong}{\dashrightarrow}} & K_2 \\ | & & | \\ F & \xrightarrow{\text{id}} & F \end{array}$$

Conclusions:

(1) Two splitting fields of the same polynomial are isomorphic,
(2) The number of those
$$\psi = \#\{\psi : K_1 \to K_2 \mid \psi|_F = \mathrm{id}_F\},$$
(3)
$$\mathrm{Aut}(K/F) := \{\gamma : K \overset{\cong}{\to} K, \gamma|_F = \mathrm{id}_F\}$$
is a group under the composition,
$$\gamma_1 \cdot \gamma_2 : K \overset{\gamma_2}{\underset{\cong}{\to}} K \overset{\gamma_1}{\underset{\cong}{\to}} K, \qquad \gamma_1 \circ \gamma_2|_F = \mathrm{id}_F\,.$$
(4) $\left|\mathrm{Aut}(K/F)\right| \leqslant [K : F] \leqslant n!$, $n = \deg f(x)$ provided that K is a finite field extension of F.

5.3. **Separable Extensions.**

Definition 5.27. $f(x) \in F[x]$ is called *separable* if $f(x)$ has no multiple roots in the splitting field of f over F.

Examples 5.28.

(1) $x^2 - 3x + 2 = (x-1)(x-2) \in \mathbb{Q}[x]$, separable,
(2) x^2 inseparable over $\mathbb{Q}$,
(3) $(x^2-2)^2$ inseparable over $\mathbb{Q}$,
(4) $x^2 - 1 = (x-1)(x+1)$ over $\mathbb{F}_2[x]$.

Remark 5.29. An irreducible polynomial $f(x) \in F[x]$ is separable if and only if $D(f) \in F[x]$ is not 0, where $D(\cdot)$ is the *formal* derivative operator.

Proof. $\boxed{\Rightarrow}$ Let $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_i)$, then
$$f'(x) = a_n \sum_k \prod_{i \neq k}(x - \alpha_i)$$
in $K \supset F$, and $(f(x), f'(x)) = 1$ ($f'(x) \in F$). $f'(x) \not\equiv 0$.
$\boxed{\Leftarrow}$ [✓] □

Definition 5.30. A finite field extension K/F is called a Galois extension if $\left|\mathrm{Aut}(K/F)\right| = [K : F]$.

Proposition 5.31. *Let K/F be a field extension, $\alpha \in K$ algebraic over F, m_α irreducible polynomial and $m_\alpha(\alpha) = 0$, $m_\alpha = a_0 + a_1 x + \cdots + a_n x^n$.*

For all $\phi \in \mathrm{Aut}(K/F), \phi : K \to K$, *and* $\phi|_F = \mathrm{id}_F$. *We get*

$$\begin{aligned} m_\alpha(\phi(\alpha)) &= a_0 + a_1\phi(\alpha) + \cdots + a_n(\phi(\alpha))^n \\ &= \phi(a_0) + \phi(a_1)\phi(\alpha) + \cdots + \phi(a_n)\phi(\alpha^n) \\ &= \phi(a_0 + a_1\alpha + \cdots + a_n\alpha^n) \\ &= \phi(0) = 0 \end{aligned}$$

Then $\phi(\alpha)$ *is a root of* $m_\alpha(x) \in F[x]$.

Every $\phi \in \mathrm{Aut}(K/F)$ permutes the roots of the irreducible polynomials.

Examples 5.32. Find all the elements of $\mathrm{Aut}(K/F)$.

(1) $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$, $\sqrt{2}$ is a root of x^2-2 irreucible over $\mathbb{Q}$. $\phi \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}), \phi : \sqrt{2} : \sqrt{2}, -\sqrt{2}$, so $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$. $\left|\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})\right| \leqslant [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. So $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is a Galois extension.

(2) $G = \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, $\sqrt[3]{2}$ is a root of $x^3 - 2$ which is irreducible over $\mathbb{Q}$.

$$x^3 - 2 = (x - \sqrt[3]{2})\underbrace{(x - \alpha_2)}_{\in \mathbb{C}\setminus\mathbb{R}}\underbrace{(x - \alpha_3)}_{\in \mathbb{C}\setminus\mathbb{R}}$$

$\phi \in G, \phi : \sqrt[3]{2} \to$ either $\sqrt[3]{2}, \underbrace{\alpha_2, \alpha_3}_{\notin \mathbb{Q}(\sqrt[3]{2})}, \phi : \sqrt[3]{2} \mapsto \sqrt[3]{2}$. Then $G = \{\mathrm{id}\}$, and $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a Galois extension.

Theorem 5.33.

(1) If K/F, *a splitting field of separable polynomial* $f(x)$, *then* K/F *is a Galois extension.*

(2) (Fundamental Theorem of Galois Theory) If K/F *is a Galois extension, if* K *is an extension of* E *which is an extension of* F, *then there exists a bijection between the set of fields which satisfy the properties of the field* E *and the subgroups of* $\mathrm{Aut}(K/F)$.

Proof. [✓] □

Example 5.34. $f(x) = (x^2-2)(x^2-3)$ over $\mathbb{Q}$. $K = \mathbb{Q}(\pm\sqrt{2}, \pm\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. $K/\mathbb{Q}$ is a splitting field of separable polynomials so $K/\mathbb{Q}$ is a Galois extension. Note $[K : \mathbb{Q}] = 4$. $G = \mathrm{Aut}(K/\mathbb{Q})$ is a group of 4 elements,

$$\underbrace{\mathrm{id} : \begin{smallmatrix}\sqrt{2}\to\sqrt{2}\\ \sqrt{3}\to\sqrt{3}\end{smallmatrix}}_{K} \quad \underbrace{\sigma : \begin{smallmatrix}\sqrt{2}\to-\sqrt{2}\\ \sqrt{3}\to\sqrt{3}\end{smallmatrix}}_{\mathbb{Q}(\sqrt{3})=E} \quad \underbrace{\tau : \begin{smallmatrix}\sqrt{2}\to\sqrt{2}\\ \sqrt{3}\to-\sqrt{3}\end{smallmatrix}}_{\mathbb{Q}(\sqrt{2})} \quad \sigma\tau : \begin{smallmatrix}\sqrt{2}\to-\sqrt{2}\\ \sqrt{3}\to-\sqrt{3}\end{smallmatrix}$$

5.4. **Worked Problems.**

Problem 5.35. Determine the Galois group of $(x^2-2)(x^2-3)(x^2-5)$. Determine all the subfields of the splitting field of this polynomial.

Proof. This proof comes from `here`.

$K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ is the splitting field of the polynomial $f(x) = (x^2-2)(x^2-3)(x^2-5)$ over $\mathbb{Q}$. Moreover $\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}$ is a $\mathbb{Q}$-basis for K and thus $[K : \mathbb{Q}] = 8$. So if $G = \mathrm{Gal}(K/\mathbb{Q})$ then $|G| = 8$.

Consider the following automorphisms (of order 2 in G)

$$\sigma_2 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{cases} \quad \sigma_3 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{cases} \quad \sigma_5 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto -\sqrt{5} \end{cases}$$

then

$$G = \langle \sigma_2, \sigma_3, \sigma_5 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Note that G is abelian, which means that all its subgroups are normal. By the Fundamental theorem of Galois theory, every normal subgroup $H \leqslant G$ corresponds to a subfield K^H, which is a splitting field over $\mathbb{Q}$. Since $|H|$ divides 8, we distinguish 4 cases:

(1) $|H| = 1$, then clearly $K^H = K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

(2) $|H| = 2$, then H contains the identity and an element of order 2, so it can be any of the following 7 groups:

$$\{1, \sigma_2\}, \{1, \sigma_3\}, \{1, \sigma_5\}, \{1, \sigma_2\sigma_3\}, \{1, \sigma_3\sigma_5\}, \{1, \sigma_5\sigma_2\}, \{1, \sigma_2\sigma_3\sigma_5\}.$$

By looking at the action on the basis elements we find that the corresponding fixed subfields of the above group are:

$$\mathbb{Q}(\sqrt{3}, \sqrt{5}), \mathbb{Q}(\sqrt{2}, \sqrt{5}), \mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{5}, \sqrt{6}), \mathbb{Q}(\sqrt{2}, \sqrt{15}), \mathbb{Q}(\sqrt{3}, \sqrt{10}), \mathbb{Q}(\sqrt{6}, \sqrt{10}).$$

(3) $|H| = 4$, then H contains the identity, two distinct elements of order 2, and their product so it can be any of the following 7 groups:

(a) $\{1, \sigma_2, \sigma_3, \sigma_2\sigma_3\}$,
(b) $\{1, \sigma_3, \sigma_5, \sigma_3\sigma_5\}$,
(c) $\{1, \sigma_5, \sigma_2, \sigma_5\sigma_2\}$,
(d) $\{1, \sigma_2, \sigma_3\sigma_5, \sigma_2\sigma_3\sigma_5\}$,
(e) $\{1, \sigma_3, \sigma_2\sigma_5, \sigma_2\sigma_3\sigma_5\}$,
(f) $\{1, \sigma_5, \sigma_2\sigma_3, \sigma_2\sigma_3\sigma_5\}$,
(g) $\{1, \sigma_2\sigma_3, \sigma_3\sigma_5, \sigma_5\sigma_2\}$.

Their corresponding fixed subfields are:

$$\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{15}), \mathbb{Q}(\sqrt{10}), \mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{30}).$$

(4) $|H| = 8$, then $K^H = \mathbb{Q}$.

□

References

[1] G. Tran, 'Algebraic Structures I', The University of Texas at Austin, 2016.
[2] I. Herstein, Topics in Algebra. New York: Blaisdell Pub. Co., 1964.
[3] D. Dummit and R. Foote, Abstract algebra. Hoboken, NJ: Wiley, 2004.