Abstract Algebra

Personal notes on Contemporary Abstract Algebra

Himanshu Dongre

Based on the textbook by Joseph A. Gallian

These are personal study notes based on Joseph A. Gallian's *Contemporary Abstract Algebra*, tenth edition (CRC Press, 2021). They are not official textbook materials and are not endorsed by the author or publisher. The selection, organization, annotations, and any errors are my own.

Definitions, theorem statements, and selected arguments follow the textbook, with additional observations and examples. Quotations are attributed where they appear. The chapter's "ft." line highlights mathematicians relevant to its subject; it does not attribute every result in that chapter to them. No blanket publication license is asserted over third-party material.

Contents

1 Groups

ft. Heinrich Martin Weber

Definition. Let G be a set. A *binary operation* on G is a function that assigns each ordered pair of elements of G an element of G. This condition is called *closure*.

Definition. Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab. We say G is a ***group*** under this operation if the following three properties are satsified:

1) *Associativity.* The operation is associative; i.e., $(ab)c = a(bc)$ for all $a, b, c \in G$.
2) *Identity.* There is an element $e \in G$ (called the *identity*) such that $ae = ea = a$ for all $a \in G$.
3) *Inverses.* For each element $a \in G$, there is an element $b \in G$ (called the *inverse* of a) such that $ab = ba = e$.

If a group has the property that $\forall a, b \in G,\ ab = ba$, we say the group is *Abelian*.

Theorem. In a group G, there is only one identity element.

Theorem. In a group G, the right and left cancellation laws hold; i.e., $ba = ca \implies b = c$, and $ab = ac \implies b = c$.

Theorem. For each element a in a group G, there is a unique element $b \in G$ such that $ab = ba = e$.

Owing to the uniqueness of the group identity and the inverse of an element, we may unambiguously speak of "the identity" of a group, and denote it by 'e', as well as "the inverse" of an element g, and denote it by g^{-1}. When n is a positive integer, the associative law allows us to use g^n to denote the unambiguous product $\underbrace{gg\ldots g}_{n \text{ factors}}$. We define $g^0 = e$. When $n < 0$, we define $g^n = (g^{-1})^{|n|}$. In an abstract group we do not permit noninteger exponents.

Theorem. *Socks-shoes property.* For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$.

⋆ The notation becomes different but analogous for additive groups.

" 'For example' is not proof."

Jewish Proverb

2 Finite Groups; Subgroups

ft. Philip Hall

Definition. The number of elements of a group (finite or infinite) is called its *order*. We use $|G|$ to denote the order of G.

Definition. Let G be a group and $g \in G$ be an element of G. The *order of g in G* is the smallest positive integer n such that $g^n = e$. If no such integer exists, we say that g has *infinite order* in G. The order of an element g is denoted by $|g|$.

Definition. If a subset H of a group G is itself a group under the operation of G, we say that H is a *subgroup* of G. We denote this by $H \leq G$.

If we want to indicate that H is a subgroup of G but is not equal to G itself, we write $H < G$. Such a subgroup is called a *proper subgroup*. The subgroup $\{e\}$ is called the *trivial subgroup*; a subgroup that is not $\{e\}$ is called a *nontrivial subgroup*.

2.1 Subgroup Tests

Theorem. *One-step Subgroup test.* Let g be a group and let H be a nonempty subset of G. If $ab^{-1} \in H$ whenever $a, b \in H$, then $H \leq G$.

Theorem. *Two-step Subgroup test.* Let G be a group and let H be a nonempty subset of G. If $ab \in H$ whenever $a, b \in H$ (H is closed under the operation), and $a^{-1} \in H$ whenever $a \in H$ (H is closed under taking inverses), then $H \leq G$.

Theorem. *Finite Subgroup test.* Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then $H \leq G$.

How do you prove that the subset of a group is *not* a subgroup? Here are three possible ways, any one of which guarantees that the subset is not a subgroup:

1. Show that the identity is not in the set.
2. Exhibit an element of the set whose inverse is not in the set.
3. Exhibit two elements of the set whose product is not in the set.

2.2 Examples of Subgroups

Notation. For any element a from a group, we let $\langle a \rangle$ denote the set $\{a^n : n \in \mathbb{Z}\}$.

Theorem. Let G be a group, and let a be any element of G. Then, $\langle a \rangle \leq G$.

$\star$ The subgroup $\langle a \rangle$ is called the *cyclic subgroup of G generated by a*. In the case that $G = \langle a \rangle$, we say that G is *cyclic* and a is a *generator of G*. More on this in section 3.

$\star$ For any element a of a group G, it is useful to think of $\langle a \rangle$ as the smallest subgroup of G containing a. This notion can be extended to any collection S of elements from a group G by defining $\langle S \rangle$ as the subgroup of G with the property that $\langle S \rangle$ contains S and if H is any subgroup of G containing S, then H also contains $\langle S \rangle$. Thus, $\langle S \rangle$ is the smallest subgroup of G that contains S. The set $\langle S \rangle$ is called the *subgroup generated by S*.

Definition. The *center*, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G. In symbols,

$$Z(G) = \{a \in G : ax = xa \ \forall x \in G\}.$$

Theorem. $Z(G) \leq G$.

Definition. Let a be a fixed element of a group G. The *centralizer of a in G*, $C(a)$, is the set of all elements in G that commute with a. In symbols,

$$C(a) = \{g \in G : ga = ag\}.$$

Theorem. $\forall a \in G,\ C(a) \leq G$.

$\star$ $\forall a \in G,\ Z(G) \subseteq C(a)$. In fact, $Z(G) = \bigcap_{a \in G} C(a)$. Also, G is Abelian if and only if $C(a) = G$ for all $a \in G$.

> "The purpose of proof is to understand, not to verify."
>
> — Arnold Ross

3 Cyclic Groups

ft. Leonhard Euler

Definition. A group G is called *cyclic* if there is an element $a \in G$ such that $G = \{a^n : n \in \mathbb{Z}\}$. Such an element a is called a *generator* of G. G is denoted by $\langle a \rangle$.

3.1 Properties of Cyclic Groups

Theorem. Let G be a group, and let $a \in G$ be an element. If a has infinite order, then $a^i = a^j \iff i = j$. If a has finite order, say, n, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j \iff n \mid i - j$.

Corollary. For any group element a, $|a| = |\langle a \rangle|$.

Corollary. For any group element a, $a^k = e \iff |a| \mid k$; i.e., $a^k = e$ iff k is a multiple of $|a|$.

Corollary. If a and b belong to a finite group and $ab = ba$, then $|ab|$ divides $|a||b|$.

Theorem. Let a be an element of order n in a group and let k be a positive integer. Then $\left\langle a^k \right\rangle = \left\langle a^{\gcd(n,k)} \right\rangle$ and $\left|a^k\right| = \frac{n}{\gcd(n,k)}$.

Corollary. In a finite cyclic group, the order of an element divides the order of the group.

Corollary. Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle \iff \gcd(n, i) = \gcd(n, j)$, and $|a^i| = |a^j| \iff \gcd(n, i) = \gcd(n, j)$.

Corollary. Let $|a| = n$. Then $\langle a \rangle = \langle a^j \rangle \iff \gcd(n, j) = 1$, and $|a| = |\langle a^j \rangle| \iff \gcd(n, j) = 1$.

Corollary. An integer $k \in \mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if $\gcd(n, k) = 1$.

3.2 Classification of Subgroups of Cyclic Groups

Theorem. *Fundamental thm of Cyclic Groups.* Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k—viz. $\left\langle a^{\frac{n}{k}}\right\rangle$.

Corollary. For each positive divisor k of n, the set $\left\langle \frac{n}{k}\right\rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k; moreover, these are the only subgroups of $\mathbb{Z}_n$.

Notation. Let φ denote Euler's totient function.

Theorem. If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\varphi(d)$.

Corollary. In a finite group, the number of elements of order d is a multiple of $\varphi(d)$.

The relationships among the various subgroups of a group can be illustrated with a *subgroup lattice* of the group. This is a diagram that includes all subgroups of the group and connects a subgroup H at one level to a subgroup K at a higher level with a sequence of line segments if and only if $H < K$. Although there are many ways to draw such a diagram, the connections between subgroups must be the same.

> "It is not unreasonable to use the hypothesis."
>
> — Arnold Ross

4 Permutation Groups

ft. Augustin Louis Cauchy

Definition. A *permutation* of a set A is a bijective function from A to A. A *permutation group* of a set A is a set of permutations of A that forms a group under the operation of function composition.

Although groups of permutations of any nonempty set A of objects exist, we will focus on the case where A is finite. Furthermore, it is customary, as well as convenient to take A to be a set of the form $\{1, 2, 3, \ldots, n\}$ for some positive integer n. Permutations of finite sets can be given by an explicit listing of each element of the domain and its corresponding functional value.

Definition. Let $A = \{1, 2, \ldots, n\}$. The set of all permutations of A is called the *symmetric group of degree* n and is denoted by S_n. Elements of S_n have the form

$$\alpha = \begin{bmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{bmatrix}.$$

The identity of the group is the identity permutation $\varepsilon = \begin{bmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{bmatrix}$.

$\star$ $|\mathsf{S}_n| = n!$.

4.1 Cycle Notation

Definition. An expression of the form $(a_1, a_2, \ldots, a_m)$ (when the domain consists of single-digit integers, it is common practice to omit the commas between the digits) is called a *cycle of length* m or an m-cycle. A multiplication of cycles can be introduced by thinking of a cycle as a permutation that fixes any symbol not appearing in the cycle. Cycles with single elements are generally omitted from the product in the notation.

Definition. When the various cycles in the cycle notation of a permutation have no numbers in common, then they are *disjoint*, and the representation is called *disjoint cycle* form.

4.2 Properties of Permutations

Theorem. Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Theorem. If the pair of cycles $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$; i.e., disjoint cycles commute.

Theorem. *Ruffini, 1799.* The order of a permutation of a finite set written in disjoint cycle form is the LCM of the lengths of the cycles.

Theorem. Every permutation in S_n, $n > 1$, is a product of 2-cycles.

Lemma. If $\varepsilon = \beta_1\beta_2 \ldots \beta_r$, where the βs are 2-cycles, then r is even.

Theorem. If a permutation α can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even (odd) number of 2-cycles.

Definition. A permutation that can be expressed as a product of an even number of 2-cycles is called an *even* permutation. A permutation that can be expressed as a product of an odd number of 2-cycles is called an *odd* permutation.

Theorem. The set of even permutations in S_n forms a subgroup of S_n.

Definition. The group of even permutations of n symbols is denoted by A_n and is called the *alternating group of degree* n.

Theorem. For $n > 1$, $|\mathsf{A}_n| = \frac{n!}{2}$.

> "My mind rebels at stagnation. Give me problems, give me work, give me the most abstruse cryptogram, or the most intricate analysis, and I am in my own proper atmosphere."
>
> — Sherlock Holmes, *The Sign of Four*

5 Isomorphism

ft. Arthur Cayley

Definition. An *isomorphism* ϕ from a group G to a group G' is a bijective mapping (or function) from G to G' that preserves the group operation; i.e., $\forall a, b \in G,\ \phi(ab) = \phi(a)\phi(b)$. If there is an isomorphism from G onto G', we say that G and G' are *isomorphic* and write $G \cong G'$.

$\star$ It is implicit in the definition of isomorphism that the operation on the LHS is that of G, whereas the operation on the RHS is that of G'.

There are four separate steps involved in proving that a group G is isomorphic to a group G':

1. *Mapping:* Define a candidate function ϕ for the isomorphism.
2. *Injective.* Prove that ϕ is 1-1.
3. *Surjective.* Prove that ϕ is onto.
4. *Operation-preserving.* Prove that $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

5.1 Properties of Isomorphisms

Theorem. Suppose that ϕ is an isomorphism from a group G onto a group G'. Then,

1) $\phi(e) = e'$.
2) $\forall n \in \mathbb{Z}\ \forall a \in G,\ \phi(a^n) = [\phi(a)]^n$.
3) $\forall a, b \in G$, a and b commute iff $\phi(a)$ and $\phi(b)$ commute.
4) $G = \langle a \rangle \iff G' = \langle \phi(a) \rangle$.
5) $\forall a \in G,\ |a| = |\phi(a)|$.
6) For a fixed $k \in \mathbb{Z}$ and a fixed $b \in G$, the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in G'.
7) If G is finite, then G and G' have exactly the same number of elements of every order.

Theorem. Suppose ϕ is an isomorphism from a group G onto a group G'. Then,

1) ϕ^{-1} is an isomorphism from G' onto G.
2) G is Abelian iff G' is Abelian.
3) G is cyclic iff G' is cyclic.
4) If $K \leq G$ is a subgroup, then $\phi(K) = \{\phi(k) : k \in K\} \leq G'$.
5) If $K' \leq G'$ is a subgroup, then $\phi^{-1}(K') = \{g \in G : \phi(g) \in K'\} \leq G$.
6) $\phi(Z(G)) = Z(G')$.

$\star$ Isomorphic groups have *all* group theoretic properties in common.

5.2 Automorphisms

Definition. An isomorphism from a group G onto itself is called an *automorphism*.

Notation. The set of all automorphisms of G is denoted by $\mathsf{Aut}(G)$.

Definition. Let G be a group, and $a \in G$ be an element. The function $\phi_a : G \to G,\ g \mapsto aga^{-1}$ is called the *inner automorphism of G induced by a*.

Notation. The set of all inner sutomorphisms of G is denoted by $\mathsf{Inn}(G)$.

Theorem. $\mathsf{Aut}(G)$ and $\mathsf{Inn}(G)$ are both groups under the operation of function composition.

Theorem. $\forall n \in \mathbb{N},\ \mathsf{Aut}(\mathbb{Z}_n) \cong U(n)$.

5.3 Cayley's Theorem

Theorem. *Cayley.* Every group is isomorphic to a group of permutations.

Proof sketch. Let G be a group. Define the permutation T_g on G as $T_g(x) = gx$ for all $x \in G$, where $g \in G$. Define the group $\Gamma = \{T_g : g \in G\}$. Then Γ is a set of permutations on G that is a group under the operation of function composition. The mapping $\phi : G \to \Gamma,\ g \mapsto T_g$ is an isomorphism from G onto Γ.

$\star$ The group of permutations Γ is called the *left regular representation* of G.

5.4 Bonus Results

Theorem. $(\mathbb{R}, +) \cong (\mathbb{C}, +)$.

Theorem. $(\mathbb{C} \setminus \{0\}, \cdot) \cong (\{z \in \mathbb{C} : |z| = 1\}, \cdot)$.

> "Being a mathematician is a bit like being a manic depressive: you spend your life alternating between giddy elation and black despair."
>
> — Steven G. Krantz, *A Primer of Mathematical Writing*

6 Cosets And Lagrange's Theorem

ft. Joseph Louis Lagrange

Definition. Let G be a group and let H be a nonempty subset of G. For any $a \in G$, the set $\{ah : h \in H\}$ is denoted by aH. Analogously, $Ha = \{ha : h \in H\}$, and $aHa^{-1} = \{aha^{-1} : h \in H\}$. When H is a subgroup of G, the set aH is called the *left coset of H in G containing a*, whereas Ha is called the *right coset of H in G containing a*. In this case, the element a is called the *coset representative* of aH (or Ha).

$\star$ Cosets are usually not subgroups

$\star$ aH may be the same as bH, even though a is not the same as b.

Lemma. Let H be a subgroup of G, and let $a, b \in G$ be arbitrary elements. Then,

1) $a \in aH$.
2) $aH = H \iff a \in H$.
3) $(ab)H = a(bH)$ and $H(ab) = (Ha)b$.
4) $aH = bH \iff a \in bH$.
5) $aH = bH$ or $aH \cap bH = \emptyset$.
6) $aH = bH \iff a^{-1}b \in H$.
7) $|aH| = |bH|$.
8) $aH = Ha \iff H = aHa^{-1}$.
9) $aH \leq G \iff a \in H$.

$\star$ Property 5 says that two left cosets of H are either identical or disjoint. Hence, a left coset of H is uniquely determined by any one of its elements.

$\star$ By properties 1, 5, and 7, the left cosets of a subgroup $H \leq G$ partition G into blocks of equal size. Indeed we may view the cosets of H as a partitioning of G into equivalence classes under the equivalence relation defined by $a \sim b$ if $aH = bH$.

6.1 Langrange's Theorem

Theorem. *Lagrange.* If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $\frac{|G|}{|H|}$.

$\star$ Lagrange's theorem is subgroup candidate criterion for finite groups. The converse of Lagrange's theorem is false.

Definition. The *index* of a subgroup H in G is the number of distinct left cosets of H in G. This number is denoted by $|G : H|$.

Corollary. If G is a finite group and H is a subgroup of G, then $|G : H| = \frac{|G|}{|H|}$.

Corollary. In a finite group G, the order of each element of G divides $|G|$.

Corollary. Let G be a finite group, and let $a \in G$ be an element. Then $a^{|G|} = e$.

Corollary. Every group of prime order p is isomorphic to $\mathbb{Z}_p$.

Corollary. *Fermat's Little Theorem.* For every integer a and every prime p, $a^p \equiv a \bmod p$.

6.2 More Theorems

Theorem. For two finite subgroups H and K of a group, define the set $HK = \{hk : h \in H,\ k \in K\}$. Then $|HK| = \frac{|H||K|}{|H \cap K|}$.

Theorem. Let G be a group of order $2p$, where p is an odd prime. Then $G \cong \mathbb{Z}_{2p}$ or $G \cong \mathsf{D}_p$.

Corollary. $\mathsf{S}_3 \cong \mathsf{D}_3$, $\mathsf{GL}(2, \mathbb{Z}_2) \cong \mathsf{D}_3$.

6.2.1 Applications to Permutation Groups

Definition. Let G be a group of permutations of a set S (i.e., $G \leq \mathsf{S}_{|S|}$). For each $i \in S$, let $\mathsf{stab}_G(i) = \{\sigma \in G : \sigma(i) = i\}$. We call stab_G the *stabilizer* of i in G.

$\star$ $\mathsf{stab}_G \leq G$.

Definition. Let G be a group of permutations of a set S (i.e., $G \leq \mathsf{S}_{|S|}$). For each $i \in S$, let $\mathsf{orb}_G(i) = \{\sigma(i) : \sigma \in G\}$. The set $\mathsf{orb}_G(i) \subseteq S$ is called the *orbit of i under G*.

$\star$ The orbits of the elements of a set S under a group partition S.

Theorem. *Orbit-Stabilizer.* Let G be a finite group of permutations of a set S (i.e., $G \leq \mathsf{S}_{|S|}$). Then, $\forall i \in S,\ |G| = |\mathsf{orb}_G(i)||\mathsf{stab}_G(i)|$.

Theorem. The group of rotations of a cube is isomorphic to S_4.

Theorem. The group of rotations of a soccer ball is isomorphic to A_5.

Theorem. Every Rubik's cube configuration can be solved in at most 20 moves.

> "I don't know Marge. Trying is the first step towards failure."
>
> — Homer Simpson, *The Simpsons*

7 External Direct Products

ft. Robert Remak

Definition. Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The *external direct product (EDP)* of $G_1, G_2, \ldots, G_n$, written as $G_1 \times G_2 \times \ldots \times G_n$, is the set of all n-tuples for which the i^{th} component is an element of G_i and the operation is component-wise. In symbols,

$$G_1 \times G_2 \times \ldots \times G_n = \{(g_1, g_2, \ldots, g_n) : g_i \in G_i\},$$

where $(g_1, g_2, \ldots, g_n)(g_1', g_2', \ldots, g_n')$ is defined to be $(g_1 g_1', g_2 g_2', \ldots, g_n g_n')$.

$\star$ $|G_1 \times G_2 \times \ldots \times G_n| = \prod_{i=1}^{n} |G_i|$.

$\star$ The EDP of groups is itself a group.

$\star$ Every group of order 4 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

7.1 Properties of EDPs

Theorem. Let $G_1, G_2, \ldots, G_n$ be finite groups and $\mathcal{G} = G_1 \times G_2 \times \ldots \times G_n$. For an element $(g_1, g_2, \ldots, g_n) \in \mathcal{G}$,

$$|(g_1, g_2, \ldots, g_n)| = \text{lcm}(|g_1|, |g_2|, \ldots, |g_n|)\,.$$

Corollary. If m and n are positive integers that are divisible by a prime p, then the number of elements of order p in $\mathbb{Z}_m \times \mathbb{Z}_n$ is $p^2 - 1$.

Corollary. For each divisor r of m and s of n, the group $\mathbb{Z}_m \times \mathbb{Z}_n$ has a subgroup isomorphic to $\mathbb{Z}_r \times \mathbb{Z}_s$.

Theorem. Let G and H be finite cyclic groups. The $G \times H$ is cyclic if and only if $|G|$ and $|H|$ are coprime.

Corollary. An EDP $G_1 \times G_2 \times \ldots \times G_n$ of a finite number of finite cyclic groups is cyclic if and only if $|G_i|$ and $|G_j|$ are coprime when $i \neq j$.

Corollary. Let $m = n_1 n_2 \ldots n_k$. Then $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ if and only if n_i and n_j are coprime when $i \neq j$.

7.2 U-group as an EDP

Recall that $U(n)$ denotes the *group of units modulo* n; i.e.,

$$U(n) = \{i \in \mathbb{N}_{<n} : i \text{ is coprime to } n\},$$

where the group operation is multiplication modulo n.

Notation. If $k > 1$ is a proper divisor of a positive integer n, let

$$U_k(n) = \{x \in U(n) : n \bmod k = 1\}.$$

$\star$ $U_k(n) \leq U(n)$.

Theorem. Suppose s and t are coprime. Then $U(st) \cong U(s) \times U(t)$. Moreover, $U_s(st) \cong U(t)$ and $U_t(st) \cong U(s)$.

Corollary. Let $m = n_1 n_2 \ldots n_k$, where $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then,

$$U(m) \cong U(n_1) \times U(n_2) \times \ldots \times U(n_k).$$

$\star$ $U(2) \cong \{0\}$, $U(4) \cong \mathbb{Z}_2$, $U(2^n) \cong \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_2$ for $n > 3$.

$\star$ $U(p^n) \cong \mathbb{Z}_{p^n - p^{n-1}}$ for p an odd prime.

> What's the most difficult aspect of your life as a mathematician, Diane Maclagan, an assistant professor at Rutgers, was asked. "Trying to prove theorems." she said. And the most fun? "Trying to prove theorems."

8 Normal Subgroups And Factor Groups

ft. Otto Hölder

Definition. A subgroup H of a group G is called a *normal* subgroup of G if $aH = Ha$ for all $a \in G$. We denote this by $H \triangleleft G$.

Theorem. *Normal Subgroup test.* A subgroup H of G is normal in G if and only if $xHx^{-1} \subseteq H$ for all $x \in G$.

Corollary. if a group G has a unique subgroup H of some finite order, then $H \triangleleft G$.

8.1 Factor Groups

Theorem. *O. Hölder, 1889.* Let H be a normal subgroup of a group G. The set

$$G/H = \{aH : a \in G\}$$

is a group under the operation $(aH)(bH) = abH$.

$\star$ The converse is also true; i.e., if the correspondence $(aH)(bH) = abH$ defines a group operation on the set of left cosets of H in G, then $H \triangleleft G$.

$\star$ If for any $n \in \mathbb{N}$ we let $n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$, then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

It is crucial to understand that when we factor out by a normal subgroup H, what we are essentially doing is defining every element in H to be the identity. Algebraists often refer to the process of creating the factor group G/H as "killing" H.

8.1.1 Applications of Factor Groups

Theorem. *G/Z.* Let G be a group and let $Z(G)$ be the center of G. If $G/Z(G)$ is cyclic, then G is Abelian.

$\star$ A better result is possible: If G/H is cyclic, where $H \leq Z(G)$, then G is Abelian.

$\star$ The contrapositive of the statement is useful enough to be stated separately: If G is non-Abelian, then $G/Z(G)$ is not cyclic.

Corollary. A non-Abelian group of order pq, where p and q are primes, must have a trivial center.

Corollary. If $G/Z(G)$ is cyclic, it must be trivial.

Theorem. For any group G, $G/Z(G) \cong \mathsf{Inn}(G)$.

Theorem. *Cauchy's thm for Abelian Groups.* Let G be a finite Abelian group and let p be a prime such that $p \mid |G|$. Then G has an element of order p.

8.2 Internal Direct Products

Definition. We say that G is the *internal direct product (IDP)* of H and K, and write $G = H \cdot K$, if all four of the following conditions are satisfied:

1) $H \triangleleft G$,

2) $K \triangleleft G$,

3) $H \cap K = \{e\}$, and

4) $G = HK$.

$\star$ If s and t are coprime positive integers, then $U(st) = U_s(st) \cdot U_t(st)$.

Definition. Let $H_1, H_2, \ldots, H_n$ be a finite collection of normal subgroups of G. We say that G is the *internal direct product (IDP)* of $H_1, H_2, \ldots, H_n$, and write $G = H_1 \cdot H_2 \cdot \ldots \cdot H_n$, if

1) $G = H_1 H_2 \ldots H_n = \{h_1 h_2 \ldots h_n : h_i \in H_i\}$, and

2) $(H_1 H_2 \ldots H_i) \cap H_{i+1} = \{e\}$ for $i = 1, 2, \ldots, n-1$.

Theorem. If a group G is the IDP of a finite number of subgroups $H_1, H_2, \ldots, H_n$, then G is isomorphic to the EDP of $H_1, H_2, \ldots, H_n$.

8.3 Classification Theorems

A couple of classification theorems can be proved using the previous theorem. Before stating those, recall the classification theorems we have stated thus far:

1) Classification of subgroups of finite cyclic groups: There is exactly one subgroup for each divisor of the order of the group and no others.

2) Classification of groups of prime order: Every group of prime order p is isomorphic to $\mathbb{Z}_p$.

3) Classification of groups of $2p$ where p is an odd prime: Every group of order $2p$, where p is an odd prime, is isomorphic to $\mathbb{Z}_{2p}$ or D_p.

4) Classification of groups of order 4: Every group of order 4 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Theorem. *Classification of Finite Abelian Groups of Squre-free Order.* Every Abelian group of order $p_1 p_2 \ldots p_k$ where the p_i are distinct primes is cyclic.

Theorem. *Classification of Groups of Order p^2.* Every group of order p^2, where p is a prime, is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Corollary. If G is a group of order p^2, where p is a prime, then G is Abelian.

> "The heart of mathematics is its problems."
>
> — Paul Halmos

9 Group Homomorphisms

ft. Camille Jordan

Definition. A *homomorphism* ϕ from a group G to a group G' is a mapping from G to G' that preserves the group operation; i.e., $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

Definition. The *kernel* of a homomorphism ϕ from a group G to a group with identity e' is the set $\{x \in G : \phi(x) = e'\}$. The kernel of ϕ is denoted by $\ker \phi$.

$\star$ Any isomorphism is a homomorphism that is also onto and 1-1. The kernel of an isomorphism is the trivial subgroup $\{e\}$.

When defining a homomorphism from a group in which there are several ways to represent the elements, caution must be exercised to ensure that the correspondence is a function. The term *well-defined* is often used in this context.

9.1 Properties of Homomorphisms

Theorem. Let ϕ be a homomorphism from a group G to a group G', and let $g \in G$ be an element. Then,

1) ϕ carries the identity of G to the identity of G'.
2) $\phi(g^n) = (\phi(g))^n$ for all $n \in \mathbb{Z}$.
3) If $|g|$ is finite then $|\phi(g)|$ divides $|g|$, and if $|G|$ is finite then $|\phi(g)|$ divides $|g|$ and $|\phi(G)|$.
4) $\ker \phi \leq G$.
5) $\phi(a) = \phi(b) \iff a \ker \phi = b \ker \phi$.
6) If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G : \phi(x) = g'\} = g \ker \phi$.

Theorem. Let ϕ be a homomorphism from a group G to a group G', and let H be a subgroup of G. Then,

1) $\phi(H) = \{\phi(h) : h \in H\} \leq G'$.
2) If H is cyclic, then $\phi(H)$ is cyclic.
3) If H is Abelian, then $\phi(H)$ is Abelian.
4) $H \triangleleft G \implies \phi(H) \triangleleft \phi(G)$. In particular, if ϕ is onto, then $\phi(H) \triangleleft G'$.
5) If $|\ker \phi| = n$, then ϕ an n-1 mapping from G onto $\phi(G)$.
6) If $|H|$ is finite, then $|\phi(H)|$ divides $|H|$.
7) $\phi(Z(G)) \leq Z(\phi(G))$.
8) If $K' \leq G'$, then $\phi^{-1}(K') = \{k \in G : \phi(k) \in K'\} \leq G$.
9) If $K' \triangleleft G'$, then $\phi^{-1}(K') = \{k \in G : \phi(k) \in K'\} \triangleleft G$.
10) If ϕ is surjective and $\ker \phi$ is the trivial subgroup, then ϕ is an isomorphism from G onto G'.

$\star$ The set $\phi^{-1}(K')$ defined in property 8 in the previous theorem is called the *inverse image* of K' (or the *pullback* of K').

Corollary. Let ϕ be a group homomorphism from G to G'. Then $\ker\phi \triangleleft G$.

9.2 Fundamental Theorem of Group Homomorphisms

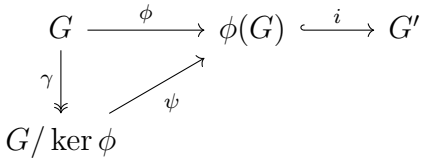
The group homomorphisms, like factor groups, cause a *systematic collapse* of a group to a simpler but closely related group (visualized as dividing the Cayley table into boxes). This can be likened to viewing a group through the reverse end of a telescope—the general features of the group are present, but the apparent size is diminished.

Theorem. *First Isomorphism thm (Jordan, 1870).* Let ϕ be a group homomorphism from G to G'. Then the mapping from $G/\ker\phi$ to $\phi(G)$ given by $g\ker\phi \mapsto \phi(g)$ is an isomorphism. Hence, $G/\ker\phi \cong \phi(G)$.

Corollary. If ϕ is a homomorphism from a finite group G to G', then $\frac{|G|}{|\ker\phi|} = |\phi(G)|$.

Corollary. If ϕ is a homomorphism from a finite group G to G', then $|\phi(G)|$ divides $|G|$ and $|G'|$.

Define the mapping $\gamma : G \to G/\ker\phi$ by $g \mapsto g\ker\phi$. The mapping γ is called the *natural mapping* from G to $G/\ker\phi$. Let ψ be the isomorphism from $G/\ker\phi$ onto $\phi(G)$ defined in the theorem statement. Then, the first isomorphism theorem is often pictorially represented as a *commutative diagram* (where i is the natural inclusion). The diagram is so-called because every path with the same start and end points in the diagram gives the same result when the arrows are composed.



Definition. Let H be a subgroup of a group G. The set $N(H) = \{g \in G : gHg^{-1} = H\}$ is called the *normalizer* of H in G.

Definition. Let H be a subgroup of a group G. The set $C(H) = \{g \in G : ghg^{-1} = h \ \forall h \in H\}$ is called the *centralizer* of H in G.

$\star$ $H \leq G \implies N(H) \leq G$ and $C(H) \leq G$.

Theorem. *N/C.* Let H be a subgroup of a group G. Consider the mapping $\nu : N(H) \to \mathsf{Aut}(H)$ given by $g \mapsto \phi_g$, where ϕ_g is the inner automorphism of H induced by g (i.e., $\phi_g(h) = ghg^{-1}$ for all $h \in H$). This mapping is a homomorphism with kernel $C(H)$. So, by the FIT, $N(H)/C(H) \cong \nu(N(H)) \leq \mathsf{Aut}(H)$.

Theorem. Every normal subgroup of a group G is the kernel of a homomorphism of G. In particular, a normal subgroup N is the kernel of the *projection* mapping $\pi : G \to G/N$ given by $g \mapsto gN$.

In certain branches of group theory, and especially in physics and chemistry, one often wants to know all homomorphic images of a group that are matrix groups over the complex numbers (these are called *group representations*). Several homomorphic images of a group reveal much about the group.

> "The greater the difficulty, the more the glory in surmounting it. Skillful pilots gain their reputation from storms and tempests."
>
> — Epicurus

10 Fundamental Theorem Of Finite Abelian Groups

ft. Georg Frobenius, Ludwig Stickelberger

Theorem. *Fundamental thm of Finite Abelian Groups.* Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

Since a cyclic group of order n is isomorphic to $\mathbb{Z}_n$, the FTFAG shows that every finite Abelian group G is isomorphic to a group of the form

$$\mathbb{Z}_{{p_1}^{n_1}} \times \mathbb{Z}_{{p_2}^{n_2}} \times \ldots \times \mathbb{Z}_{{p_k}^{n_k}} ,$$

where the p_is are not necessarily distinct primes and the prime powers $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$ are uniquely determined by G. Writing a group in this form is called *determining the isomorphism class of* G.

10.1 Isomorphism Classes of Abelian Groups

Definition. Let k be a positive integer. A set of positive integers whose sum is k is called a *partition* of k.

$\star$ If a positive integer k has a partition $\{n_1, n_2, \ldots, n_t\}$, then

$$\mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \ldots \times \mathbb{Z}_{p^{n_t}}$$

is an Abelian group of order p^k. Furthermore, the uniqueness portion of the FTFAG guarantees that distinct partitions of k yield distinct isomorphism classes.

$\star$ If A is a finite group, then $A \times B \cong A \times C \iff B \cong C$.

Now that we know how to construct all the Abelian groups of prime-power order, we move to the problem of constructing all Abelian groups of a certain order n, where n has two or more distinct prime divisors:

1. Write n in its canonical form $n = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$.
2. Individually form all Abelian groups of order $p_i^{n_i}$ for all $1 \leq i \leq k$.

3. Form all possible EDPs of these groups. These are the isomorphism classes.

If we are given an Abelian group G of order n, the question we want to answer about G is: Which of the preceding isomorphism classes represents the structure of G? We can answer this question by comparing the orders of the elements of G with the orders of the elements in the different EDPs, since it can be shown that two Abelian groups are isomorphic iff they have the same number of elements of each order. In practice, a combination of theory and calculation of the orders of a few elements will usually suffice.

Corollary. If m divides the order of a finite Abelian group G, then G has a subgroup of order m.

This corollary of the FTFAG shows that the converse of Lagrange's theorem is true for finite Abelian groups.

10.2 Proof Sketch of the FTFAG

Lemma 1. Let G be a finite Abelian group of order $p^n m$, where p is a prime that does not divide m. Then, $G = H \cdot K$, where $H = \left\{x \in G : x^{p^n} = e\right\}$ and $K = \{x \in G : x^m = e\}$. Moreover, $|H| = p^n$.

Given a finite Abelian group G with $|G| = \prod_{i=1}^{k} p_i^{n_i}$, where the p_is are distinct primes, we let $G(p_i)$ denote the set $\left\{x \in G : x^{p_i^{n_i}} = e\right\}$. It then follows immediately from lemma 1 and induction that $G = G(p_1) \cdot G(p_2) \cdot \ldots \cdot G(p_k)$ and $|G(p_i)| = p_i^{n_i}$.

Lemma 2. Let G be an Abelian group of prime-power order and let $a \in G$ be an element of maximum order. Then, G can be written in the form $\langle a \rangle \cdot K$ for some $K \leq G$.

This lemma and induction on the order of the group give the following.

Lemma 3. A finite Abelian group of prime-power order is an IDP of cyclic groups.

Thus, we have sketched that G is an IDP of cyclic groups of prime-power order. All that remains is to prove the uniqueness of these factors.

Lemma 4. Suppose G is a finite Abelian group of prime-power order. If

$$G = H_1 \cdot H_2 \cdot \ldots \cdot H_m = K_1 \cdot K_2 \cdot \ldots \cdot K_n \,,$$

where the Hs and Ks are nontrivial cyclic subgroups with $|H_1| \geq |H_2| \geq \ldots \geq |H_m|$ and $|K_1| \geq |K_2| \geq \ldots \geq |K_n|$, then $m = n$ and $|H_i| = |K_i|$ for all i.

> "One problem after another presents itself and in the solving of them we can find our greatest pleasure."
>
> — Karl Menninger

11 Introduction To Rings

ft. David Hilbert

Definition. A ***ring*** R is a set with *two* binary operations, addition (denoted by $a+b$) and multiplication (denoted by ab), such that $\forall a, b, c \in R$:

1) $a+b=b+a$.
2) $(a+b)+c=a+(b+c)$
3) There is an additive identity 0; i.e., there is an element $0 \in R$ such that $a+0=a$ for all $a \in R$.
4) $\forall a \in R$, there is an element $-a \in R$ such that $a+(-a)=0$.
5) $a(bc)=(ab)c$.
6) $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$.

A ring is an Abelian group under addition, also having an associative multiplication that is left and right distributive over addition.

$\star$ Note that multiplication need not be commutative. When it is, we say that the ring is *commutative*.

$\star$ A ring need not have an identity under multiplication. A *unity* (or *identity*) in a ring is a non-additive-identity (*nonzero*) element that is an identity under multiplication.

$\star$ A nonzero element of a commutative ring with unity need not have a multiplicative inverse. When it does, we say that it is a *unit* of the ring. Thus $a \in R$ is a unit if a^{-1} exists.

$\star$ If a and b belong to a commutative ring R and a is nonzero, we say that a *divides* b (or that a is a *factor* of b) and write $a \mid b$, if there exists an element $c \in R$ such that $b=ac$. If a does not divide b, we write $a \nmid b$.

Notation. If an element a of a ring is summed n times, the sum can be written as a multiplication of the integer n and the ring element a. To not confuse this with ring multiplication, we will write $n \odot a$ to mean $\underbrace{a+a+\ldots+a}_{n \text{ times}}$.

$\star$ Let $R_1, R_2, \ldots, R_n$ be rings. We can use these to construct a new ring as follows. Let

$$R_1 \oplus R_2 \oplus \ldots \oplus R_n = \{(a_1, a_2, \ldots, a_n) : a_i \in R_i\}$$

and perform componentwise addition and multiplication. This ring is called the *direct sum* of $R_1, R_2, \ldots, R_n$.

11.1 Properties of Rings

Theorem. Let a, b, and c belong to a ring R. Then

1) $a0=0a=0$.
2) $a(-b)=(-a)b=-(ab)$.
3) $(-a)(-b)=ab$.

4) $a(b-c) = ab - ac$ and $(b-c)a = ba - bc$.

Furthermore, if R has a unity element 1, then

5) $(-1)a = -a$.

6) $(-1)(-1) = 1$.

Theorem. If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.

⋆ A ring need not have multiplicative cancellation because it need neither have a multiplicative identity nor multiplicative inverses for elements.

11.2 Subrings

Definition. A subset S of a ring R is a *subring* of R if S is itself a ring with the operations of R.

Theorem. *Subring test.* A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication; i.e., if $a - b$ and ab are in S whenever a and b are in S.

⋆ $\{0\}$ is called the *trivial* subring of a ring.

We can picture the relationship between a ring and its various subrings by way of a subring lattice diagram. In such a diagram, any ring is a subring of all the rings that it is connected to by one or more upward lines.

> "There is no substitute for hard work."
>
> — Thomas Alva Edison, *Life*

12 Integral Domains

ft. Richard Dedekind

Definition. A *zero-divisor* is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

Definition. An *integral domain* is a commutative ring with unity and no zero-divisors.

⋆ Thus, in an integral domain, a product is 0 only when one of the factors is 0; i.e., $ab = 0 \iff a = 0 \vee b = 0$.

Theorem. *Cancellation.* Let a, b, and c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

12.1 Fields

Definition. A ***field*** is a commutative ring with unity in which every nonzero element is a unit.

⋆ Every field is an integral domain.

⋆ A field can be thought of as simply an algebraic system that is closed under addition, subtraction, multiplication, and division (except by 0).

Theorem. A finite integral domain is a field.

Corollary. The ring of integers modulo n, $\mathbb{Z}_n$, is a field if and only if n is prime.

12.2 Characteristic of a Ring

Definition. The *characteristic* of a ring R is the least positive integer n such that $n \odot x = 0$ for all $x \in R$. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by $\operatorname{char} R$.

Theorem. Let R be a ring with unity 1. If 1 has infinite order under addition, then $\operatorname{char} R = 0$. If 1 has order n under addition, then $\operatorname{char} R = n$.

Theorem. The characteristic of an integral domain is 0 or prime.

> "It looked absolutely impossible. But it so happens that you go on worrying away at a problem in science and it seems to get tired, and lies down and lets you catch it."
>
> — William Lawrence Bragg

13 Ideals And Factor Rings

ft. Emmy Noether

13.1 Ideals

Definition. A subring A of a ring R is called a (two-sided) *ideal* of R if for every $r \in R$ and every $a \in A$, $ra \in A$ and $ar \in A$.

So, a subring A of a ring R is an ideal of R if A "absorbs" elements from R; i.e., if $rA = \{ra : a \in A\} \subseteq A$ and $Ar = \{ar : a \in A\} \subseteq A$ for all $r \in R$.

Theorem. *Ideal test.* A nonempty subset A of a ring R is an ideal of R if

1) $a, b \in A \implies a - b \in A$.

2) ra and ar are in A whenever $a \in A$ and $r \in R$.

⋆ The ideal $\{0\}$ is called the *trivial* ideal.

Definition. Let R be a commutative ring with unity and let $a \in R$ be an element. The set $\langle a \rangle = \{ra : r \in R\}$ is an ideal of R called the *principal ideal generated by* a.

Similarly, we can define an ideal generated by elements $a_1, a_2, \ldots, a_n \in R$ as $\langle a_1, a_2, \ldots, a_n \rangle = \{\sum_{i=1}^{n} r_i a_i : r_i \in R\}$.

Definition. A *prime ideal* A of a ring R is a proper ideal of R such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$.

⋆ Let n be an integer greater than 1. Then, in the ring of integers, the ideal $n\mathbb{Z}$ is prime if and only if n is prime. The trivial ideal is also a prime ideal of $\mathbb{Z}$.

Definition. A *maximal ideal* A of a commutative ring R is a proper ideal of R such that, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

13.2 Factor Rings

Theorem. Let R be a ring and let A be a subring of R. The set of cosets $\{r + A : r \in R\}$ is a ring under the operation $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$ if and only if A is an ideal of R. This ring is called the *factor ring* of R by A, and is denoted by R/A.

Theorem. Let R be a commutative ring with unity and let A be an ideal of R. Then, R/A is an integral domain if and only if A is prime.

Theorem. Let R be a commutative ring with unity and let A be an ideal of R. Then, R/A is a field if and only if A is maximal.

⋆ When a commutative ring has a unity, it follows from the last two theorems that a maximal ideal is a prime ideal. A prime ideal need not be maximal.

> "There's no other way, really. It's just hard work."
>
> — Andrew Wiles

14 Ring Homomorphisms

ft. Emil Artin

Definition. A *ring homomorphism* ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations; i.e., for all $a, b \in R$:

$$\phi(a + b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a)\phi(b)\,.$$

A ring homomorphism that is both 1-1 and onto is called a *ring isomorphism*.

Theorem. Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S.

1) For any $r \in R$ and any positive integer n, $\phi(n \odot r) = n \odot \phi(r)$ and $\phi(r^n) = (\phi(r))^n$.

2) $\phi(A) = \{\phi(a) : a \in A\}$ is a subring of S.

3) If A is an ideal and ϕ is onto S, then $\phi(A)$ is an ideal.

4) $\phi^{-1}(B) = \{r \in R : \phi(r) \in B\}$ is an ideal of R.

5) If R is commutative, then $\phi(R)$ is commutative.

6) If R has a unity, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S and units in R map to units in S.

7) ϕ is an isomorphism if and only if ϕ is onto and $\ker \phi = \{r \in R : \phi(r) = 0\} = \{0\}$.

8) If ϕ is an isomorphism from R onto S, then ϕ^{-1} is an isomorphism from S onto R.

Theorem. Let ϕ be a ring homomorphism from a ring R to a ring S. Then $\ker \phi = \{r \in R : \phi(r) = 0\}$ is an ideal of R.

Theorem. *First Isomorphism thm for Rings.* Let ϕ be a ring homomorphism from R to S. Then the mapping from $R/\ker \phi$ to $\phi(R)$, given by $r + \ker \phi \mapsto \phi(r)$, is an isomorphism. In symbols, $R/\ker \phi \cong \phi(R)$.

Theorem. *Fundamental thm of Ring Homomorphisms.* Every ideal of a ring R is the kernel of a ring homomorphism of R. In particular, an ideal A is the kernel of the mapping $r \mapsto r + A$ from R to R/A. This homomorphism is called the *natural homomorphism* from R to R/A.

Theorem. Let R be a ring with unity 1. The mapping $\phi : \mathbb{Z} \to R$ given by $n \mapsto n \odot 1$ is a ring homomorphism.

Corollary. If R is a ring with unity and the characteristic of R is $n > 0$, then R contains a subring isomorphic to $\mathbb{Z}_n$. if the characteristic of R is 0, then R contains a subring isomorphic to $\mathbb{Z}$.

Corollary. For any positive integer m, the mapping $\phi : \mathbb{Z} \to \mathbb{Z}_m$ given by $x \mapsto x \bmod m$ is a ring homomorphism.

Corollary. If F is a field of characteristic p, then F contains a subfield isomorphic to $\mathbb{Z}_p$. If F is a field of characteristic 0, then F contains a subfield isomorphic to $\mathbb{Q}$.

$\star$ The intersection of all subfields of a field is itself a subfield. Hence, every field has a smallest subfield (i.e., a subfield that is contained in every subfield). This subfield is called the *prime subfield* of the field.

14.1 Field of Quotients

Theorem. Let D be an integral domain. Then there exists a field F (called the *field of quotients* of D) that contains a subring isomorphic to D.

The concept of a field of quotients is inspired by the relation between the rational numbers and the integers. Although the integral domain $\mathbb{Z}$ is not a field, it is at least contained in a field—the field $\mathbb{Q}$—which is nothing more than quotients of integers. This construction of

the rationals from the integers is used as a model for constructing the field of quotients for a general integral domain D.

Notation. When F is a field, the field of quotients of $F[x]$ is traditionally denoted by $F(x)$.

"We can work it out."

— John Lennon and Paul McCartney, "*We Can Work It Out*" (single)

15 Polynomial Rings

ft. James Joseph Sylvester

Definition. Let R be a commutative ring. The set of formal symbols

$$R[x] = \left\{ a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 : a_i \in R,\ n \in \mathbb{W} \right\}$$

is called the *ring of polynomials over* R in the indeterminate x. Two elements

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

and

$$b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$$

of $R[x]$ are considered equal if and only if $a_i = b_i$ for all $i \in \mathbb{W}$ (define $a_i = 0$ when $i > n$ and $b_i = 0$ when $i > m$).

$\star$ In general, given $f(x) \in R[x]$ and $a \in R$, $f(a)$ means substitute a for x in the formula for $f(x)$. This substitution is a homomorphism from $R[x]$ to R.

Definition. Let R be a commutative ring and let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

and

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$$

belong to $R[x]$. Then,

$$f(x) + g(x) = (a_s + b_s) x^s + (a_{s-1} + b_{s-1}) x^{s-1} + \ldots + (a_1 + b_1) x + a_0 + b_0 \,,$$

where $s = \max(m, n)$, $a_i = 0$ for all $i > n$, and $b_i = 0$ for all $i > m$. Also,

$$f(x) g(x) = c_{m+n} x^{m+n} + c_{m+n-1} x^{m+n-1} + \ldots + c_1 x + c_0 \,,$$

where $c_k = \sum_{j=0}^{k} a_j b_{k-j}$ for $k = 0, \ldots, m+n$.

$\star$ Using these definitions of addition and multiplication, $R[x]$ is a ring.

Terminology. If

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \,,$$

where $a_n \neq 0$, we say that $f(x)$ has *degree* n; the term a_n is called the *leading coefficient* of $f(x)$, and if the leading coefficient is the unity of R, we say that $f(x)$ is a *monic* polynomial. Polynomials of the form $f(x) = a_0$ are called *constant*. The polynomial $f(x) = 0$ has no degree.

Theorem. If D is an integral domain, then $D[x]$ is an integral domain.

15.1 Division Algorithm and Consequences

Theorem. Let F be a field and let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

The polynomials $q(x)$ and $r(x)$ in the division algorithm are called the *quotient* and *remainder* in the division of $f(x)$ by $g(x)$. When the ring of coefficients is a field, we can use the long division process to determine the quotient and remainder.

Let D be an integral domain. If $f(x)$ and $g(x)$ belong to $D[x]$, we say that $g(x)$ *divides* $f(x)$ *in* $D[x]$ and write $g(x) \mid f(x)$ if there exists an $h(x) \in D[x]$ such that $f(x) = g(x)h(x)$. In this case, we also call $g(x)$ a *factor* of $f(x)$. An element a is a *zero* (or a *root*) of a polynomial $f(x)$ if $f(a) = 0$. When F is a field, and $a \in F$, and $f(x) \in F[x]$, we say that a is a *zero of multiplicity* k ($k \geq 1$) if $(x-a)^k$ is a factor of $f(x)$ but $(x-a)^{k+1}$ is not a factor of $f(x)$.

Corollary. *Remainder thm.* For F a field, $a \in F$, and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

Corollary. *Factor thm.* Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then a is a zero of $f(x)$ iff $x - a$ is a factor of $f(x)$.

Theorem. A polynomial of degree n over a field has at most n zeros, counting multiplicity.

$\star$ This theorem is not true for arbitrary polynomial rings. Counterexample: the polynomial $x^2 + 7$ has 1, 3, 5, and 7 as zeros over $\mathbb{Z}_8$.

A special mention here goes to the n^{th} roots of unity. We find all complex zeros of $x^n - 1$. Let $\omega = e^{\frac{2\pi}{n}\iota}$. It follows that $\omega^n = 1$ and $\omega^k \neq 1$ for $1 \leq k < n$. Thus, each of $1, \omega, \omega^2, \ldots, \omega^{n-1}$ is an n^{th} root of unity and, by the previous theorem, there are no others. The complex number ω is called a *primitive* n^{th} *root of unity.*

15.2 Principal Ideal Domains

Definition. A *principal ideal domain (PID)* is an integral domain in which every ideal has the form $\langle a \rangle = \{ra : r \in R\}$ for some $a \in R$; i.e., every ideal of the integral domain is a principal ideal generated by some element in the domain.

Theorem. Let F be a field. Then $F[x]$ is a PID.

$\mathbb{Z}[x]$ is not a PID.

Theorem. Let F be a field, I a nonzero ideal in $F[x]$, and $g(x) \in F[x]$. Then, $I = \langle g(x) \rangle$ if and only if $g(x)$ is a nonzero polynomial of minimum degree in I.

> "If I feel unhappy, I do mathematics to become happy. If I am happy, I do mathematics to keep happy."
>
> — Paul Turán

16 Factorization Of Polynomials

ft. Ferdinand Eisenstein

Definition. Let D be an integral domain. A polynomial $f(x) \in D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be *irreducible* over D if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x), h(x) \in D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$. A nonzero, nonunit element of $D[x]$ that is not irreducible over D is called *reducible* over D.

Definition. The *content* of a nonzero polynomial $\sum_{i=1}^{n} a_i x^i$, where the a's are integers, is the GCD of the integer coefficients.

Definition. A *primitive* polynomial is an element of $\mathbb{Z}[x]$ with content 1.

Lemma. *Gauss.* The product of two primitive polynomials is primitive.

16.1 Reducibility Tests

In general, it is a difficult problem to decide whether or not a particular polynomial is reducible over an integral domain, but there are special cases when it is easy.

Theorem. *Reducibility test for Degrees 2 and 3.* Let F be a field. If $f(x) \in F[x]$ and $\deg f(x)$ is 2 or 3, then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.

Theorem. Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

16.2 Irreducibility Tests

Theorem. *Mod p Irreducibility test.* Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $\deg f(x) \geq 1$. Let $f_p(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $f_p(x)$ is irreducible over $\mathbb{Z}_p$ and $\deg f_p(x) = \deg f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

$\star$ The converse of this is false. If $f(x) \in \mathbb{Z}[x]$ and $f_p(x)$ is reducible over $\mathbb{Z}_p$ for some p, $f(x)$ may still be irreducible over $\mathbb{Q}$.

$\star$ The mod p irreducibility test may fail for some p's and work for others. To conclude that a particular $f(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$, all we need to do is find a single p for which the corresponding polynomial $f_p(x) \in \mathbb{Z}_p[x]$ is irreducible over $\mathbb{Z}_p$.

The mod p irreducibility test can be helpful in checking for irreducibility of polynomials of degree greater than 3 and polynomials with rational coefficients.

Theorem. *Eisenstein's Criterion (1850).* Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. If there is a prime p such that $p \nmid a_n$, $p \mid a_{n-1}$, $\ldots$, $p \mid a_0$, and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Corollary. *Gauss.* For any prime p, th p^{th} cyclotomic polynomial

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

is irreducible over $\mathbb{Q}$.

16.3 Irreducibility, Maximal Ideals, and Fields

Theorem. Let F be a field and let $p(x) \in F[x]$. Then, $\langle p(x) \rangle$ is a maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible.

Corollary. Let F be a field and $p(x) \in F[x]$ be an irreducible polynomial over F. The $F[x]/\langle p(x) \rangle$ is a field.

Corollary. Let F be a field and let $p(x), a(x), b(x) \in F[x]$. If $p(x)$ is irreducible over F and $p(x) \mid a(x)b(x)$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

16.4 Unique Factorization in $\mathbb{Z}[x]$

Recall that

- the units in $\mathbb{Z}[x]$ are precisely $f(x) = \pm 1$,
- the irreducible polynomials of degree 0 over $\mathbb{Z}$ are precisely those of the form $f(x) = \pm p$, where p is a prime, and
- every nonconstant polynomial from $\mathbb{Z}[x]$ that is irreducible over $\mathbb{Z}$ is primitive.

Theorem. Every polynomial in $\mathbb{Z}[x]$ that is not the zero polynomial or a unit in $\mathbb{Z}[x]$ can be written in the form

$$b_1 b_2 \ldots b_s p_1(x) p_2(x) \ldots p_m(x)\,,$$

where the b_is are ireducible polynomials of degree 0, and the $p_i(x)$s are irreducible polynomials of positive degree. Furthermore, if

$$b_1 b_2 \ldots b_s p_1(x) p_2(x) \ldots p_m(x) = c_1 c_2 \ldots c_t q_1(x) q_2(x) \ldots q_n(x)\,,$$

where the b_is and c_is are irreducible polynomials of degree 0, and the $p_i(x)$s and $q_i(x)$s are irreducible polynomials of positive degree, then $s = t$, $m = n$, and, after renumbering the c's and $q(x)$s, we have $b_i = \pm c_i$ for $i = 1, \ldots, s$, and $p_i(x) = \pm q_i(x)$ for $i = 1, \ldots, m$.

The two parts of the statement state existence and uniqueness respectively of the factorization of a polynomial in $\mathbb{Z}[x]$ into irreducibles. Hence, the theorem guarantees that every nonzero, nonunit polynomial in $\mathbb{Z}[x]$ has a unique factorization in terms of irreducibles.

"No matter how good you are at something, there's always about a million people better than you."

— Homer Simpson, *The Simpsons*

17 Divisibility In Integral Domains

ft. Euclid, Ernst Eduard Kummer

17.1 Irreducibles and Primes

Definition. Elements a and b of an integral domain D are called *associates* if $a = ub$, where u is a unit of D.

Definition. A nonzero element a of an integral domain D is called an *irreducible* if a is not a unit and, whenever $b, c \in D$ with $a = bc$, then b or c is a unit.

Definition. A nonzero element a of an integral domain D is called a *prime* if a is not a unit and $a \mid bc$ implies $a \mid b$ or $a \mid c$.

$\star$ An element a is prime iff $\langle a \rangle$ is a prime ideal.

$\star$ In the case of integers, the concepts of irreducibles and primes are equivalent, but in general, they are not.

The distinction between primes and irreducibles is best illustrated by integral domains of the form $\mathbb{Z}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} : a, b \in \mathbb{Z}\right\}$, where d is neither 1 nor is divisible by the square of a prime (square-free). These rings are of fundamental importance in number theory. To analyze these rings, we need a convenient method of determining their units, irreducibles, and primes. To do this, we define a function N, called the *norm* from $\mathbb{Z}\left[\sqrt{d}\right]$ into the whole numbers by $N\left(a + b\sqrt{d}\right) = |a^2 - db^2|$. The norm satisfies the following properties:

1) $N(x) = 0 \iff x = 0$.

2) $\forall x, y \in \mathbb{Z}\left[\sqrt{d}\right],\ N(xy) = N(x)N(y)$.

3) x is a unit in $\mathbb{Z}\left[\sqrt{d}\right]$ if and only if $N(x) = 1$.

4) If $N(x)$ is prime, then x is irreducible in $\mathbb{Z}\left[\sqrt{d}\right]$. The converse is not true.

Theorem. In an integral domain, every prime is an irreducible.

Theorem. In a PID, an element is an irreducible if and only if it is a prime.

It is an easy consequence of the respective division algorithms for $\mathbb{Z}$ and $F[x]$, where F is a field, that $\mathbb{Z}$ and $F[x]$ are PIDs. $\mathbb{Z}[x]$, however, is not.

17.2 Unique Factorization Domains

Definition. An integral domain D is a *unique factorization domain (UFD)* if

1) every nonzero element of D that is not a unit can be written as a product of irreducibles of D, and

2) the factorization into irreducibles is unique up to associates and the order in which the factors appear.

Another way to formulate part 2 of this definition is the following: If $p_1^{n_1}p_2^{n_2}\dots p_r^{n_r}$ and $q_1^{m_1}q_2^{m_2}\dots q_s^{m_s}$ are two factorizations of some element as a product of irreducibles, where no two of the p_is are associates and no two of the q_js are associates, then $r = s$, each p_i is an associate of one and only one q_j, and $n_i = m_j$.

The fundamental theorem of arithmetic tells us the ring of integers $\mathbb{Z}$ is a UFD, and the theorem in section 16.4 on unique factorization in $\mathbb{Z}[x]$ tells us that so is $\mathbb{Z}[x]$.

Lemma. *Ascending Chain Condition.* In a PID, any strictly increasing chain of ideals $I_1 \subset I_2 \subset \dots$ must be finite in length.

Theorem. Every PID is a UFD.

Corollary. Let F be a field. Then, $F[x]$ is a UFD.

Theorem. If D is a UFD, then $D[x]$ is a UFD.

17.2.1 Noetherian Domains

An integral domain that satisfies the ascending chain condition is called a *Noetherian domain (ND)*, named after Emmy Noether who inaugurated the use of chain conditions in algebra. Every PID is a Noetherian domain but not the other way round. Noetherian domains are of utmost importance in algebraic geometry. One reason for this is that, for many important rings R, the polynomial ring $R[x]$ is a Noetherian domain but not a PID. One such example is $\mathbb{Z}[x]$. In particular, $\mathbb{Z}[x]$ shows that a Noetherian domain need not be a PID.

17.3 Euclidean Domains

Definition. An integral domain D is called a *Euclidean domain (ED)* if there is a function d (called the *measure*) from the nonzero elements of D to the nonnegative integers such that

1) $d(a) \leq d(ab)$ for all nonzero $a, b \in D$; and

2) if $a, b \in D$, $b \neq 0$, then there exist elements q and r in D such that $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

The ring $\mathbb{Z}$ is an Euclidean domain with $d(a) = |a|$. Let F be a field. Then, $F[x]$ is an Euclidean domain with $d(f(x)) = \deg f(x)$. The ring of Gaussian integers $\mathbb{Z}[\iota]$ is a Euclidean domain where the norm is the measure.

Theorem. Every Euclidean domain is a PID.

If D is an Euclidean domain and I a nonzero ideal of D, then $I = \langle a \rangle$, where $a \in \arg\min_{x \in I \setminus \{0\}} d(x)$.

Corollary. Every Euclidean domain is a UFD.

Thus, to summarize:

$$\begin{aligned} \text{ED} &\implies \text{PID} \implies \text{UFD} \\ \text{UFD} &\not\Longrightarrow \text{PID} \not\Longrightarrow \text{ED} \\ \text{PID} &\implies \text{ND}, \ \text{ND} \not\Longrightarrow \text{PID}\,. \end{aligned}$$

> "I tell them that if they occupy themselves with the study of mathematics they will find in it the best remedy against lust of the flesh."
>
> — Thomas Mann, *The Magic Mountain*

18 Extension Fields

ft. Leopold Kronecker

Definition. A field E is an *extension field* of a field F if $F \subseteq E$ and the operations of F are those of E restricted to F (i.e., F is a subfield of E).

Theorem. *Fundamental thm of Field Theory (Kronecker, 1887).* Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then, there is an extension field E of F in which $f(x)$ has a zero.

Proof sketch. Since $F[x]$ is a UFD, $f(x)$ has an irreducible factor, say, $p(x)$. Consider the field $E = F[x]/\langle p(x) \rangle$. Since the mapping $\phi : F \to E$ given by $a \mapsto a + \langle p(x) \rangle$ is 1-1 and preserves both operations, E has a subfield isomorphic to F. We may think of E as containing F if we simply identify the coset $a + \langle p(x) \rangle$ with its unique coset representative $a \in F$. In E, $x + \langle p(x) \rangle$ is a zero of $p(x)$, and therefore of $f(x)$.

18.1 Splitting Fields

Notation. Let F be a field, and let $a_1, a_2, \ldots, a_n$ be elements of some extension E of F. We use $F(a_1, a_2, \ldots, a_n)$ to denote the smallest subfield of E that contains F *and* the set $\{a_1, a_2, \ldots, a_n\}$.

$\star$ $F(a_1, a_2, \ldots, a_n)$ is the intersection of all subfields of E that contain F and the set $\{a_1, a_2, \ldots, a_n\}$. That is, if K is any field that contains F and the set $\{a_1, a_2, \ldots, a_n\}$, then K contains $F(a_1, a_2, \ldots, a_n)$.

$\star$ $F(x)$ is the field of quotients of $F[x]$; i.e.,

$$F(x) = \{f(x)/g(x) : f(x), g(x) \in F[x], \ g(x) \neq 0\}\,.$$

Definition. Let E be an extension field of F and let $f(x) \in F[x]$ with degree at least 1 (nonconstant). We say that $f(x)$ *splits in* E if there are elements $a \in F$ and $a_1, a_2, \ldots, a_n \in E$ such that

$$f(x) = a(x - a_1)(x - a_2) \ldots (x - a_n) .$$

We call E the *splitting field of* $f(x)$ *over* F if $E = F(a_1, a_2, \ldots, a_n)$.

Note that a splitting field of a polynomial over a field depends not only on the polynomial but on the field as well. Indeed, a splitting field of $f(x)$ over F is just a smallest extension field of F in which $f(x)$ splits.

Theorem. Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then, there exists a splitting field E for $f(x)$ over F.

Theorem. Let F be a field and let $p(x) \in F[x]$ be irreducible over F. If a is a zero of $p(x)$ in some extension E of F, then $F(a)$ is isomorphic to $F[x]/\langle p(x) \rangle$. Furthermore, if $\deg p(x) = n$, then every member of $F(a)$ can be uniquely expressed in the form $\sum_{i=0}^{n} c_i a^i$, where each $c_i \in F$.

$\star$ In the language of vector spaces, the latter portion of the above theorem says that if a is a zero of an irreducible polynomial over F of degree n, then the set $\{1, a, \ldots, a^{n-1}\}$ is a basis for $F(a)$ over F.

$\star$ The above theorem does not apply to fields of the form $F(a)$ where a is in some extension field of F but not the zero of an element of $F(x)$. For instance, in 1882, Ferdinand von Lindemann proved that π is not the zero of any polynomial in $\mathbb{Q}[x]$. Because of this important result, the above theorem does not apply to $\mathbb{Q}(\pi)$.

Corollary. Let F be a field and let $p(x) \in F[x]$ be irreducible over F. If a is a zero of $p(x)$ in some extension E of F and b is a zero of $p(x)$ in some extension E' of F, then the fields $F(a)$ and $F(b)$ are isomorphic.

Notation. Any ring isomorphism ϕ from F to F' has a natural extension from $F[x]$ to $F'[x]$ given by $\sum_{i=0}^{n} c_n x^n \mapsto \sum_{i=0}^{n} \phi(c_n) x^n$. Since this mapping agrees with ϕ on F, it is convenient and natural to use ϕ to denote this mapping as well.

Lemma. Let F be a field, and let $p(x) \in F[x]$ be irreducible over F, and let a be a zero of $p(x)$ in some extension of F. If ϕ is a field isomorphism from F to F', and b is a zero of $\phi(p(x))$ in some extension of F', then there is an isomorphism from $F(a)$ to $F'(b)$ that agrees with ϕ on F and carries a to b.

Proof sketch. We know that there is an isomorphism α from $F(a)$ onto $F[x]/\langle p(x) \rangle$ that is the identity on F and carries $a \mapsto x + \langle p(x) \rangle$. Similarly, there is an isomorphism β from $F'[x]/\langle \phi(p(x)) \rangle$ onto $F'(b)$ that is the identity on F' and carries $x + \langle \phi(p(x)) \rangle \mapsto b$. Thus, $\beta\phi\alpha$ is the desired isomorphism from $F(a)$ onto $F'(b)$.

Theorem. Let ϕ be an isomorphism from a field F to a field F' and let $f(x) \in F[x]$. If E is a splitting field for $f(x)$ over F and E' is a splitting field for $\phi(f(x))$ over F', then there is an isomorphism from E to E' that agrees with ϕ on F.

Corollary. Let F be a field and let $f(x) \in F[x]$. Then any two splitting fields of $f(x)$ over F are isomorphic.

In light of the above corollary, we may refer to *the* splitting field of a polynomial over F without ambiguity.

Let a be a positive rational number and let ω be a primitive n^{th} root of unity. Then each of

$$a^{\frac{1}{n}}, \omega a^{\frac{1}{n}}, \omega^2 a^{\frac{1}{n}}, \ldots, \omega^{n-1} a^{\frac{1}{n}}$$

is a zero of $x^n - a$ in $\mathbb{Q}(\sqrt[n]{a}, \omega)$.

18.2 Zeros of an Irreducible Polynomial

Definition. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ belong to $F[x]$. The *derivative* of $f(x)$, denoted by $f'(x)$, is the polynomial $\sum_{i=1}^{n} i a_i x^{i-1}$ in $F[x]$.

Note that although this definition has origins in calculus, it does not involve the notion of a limit. The standard rules for handling sums and products of functions in calculus carry over to arbitrary fields as well.

Lemma. Let $f(x), g(x) \in F[x]$ and let $a \in F$. Then,

1) $(f(x) + g(x))' = f'(x) + g'(x)$.
2) $(af(x))' = af'(x)$.
3) $(f(x)g(x))' = f(x)g'(x) + g(x)f'(x)$.

Terminology. Zeros of multiplicity greater than 1 are called *multiple zeros*.

Theorem. Let F be a field. A polynomial $f(x) \in F[x]$ has a multiple zero in some extension E of F if and only if $f(x)$ and $f'(x)$ have a common factor of positive degree in $F[x]$.

Theorem. Let $f(x)$ be an irreducible polynomial over a field F. If F has characteristic 0, then $f(x)$ has no multiple zeros. If F has characteristic $p \neq 0$, then $f(x)$ has a multiple zero only if it is of the form $f(x) = g(x^p)$ for some $g(x) \in F[x]$.

Definition. A field F is called *perfect* if F has characteristic 0 or if F has characteristic p and $F^p = \{a^p : a \in F\} = F$.

Theorem. Every finite field is perfect.

Theorem. If $f(x)$ is an irreducible polynomial over a perfect field F, then $f(x)$ has no multiple zeros.

Theorem. Let $f(x)$ be an irreducible polynomial over a field F and let E be a splitting field of $f(x)$ over F. Then all the zeros of $f(x)$ in E have the same multiplicity.

Corollary. Let $f(x)$ be an irreducible polynomial over a field F and let E be a splitting field of $f(x)$. Then $f(x)$ has the form $a\prod_{i=0}^{n}(x - a_i)^m$, where the $a_i s$ are distinct elements of E, $a \in F$, and $m \in \mathbb{N}$.

"I have yet to see any problem, however complicated, which, when you looked at it in the right way, did not become still more complicated."

— Paul Anderson, *New Scientist*

19 Algebraic Extensions

ft. Ernst Steinitz

19.1 Characterization of Extensions

Definition. Let E be an extension field of a field F and let $a \in E$. We call a *algebraic over* F if a is the zero of some nonzero polynomial in $F[x]$. If a is not algebraic over F, it is called *transcendental over* F.

Definition. An extension E of F is called an *algebraic* extension of F if every element in E is algebraic over F. If E is not an algebraic extension of F, it is called a *transcendental* extension of F.

Definition. An extension of F of the form $F(a)$ is called a *simple* extension of F.

Leonhard Euler used the term "transcendental" for numbers that are not algebraic because "they transcend the power of algebraic methods."

Theorem. Let E be an extension field of the field F and let $a \in E$. If a is transcendental over F, then $F(a) \cong F(x)$. If a is algebraic over F, then $F(a) \cong F[x]/\langle p(x) \rangle$, where $p(x)$ is a polynomial in $F[x]$ of minimum degree such that $p(a) = 0$. Moreover, $p(x)$ is irreducible over F.

Theorem. If a is algebraic over a field F, then there is a unique monic irreducible polynomial $p(x) \in F[x]$ such that $p(a) = 0$.

$\star$ $p(x)$ in the above theorem is called the *minimal polynomial for* a *over* F.

Theorem. Let a be algebraic over F, and let $p(x)$ be the minimal polynomial for a over F. If $f(x) \in F[x]$, and $f(a) = 0$, then $p(x)$ divides $f(x)$ in $F[x]$.

If E is an extension field of F, we may view E as a vector space over F (i.e., the elements of E are the vectors and the elements of F are the scalars). We are then able to use such notions as dimension and basis in our discussion.

19.2 Finite Extensions

Definition. Let E be an extension field of a field F. We say that E has *degree* n *over* F, and write $[E : F] = n$, if E has dimension n as a vector space over F.

Definition. Let E be an extension field of a field F. If $[E : F]$ is finite, E is called a *finite extension* of F; otherwise, we say that E is an *infinite extension* of F.

For example, if a is algebraic over F and its minimal polynomial over F has degree n, then, from the third theorem in the section 18, we know that $\{1, a, \ldots, a^{n-1}\}$ is a basis for $F(a)$ over F; and, therefore $[F(a) : F] = n$. In this case, we say that *a has degree n over F*.

Theorem. If E is a finite extension of F, then E is an algebraic extension of F.

$\star$ The converse is not true; i.e., an algebraic extension E of F may be infinite.

Lemma. For any field extension E of a field F, $[E : F] = n$ if and only if $E \cong F^n$ as vector spaces.

Theorem. Let K be a finite extension field of the field E and let E be a finite extension field of the field F. Then, K is a finite extension field of F and $[K : F] = [K : E][E : F]$.

The above theorem is the field theory counterpart of Lagrange's theorem for finite groups. Like all counting theorems, it has far-reaching consequences.

Theorem. *Primitive Element thm (Steinitz, 1910).* If F is a field of characteristic 0, and a and b are algebraic over F, then there is an element $c \in F(a, b)$ such that $F(a, b) = F(c)$.

Corollary. Any finite extension of a field of characteristic 0 is a simple extension. An element a with the property that $E = F(a)$ is called a *primitive element* of E.

19.3 Properties of Algebraic Extensions

Theorem. If K is an algebraic extension of E and E is an algebraic extension of F, then K is an algebraic extension of F.

Corollary. Let E be an extension field of the field F. Then, the set of all elements of E that are algebraic over F is a subfield of E.

Definition. For any extension E of a field F, the subfield of E of the elements that are algebraic over F is called the *algebraic closure of F in E*.

Definition. A field that has no proper algebraic extension is called *algebraically closed*.

Theorem. *Steinitz (1910).* Every field F has a unique (up to isomorphism) algebraic extension that is algebraically closed. This field is called the *algebraic closure* of F.

In 1799, Gauss at the age of 22, proved that $\mathbb{C}$ is algebraically closed. This result was important enough at the time that it can be appropriately called the Fundamental Theorem of Classical Algebra (although not just of Algebra in light of modern advancements).

> "It matters not what goal you seek
> Its secret here reposes:
> You've got to dig from week to week
> To get Results or Roses."
>
> — Edgar Guest

20 Finite Fields

ft. L. E. Dickson, E. H. Moore

Theorem. For each prime p and each $n \in \mathbb{N}$, there is, up to isomorphism, a unique finite field of order p^n.

Because there is only one field for each prime power p^n, we may unambiguously denote it by $\mathrm{GF}(p^n)$, in honor of Galois, and call it the *Galois field of order* p^n. A standard representative for $\mathrm{GF}(p^n)$ is $\mathbb{Z}_p[x]/\langle f(x)\rangle$, where $f(x)$ is irreducible over $\mathbb{Z}_p$ of degree n. When $n = 1$, this field is $\mathbb{Z}_p$. For $n > 1$, it is not the ring $\mathbb{Z}_{p^n}$.

Theorem. As a group under addition, $\mathrm{GF}(p^n)$ is isomorphic to

$$\underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p}_{n \text{ factors}}.$$

As a group under multiplication, the set of nonzero elements of $\mathrm{GF}(p^n)$ is isomorphic to $\mathbb{Z}_{p^n-1}$ (and is, therefore, cyclic).

Corollary. $[\mathrm{GF}(p^n) : \mathrm{GF}(p)] = n$.

Corollary. Let a be a generator of the group of nonzero elements of $\mathrm{GF}(p^n)$ under multiplication. Then, a is algebraic over $\mathrm{GF}(p)$ of degree n.

Theorem. Let $f(x) \in \mathbb{Z}_p[x]$ be an irreducible polynomial over $\mathbb{Z}_p$ of degree d and let a be a zero of $f(x)$ in some extension field E of $\mathbb{Z}_p$. Then, $a, a^p, a^{p^2}, \ldots, a^{p^{d-1}}$ are the zeros of $f(x)$, and they are distinct.

Corollary. If $f(x)$ is an irreducible polynomial over $\mathbb{Z}_p$ and a is a zero of $f(x)$ in some extension field of $\mathbb{Z}_p$, then $\mathbb{Z}_p(a)$ is the splitting field of $f(x)$ over $\mathbb{Z}_p$.

Theorem. For each divisor m of n, $\mathrm{GF}(p^n)$ has a unique subfield of order p^m. Moreover, these are the only subfields of $\mathrm{GF}(p^n)$.

Theorem. The degree of an irreducible factor of $x^{p^n} - x$ over $\mathbb{Z}_p$ divides n.

"No pressure, no diamonds."

— Mary Case

21 Geometric Constructions

ft. Pierre Wantzel, Ferdinand Lindemann

21.1 Constructible Numbers

Definition. A real number a is *constructible* if a segment of length $|a|$ can be obtained from a unit segment by a finite number of operations with an unmarked straightedge and compass.

Theorem. The constructible numbers form a subfield of $\mathbb{R}$.

Theorem. If $a > 0$ is constructible, then $\sqrt{a}$ is constructible.

⋆ Thus, every rational number is constructible. Starting with constructible lengths, one may add, subtract, multiply, divide by a nonzero length, and take square roots of positive lengths.

Theorem. A real number c is constructible if and only if it belongs to a field F_n in a finite tower

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n \subseteq \mathbb{R}\,,$$

where $F_{i+1} = F_i(\sqrt{a_i})$ for some positive $a_i \in F_i$.

Proof sketch. Lines and circles determined by points with coordinates in a field F have equations with coefficients in F. Intersecting two lines requires only linear equations. Intersecting a line and a circle requires at most a quadratic equation. Subtracting the equations of two distinct intersecting circles reduces their intersection to the preceding case. Thus, each construction step adjoins at most a square root. Conversely, the field operations and square-root operation can all be performed geometrically.

Corollary. If c is constructible, then c is algebraic over $\mathbb{Q}$ and $[\mathbb{Q}(c) : \mathbb{Q}] = 2^k$ for some nonnegative integer k.

⋆ Having degree a power of 2 is necessary but is not sufficient in general. The full criterion is membership in a tower of quadratic extensions.

21.2 The Classical Impossibilities

Theorem. A cube of twice the volume of a given cube cannot be constructed with an unmarked straightedge and compass.

Proof sketch. Starting with a unit cube would require constructing $\sqrt[3]{2}$. But $x^3 - 2$ is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Theorem. There is no straightedge-and-compass construction that trisects every angle.

Proof sketch. Trisecting a 60° angle would make $\cos 20^\circ$ constructible. The identity $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ gives

$$8\cos^3 20^\circ - 6\cos 20^\circ - 1 = 0\,.$$

The polynomial $8x^3 - 6x - 1$ is irreducible over $\mathbb{Q}$, so $\cos 20^\circ$ has degree 3 and is not constructible.

⋆ Particular angles can be trisected. For example, a right angle can be trisected by constructing 30°; the theorem rules out a procedure for *every* angle.

Theorem. A square with the same area as a given circle cannot be constructed with an unmarked straightedge and compass.

Proof sketch. For the unit circle, the square would have side $\sqrt{\pi}$. Constructibility would imply that π is algebraic, contradicting Lindemann's theorem that π is transcendental.

The impossibility statements depend on the permitted tools. The algebra identifies exactly which extensions these tools can produce. The construction of regular polygons will be settled in the section on cyclotomic extensions.

> "Only prove to me that it is impossible, and I will set about it this very evening."
>
> — A member of the audience after De Morgan's lecture on squaring the circle

22 Sylow Theorems

ft. Ludwig Sylow

22.1 Conjugacy Classes

Definition. Let a and b be elements of a group G. We say that a and b are *conjugate* in G (and call b a *conjugate* of a) if $xax^{-1} = b$ for some $x \in G$. The conjugacy class of a is the set $\mathrm{cl}(a) = \{xax^{-1} : x \in G\}$.

$\star$ Conjugacy is an equivalence relation on G, and the conjugacy class of a is the equivalence class of a under conjugacy.

Theorem. Let G be a finite group and let a be an element of G. Then, $|\mathrm{cl}(a)| = |G : C(a)|$.

Corollary. In a finite group, $|\mathrm{cl}(a)|$ divides $|G|$.

Corollary. *Class Equation.* For any finite group G,

$$|G| = \sum |G : C(a)|\,,$$

where the sum runs over one element a from each conjugacy class of G.

Theorem. Let G be a nontrivial finite group whose order is a power of a prime p. Then, $Z(G)$ has more than one element.

Corollary. If $|G| = p^2$, where p is a prime, then G is Abelian.

22.2 Sylow I

Theorem. *Sylow (1872).* Let G be a finite group and let p be a prime. If p^k divides $|G|$, then G has at least one subgroup of order p^k.

Proof. *Frobenius (1895).* Proceed by induction on $|G|$.

1. If $|G| = 1$, Sylow I is trivially true.
2. Assume that Sylow I is true for all groups of order less than $|G|$.

3. If G has a proper subgroup H such that p^k divides $|H|$, then, by the inductive hypothesis, H has a subgroup of order p^k and we are done. If p^k does not divide the order of any proper subgroup of G,

    1. consider the class equation in the form

    $$|G| = |Z(G)| + \sum |G : C(a)|\,,$$

    where we sum over a representative of each conjugacy class $\mathrm{cl}(a)$, where $a \notin Z(G)$.

    2. Since p^k divides $|G| = |G : C(a)||C(a)|$ and $p^k \nmid |C(a)|$, we know that p must divide $|G : C(a)|$ for all $a \notin Z(G)$. It then follows from the class equation that p divides $|Z(G)|$.

    3. By the fundamental theorem of finite Abelian groups, $Z(G)$ contains an element of order p, say x. Since $x \in Z(G)$, $\langle x \rangle \triangleleft G$, and we may form the factor group $G/\langle x \rangle$. Now, p^{k-1} divides $|G/\langle x \rangle|$.

    4. Thus, by the inductive hypothesis, $G/\langle x \rangle$ has a subgroup of order p^{k-1}, and it can be shown that this subgroup has the form $H/\langle x \rangle$, where $H \leq G$. $|H| = |H/\langle x \rangle||\langle x \rangle| = p^{k-1} \cdot p = p^k$.

Corollary. *Cauchy (1845).* Let G be a finite group and let p be a prime that divides the order of G. Then, G has an element of order p.

The corollary to the fundamental theorem of finite Abelian groups and Sylow I show that the converse of Lagrange's theorem is true for all finite Abelian groups and all finite groups of prime-power order.

22.3 Sylow II

Definition. Let G be a finite group and let p be a prime. If $p^k \mid |G|$ and $p^{k+1} \nmid |G|$, then a subgroup of G of order p^k is called a *Sylow p-subgroup* of G.

$\star$ A Sylow p-subgroup has the largest order that is a power of p permitted by Lagrange's theorem. The trivial subgroup is a Sylow p-subgroup if and only if $p \nmid |G|$.

Definition. Subgroups H and K of a group G are *conjugate* in G if $H = gKg^{-1}$ for some $g \in G$.

Theorem. *Sylow II.* If H is a subgroup of a finite group G and $|H|$ is a power of a prime p, then H is contained in a Sylow p-subgroup of G.

Proof sketch. Let P be a Sylow p-subgroup of G, and let $\mathcal{C} = \{gPg^{-1} : g \in G\}$. The group H acts on $\mathcal{C}$ by conjugation. Each orbit has size a power of p, whereas $|\mathcal{C}| = |G : N(P)|$ is not divisible by p. Hence, there is an orbit of size 1, say $\{Q\}$. Then $H \leq N(Q)$, so HQ is a subgroup whose order is a power of p. Since Q is a Sylow p-subgroup, $HQ = Q$; i.e., $H \leq Q$.

22.4 Sylow III

Notation. The number of Sylow p-subgroups of a finite group G is denoted by n_p.

Theorem. *Sylow III.* Let G be a finite group of order $p^k m$, where p is prime and $p \nmid m$. Then,

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

2) $n_p \mid m$.

3) Any two Sylow p-subgroups of G are conjugate in G.

Corollary. If P is a Sylow p-subgroup of G, then $n_p = |G : N(P)|$.

Corollary. A Sylow p-subgroup of a finite group G is normal in G if and only if it is the unique Sylow p-subgroup of G.

⋆ Sylow I gives existence, Sylow II gives containment, and Sylow III gives conjugacy and restrictions on the number of Sylow subgroups.

⋆ Distinct subgroups of order p intersect only in the identity. This need not be true of distinct Sylow p-subgroups of order greater than p.

22.5 Applications of Sylow Theorems

To extract information about a finite group G from its order:

1. Write $|G|$ as a product of prime powers.
2. For each prime divisor p, list the divisors of $|G|/p^k$ that are equal to 1 modulo p, where p^k is the largest power of p dividing $|G|$.
3. If the only possibility is $n_p = 1$, the corresponding Sylow subgroup is normal.
4. Use counting, intersections of subgroups, and normalizers to eliminate remaining possibilities. If the normal subgroups give an IDP, determine the corresponding EDP.

Theorem. Let G be a group of order pq, where p and q are primes, $p < q$, and $p \nmid q - 1$. Then, $G \cong \mathbb{Z}_{pq}$.

Corollary. Every group of order 15 is cyclic.

⋆ Every group of order 45 has unique Sylow 3- and Sylow 5-subgroups. Consequently, it is isomorphic to $\mathbb{Z}_{45}$ or $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

⋆ If $|G| = 30$, then $n_5 = 1$ or 6 and $n_3 = 1$ or 10. Having both $n_5 = 6$ and $n_3 = 10$ would give $6 \cdot 4 + 10 \cdot 2 = 44$ nonidentity elements. Hence, at least one of the Sylow 3- and Sylow 5-subgroups is normal. Their product is a cyclic subgroup of order 15, which is normal because it has index 2.

> "I have always grown from my problems and challenges, from the things that don't work out. That's when I've really learned."
>
> — Carol Burnett

23 Finite Simple Groups

ft. Michael Aschbacher, Daniel Gorenstein, John Thompson

Definition. A group G is *simple* if its only normal subgroups are $\{e\}$ and G.

⋆ With this definition, the trivial group is simple. It is customary elsewhere to require a simple group to be nontrivial. The nontrivial Abelian simple groups are precisely the cyclic groups of prime order.

Definition. A series of subgroups

$$\{e\} = G_n \triangleleft G_{n-1} \triangleleft \ldots \triangleleft G_1 \triangleleft G_0 = G$$

with each G_{i+1} a proper normal subgroup of G_i and each G_i/G_{i+1} simple is called a *composition series* of G. The factor groups G_i/G_{i+1} are called the *composition factors* of G.

Theorem. *Jordan–H"older.* Every nontrivial finite group has a composition series. Its composition factors are unique up to isomorphism and order.

Simple groups serve as the building blocks of finite groups, much as primes do for positive integers. One obtains a composition series by choosing a proper normal subgroup of largest order at each stage.

⋆ Composition factors do not determine a group up to isomorphism. For example, $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ both have two composition factors isomorphic to $\mathbb{Z}_2$.

23.1 Nonsimplicity Tests

Theorem. *Sylow test.* Let n be a composite positive integer and let p be a prime divisor of n. If 1 is the only divisor of n that is equal to 1 modulo p, then no group of order n is simple.

Theorem. $2 \cdot$ *Odd test.* If $n > 1$ is odd, then no group of order $2n$ is simple.

Theorem. *Generalized Cayley thm.* Let $H \leq G$, and let S be the group of all permutations of the left cosets of H in G. The mapping $\phi : G \to S$ given by $\phi(g)(xH) = gxH$ is a homomorphism. Its kernel is contained in H and contains every normal subgroup of G contained in H.

⋆ More explicitly,

$$\ker \phi = \bigcap_{x \in G} xHx^{-1}\,.$$

This subgroup is called the *core of H in G*. It is the largest normal subgroup of G contained in H.

Corollary. *Index thm.* Let G be finite and let $H < G$. If $|G| \nmid |G : H|!$, then H contains a nontrivial normal subgroup of G. In particular, G is not simple.

Corollary. *Embedding thm.* If a finite non-Abelian simple group G has a proper subgroup of index n, then G is isomorphic to a subgroup of A_n.

⋆ For a Sylow subgroup P, $|G : N(P)| = n_p$. Thus, when $n_p > 1$, the index theorem can be applied to $N(P)$. For example, a group of order 72 has $n_3 = 1$ or 4. The first case gives a normal Sylow subgroup; the second gives a nontrivial kernel since $72 \nmid 4!$.

23.2 The Simplicity of A_5

Theorem. A_5 is simple.

Proof sketch. The conjugacy classes of A_5 have sizes 1, 15, 20, 12, and 12. They consist respectively of the identity, the products of two disjoint 2-cycles, the 3-cycles, and two classes of 5-cycles. A normal subgroup is a union of conjugacy classes containing the identity. No sum of 1 with a nonempty proper selection of 15, 20, 12, and 12 is a divisor of 60. By Lagrange's theorem, no proper nontrivial normal subgroup exists.

Theorem. *Galois.* A_n is simple for all $n \geq 5$.

Corollary. Every finite group is isomorphic to a subgroup of a finite simple group.

23.3 Classification of Finite Simple Groups

Theorem. *Feit–Thompson (1963).* Every finite group of odd order is solvable. In particular, every finite non-Abelian simple group has even order.

Theorem. *Classification of Finite Simple Groups.* Every nontrivial finite simple group is isomorphic to one of the following:

1) A cyclic group of prime order.
2) An alternating group A_n, $n \geq 5$.
3) A simple group of Lie type over a finite field.
4) One of the 26 sporadic simple groups.

The classification required the work of many mathematicians over several decades. The sporadic groups are the exceptions to the infinite families; the largest is the *Monster*. The simplicity of A_5 will be essential in the section on Galois theory.

> "If you don't learn from your mistakes, there's no sense making them."
>
> — Herbert V. Prochnow

24 Generators And Relations

ft. Walther von Dyck, Marshall Hall, Jr.

24.1 Definitions and Notation

Definition. Let S be a set of distinct symbols, and let $S^{-1} = \{x^{-1} : x \in S\}$ be a set of formal inverse symbols. A *word* from S is a finite string $x_1 x_2 \dots x_k$, where each $x_i \in S \cup S^{-1}$. The string with no symbols is called the *empty word* and is denoted by e. The set of all words from S is denoted by $W(S)$.

Multiplication in $W(S)$ is juxtaposition (concatenation). This operation is associative and has the empty word as identity, but a string such as aa^{-1} is not literally the empty word. To obtain inverses, we pass to equivalence classes.

Definition. Two words $u, v \in W(S)$ are *equivalent* if one can be obtained from the other by a finite sequence of insertions or deletions of strings of the form xx^{-1} or $x^{-1}x$, where $x \in S$.

⋆ This is an equivalence relation. A word is called *reduced* if it contains no adjacent inverse pair. Every equivalence class contains exactly one reduced word.

24.2 Free Group

Theorem. Let $\overline{u}$ denote the equivalence class of $u \in W(S)$. The set of these equivalence classes is a group under the operation $\overline{u}\,\overline{v} = \overline{uv}$.

Definition. The group in the preceding theorem is called the *free group on* S and is denoted by $F(S)$.

⋆ The identity is $\overline{e}$, and $\overline{x_1 x_2 \dots x_k}^{-1} = \overline{x_k{}^{-1} \dots x_2{}^{-1} x_1{}^{-1}}$. Usually, the bars are omitted once the group has been defined.

Theorem. *Universal Mapping Property.* Any mapping from S into a group G extends uniquely to a homomorphism from $F(S)$ to G.

Corollary. Every group is a homomorphic image of a free group.

Corollary. Every group is isomorphic to a factor group of a free group.

⋆ The free group on one generator is isomorphic to $\mathbb{Z}$. A free group on at least two generators is non-Abelian: the reduced words ab and ba are distinct.

Theorem. Every subgroup of a free group is free.

24.3 Generators and Relations

Definition. Let F be the free group on $\{a_1, a_2, \dots, a_n\}$, and let $w_1, w_2, \dots, w_t \in F$. Let N be the smallest normal subgroup of F containing the w_is. The expression

$$G = \langle a_1, a_2, \dots, a_n \mid w_1 = w_2 = \dots = w_t = e \rangle$$

means that $G \cong F/N$, with $a_i N$ corresponding to the designated generator a_i of G. This expression is called a *presentation* of G.

⋆ The subgroup N is the *normal closure* of the relators $w_1, \dots, w_t$. Ordinary subgroup generation would not in general suffice, since we need a normal subgroup to form F/N.

A relation may be written implicitly. For instance, $ab = ba$ means $aba^{-1}b^{-1} = e$. The presentation specifies that all relations between the generators follow from the listed relations and the group axioms.

Theorem. *Dyck (1882).* Adding relations to a presentation gives a homomorphic image of the original group.

Corollary. Suppose G is a finite group given by a presentation, and K is generated by elements satisfying the defining relations of G. If $|K| \geq |G|$, then $K \cong G$.

To identify a group given by generators and relations:

1. Use the relations to reduce every word to one of a list of possible forms. A list of n words gives an upper bound $|G| \leq n$.
2. Find a concrete group of order n generated by elements satisfying the relations.
3. Apply Dyck's theorem to conclude that the words are distinct and the groups are isomorphic.

$\star$ Merely listing possible words does not show that they are distinct. For example,

$$\left\langle a, b \mid a^3 = b^9 = e,\ a^{-1}ba = b^{-1} \right\rangle \cong \mathbb{Z}_3 \,.$$

Conjugating b by a three times gives both b and b^{-1}, so $b^2 = e$. Together with $b^9 = e$, this forces $b = e$.

24.4 Classification of Groups of Small Order

Notation. Following the textbook, Q_4 denotes the quaternion group of order 8. It has presentation

$$\mathsf{Q}_4 = \left\langle a, b \mid a^4 = e,\ a^2 = b^2,\ b^{-1}ab = a^{-1} \right\rangle .$$

Theorem. *Cayley (1859).* Up to isomorphism, the groups of order 8 are

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathsf{D}_4, \quad \mathsf{Q}_4 \,.$$

Theorem. Up to isomorphism, the groups of order 12 are

$$\mathbb{Z}_{12}, \quad \mathbb{Z}_6 \times \mathbb{Z}_2, \quad \mathsf{D}_6, \quad \mathsf{A}_4, \quad \mathsf{Q}_6 \,,$$

where the *dicyclic group* Q_6 has presentation

$$\mathsf{Q}_6 = \left\langle a, b \mid a^6 = e,\ a^3 = b^2,\ b^{-1}ab = a^{-1} \right\rangle .$$

Together with the classifications of groups of order p, p^2, $2p$, and 15, these results determine all groups of order at most 15.

24.5 Characterization of Dihedral Groups

Theorem. For $n \geq 3$,

$$\mathsf{D}_n \cong \left\langle a, b \mid a^n = b^2 = (ab)^2 = e \right\rangle.$$

Definition. The same presentation defines D_1 and D_2. In particular, $\mathsf{D}_1 \cong \mathbb{Z}_2$ and $\mathsf{D}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Definition. The *infinite dihedral group* is

$$\mathsf{D}_\infty = \left\langle a, b \mid a^2 = b^2 = e \right\rangle.$$

Theorem. Any group generated by two elements of order 2 is dihedral. More precisely, if $G = \langle a, b \rangle$ with $|a| = |b| = 2$, then $G \cong \mathsf{D}_n$ when $|ab| = n < \infty$, and $G \cong \mathsf{D}_\infty$ when ab has infinite order.

⋆ Set $r = ab$. Then $ara^{-1} = r^{-1}$, and every element has the form r^i or $r^i a$. This recovers the familiar description of dihedral groups in terms of rotations and reflections.

> "It don't come easy."
>
> — Ringo Starr, "*It Don't Come Easy*" (single)

25 Symmetry Groups

ft. Hermann Weyl, Auguste Bravais

25.1 Isometries

Definition. An *isometry* of $\mathbb{R}^n$ is a mapping $T : \mathbb{R}^n \to \mathbb{R}^n$ that is onto and preserves distance; i.e., $d(T(p), T(q)) = d(p, q)$ for all $p, q \in \mathbb{R}^n$.

Definition. Let $F \subseteq \mathbb{R}^n$. The *symmetry group of F in $\mathbb{R}^n$* is the group of all isometries of $\mathbb{R}^n$ that carry F onto itself, under function composition.

⋆ An isometry is necessarily 1-1, and its inverse is an isometry. Symmetries carry the figure *onto* itself; they need not fix every point of the figure.

⋆ The ambient space matters. A nondegenerate line segment has a symmetry group of order 2 in $\mathbb{R}$, order 4 in $\mathbb{R}^2$, and infinite order in $\mathbb{R}^3$.

Theorem. Every isometry of $\mathbb{R}^2$ is a rotation, reflection, translation, or glide-reflection.

Definition. A *translation* moves every point by the same vector. A *reflection* across a line L fixes L pointwise and sends $p \notin L$ to the point p' such that L is the perpendicular bisector of the segment joining p and p'. A *glide-reflection* is the composition of a reflection and a translation parallel to its axis.

⋆ Rotations and translations preserve orientation. Reflections and glide-reflections reverse orientation. A nonidentity translation or a glide-reflection with nonzero translation has infinite order.

25.2 Classification of Finite Plane Symmetry Groups

Theorem. The only finite plane symmetry groups, up to isomorphism, are $\mathbb{Z}_n$ and D_n.

⋆ If a finite plane symmetry group contains a reflection, exactly half its elements are rotations and half are reflections.

25.3 Finite Groups of Rotations in $\mathbb{R}^3$

Theorem. Up to isomorphism, the finite groups of rotations in $\mathbb{R}^3$ are

$$\mathbb{Z}_n, \quad \mathsf{D}_n, \quad \mathsf{A}_4, \quad \mathsf{S}_4, \quad \mathsf{A}_5\,.$$

The three additional groups are realized by the regular solids:

1) The *tetrahedral group*, the rotation group of a regular tetrahedron, is isomorphic to A_4 and has order 12.
2) The *octahedral group*, the rotation group of a cube or a regular octahedron, is isomorphic to S_4 and has order 24.
3) The *icosahedral group*, the rotation group of a regular dodecahedron or icosahedron, is isomorphic to A_5 and has order 60.

⋆ These are groups of rotations. Including orientation-reversing isometries gives the full symmetry groups, which have orders 24, 48, and 120, respectively.

⋆ The dihedral groups occur here as groups of rotations in three dimensions. The transformations that act as reflections on a regular polygon in its plane can be realized by half-turns about axes lying in that plane.

> "Perhaps the most valuable result of all education is the ability to make yourself do the thing you have to do, when it ought to be done, whether you like it or not."
>
> — Thomas Henry Huxley, "Technical Education"

26 Symmetry And Counting

ft. William Burnside

Two designs are equivalent under a group G if an element of G carries one to the other. Thus, counting nonequivalent designs means counting orbits of designs under G.

26.1 Burnside's Theorem

Definition. Let G be a group of permutations of a set S, and let $\phi \in G$. The set

$$\text{fix}(\phi) = \{s \in S : \phi(s) = s\}$$

is called the set of *elements fixed by* ϕ.

Theorem. *Burnside.* Let G be a finite group of permutations of a finite set S. The number of orbits of S under G is

$$\frac{1}{|G|} \sum_{\phi \in G} |\text{fix}(\phi)| \,.$$

Proof sketch. Count the pairs (ϕ, s) with $\phi(s) = s$ in two ways:

$$\sum_{\phi \in G} |\text{fix}(\phi)| = \sum_{s \in S} |\text{stab}_G(s)| \,.$$

By the orbit-stabilizer theorem, the contribution of each orbit on the RHS is exactly $|G|$. Divide by $|G|$.

⋆ Burnside's theorem says that the number of orbits is the average number of fixed points. The theorem appeared in Frobenius's work before Burnside's book made it widely known.

26.2 Applications

To count designs up to symmetry:

1. Specify the set S of designs and the group G of permitted symmetries.
2. Group the elements of G according to their effect on the positions being colored.
3. Count the designs fixed by one element of each type, multiply by the number of elements of that type, and sum.
4. Divide the sum by $|G|$.

⋆ Suppose a permutation ϕ of the positions has c disjoint cycles, including 1-cycles. With q available colors and no restrictions on how often they occur, ϕ fixes q^c colorings: each cycle must be monochromatic.

For example, the rotations of a square act on the colorings of its four vertices with q colors. The identity fixes q^4 colorings, each quarter-turn fixes q, and the half-turn fixes q^2. Thus, the number of colorings up to rotation is

$$\frac{q^4 + q^2 + 2q}{4} \,.$$

If reflections are also allowed, the two diagonal reflections each fix q^3 colorings and the other two each fix q^2. Hence, the number up to all symmetries is

$$\frac{q^4 + 2q^3 + 3q^2 + 2q}{8} \,.$$

⋆ When prescribed numbers of each color must be used, the choices for the cycles are constrained. One cannot simply use q^c. For example, six vertices colored with exactly three black and three white vertices give 4 designs up to rotation, but 3 up to the full dihedral group.

26.3 Group Action

Definition. A group G *acts on* a set S if there is a homomorphism $\gamma : G \to \mathsf{Sym}(S)$, where $\mathsf{Sym}(S)$ is the group of all permutations of S.

Equivalently, an action is a mapping $G \times S \to S$, denoted by $(g, s) \mapsto g \cdot s$, such that

1) $e \cdot s = s$ for all $s \in S$.

2) $(gh) \cdot s = g \cdot (h \cdot s)$ for all $g, h \in G$ and $s \in S$.

Definition. The *orbit* and *stabilizer* of $s \in S$ are

$$\mathrm{orb}_G(s) = \{g \cdot s : g \in G\} \quad \text{and} \quad \mathrm{stab}_G(s) = \{g \in G : g \cdot s = s\}\,.$$

Theorem. *Orbit-Stabilizer thm.* For a finite group G acting on a set S,

$$|\mathrm{orb}_G(s)| = |G : \mathrm{stab}_G(s)|\,.$$

Definition. An action is *faithful* if $\ker \gamma = \{e\}$, and is *transitive* if S has exactly one orbit.

⋆ In a faithful action, distinct elements of G give distinct permutations of S. Burnside's theorem also holds for actions that are not faithful, with the sum taken over all elements of G.

We have already encountered several actions: left multiplication on G in Cayley's theorem, conjugation on Sylow subgroups, and left multiplication on the cosets of a subgroup. Their stabilizers are, respectively, $\{e\}$, the normalizer of the chosen Sylow subgroup, and the chosen subgroup (for its identity coset).

> "Whenever you can, count."
>
> — Francis Galton

27 Cayley Digraphs Of Groups

ft. William Rowan Hamilton

27.1 The Cayley Digraph of a Group

Definition. A *directed graph* (or *digraph*) consists of vertices and directed arcs between vertices. Let G be a finite group and let S be a generating set for G. The *Cayley digraph* $\mathrm{Cay}(S : G)$ is defined by

1) The vertices are the elements of G.

2) There is an arc from x to y labeled by $s \in S$ if $y = xs$.

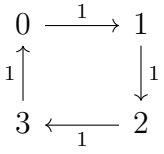
Different colors or line styles distinguish the generators. A generator of order 2 gives arcs in both directions, which may be drawn as one undirected edge.

⋆ The arcs represent multiplication on the right. Starting at e and following arcs labeled $s_1, s_2, \ldots, s_k$ leads to $s_1 s_2 \ldots s_k$. Traversing an arc in reverse represents multiplication by the inverse of its label.

⋆ A word in the generators and their inverses is a relation precisely when the corresponding walk starting at e returns to e. Reversing an arc is permitted for reading words, but a directed path must follow the directions of its arcs.

⋆ A Cayley digraph depends on the generating set as well as the group. Its geometry on the page is irrelevant; the labeled connections carry the algebraic information.

For example, $\mathrm{Cay}(\{1\} : \mathbb{Z}_n)$ is a directed n-cycle. The following is the case $n = 4$:



27.2 Hamiltonian Circuits and Paths

Definition. A *Hamiltonian circuit* in a digraph is a directed circuit that visits each vertex exactly once before returning to its starting vertex. A *Hamiltonian path* is a directed path that visits each vertex exactly once, without returning to the start.

Theorem. If $m, n > 1$ and $\gcd(m, n) = 1$, then

$$\mathrm{Cay}(\{(1,0),(0,1)\} : \mathbb{Z}_m \times \mathbb{Z}_n)$$

has no Hamiltonian circuit.

Theorem. If $n \mid m$, then $\mathrm{Cay}(\{(1,0),(0,1)\} : \mathbb{Z}_m \times \mathbb{Z}_n)$ has a Hamiltonian circuit.

Notation. For a sequence of generators $(a, b, \ldots, c)$ and a positive integer k, let $k*(a, b, \ldots, c)$ denote the concatenation of k copies of that sequence.

The circuit in the preceding theorem can be described, starting at $(0, 0)$, by

$$m * ((n-1) * (0,1), (1,0)) .$$

Theorem. If G is a finite Abelian group and S is any generating set for G, then $\mathrm{Cay}(S : G)$ has a Hamiltonian path.

⋆ Left multiplication by any $g \in G$ preserves the labeled arcs: $x \to xs$ becomes $gx \to (gx)s$. Thus, a sequence giving a Hamiltonian path or circuit from one starting vertex gives one from any starting vertex.

27.3 Applications

A Hamiltonian path gives an ordering of all group elements in which consecutive elements differ by multiplication by a chosen generator. Cayley digraphs consequently provide models for interconnection networks, systematic enumeration, and permutation problems such as change ringing. The uniformity of the graph reflects the group operation.

> "A mathematician is a machine for turning coffee into theorems."
>
> — Alfr'ed R'enyi

28 Introduction To Algebraic Coding Theory

ft. Richard W. Hamming, Jessie MacWilliams, Vera Pless

A code introduces redundancy into a message so that errors in transmission can be detected or corrected. For example, sending 00000 for 0 and 11111 for 1 allows majority rule to correct any two errors in a block. The cost is that four of the five transmitted digits are redundant.

28.1 Linear Codes

Definition. An (n, k) *linear code* over a finite field F is a k-dimensional subspace C of the vector space F^n. Its elements are called *code words*. If $F = \mathbb{Z}_2$, the code is *binary*; if $F = \mathbb{Z}_3$, it is *ternary*.

$\star$ If $|F| = q$, then C has q^k code words, whereas there are q^n possible received words. The number k/n is the *rate* of the code.

Definition. The *Hamming distance* $d(u, v)$ between $u, v \in F^n$ is the number of components in which they differ. The *Hamming weight* $\mathrm{wt}(u)$ is the number of nonzero components of u. The Hamming weight of a nonzero linear code is the minimum weight of its nonzero code words.

Theorem. For $u, v, w \in F^n$,

1) $d(u, v) = \mathrm{wt}(u - v)$.

2) $d(u, v) \le d(u, w) + d(w, v)$.

Corollary. The minimum distance d between distinct code words of a nonzero linear code equals its minimum nonzero weight.

Definition. In *nearest-neighbor decoding*, a received word w is decoded as a code word c for which $d(w, c)$ is a minimum. If there is a tie, one may decline to decode or make a fixed choice among the nearest code words.

Theorem. A linear code of minimum distance d can correct any $\lfloor (d-1)/2 \rfloor$ or fewer errors by nearest-neighbor decoding. Alternatively, it can detect any $d - 1$ or fewer errors.

⋆ The two guarantees are alternatives, not simultaneous guarantees. A code of minimum distance 3 can correct one error or detect up to two errors; a decoder attempting correction may mistake two errors for a single error from a different code word.

Definition. A *generator matrix* for an (n, k) linear code is a $k \times n$ matrix G whose rows form a basis for the code. A message $m \in F^k$ is encoded as mG.

Definition. A generator matrix of the form $G = [I_k \mid A]$ is in *standard form*. The resulting code is *systematic*: the first k components of mG are the message and the last $n - k$ are the redundant components.

⋆ Throughout, messages and code words are row vectors. All arithmetic takes place in F.

28.2 Parity-Check Matrix Decoding

Definition. If $G = [I_k \mid A]$, the *parity-check matrix* is the $n \times (n - k)$ matrix

$$H = \begin{bmatrix} -A \\ I_{n-k} \end{bmatrix} .$$

⋆ Many references call H^{T} the parity-check matrix and use column vectors instead. Here, the convention is chosen so that we multiply a received word by H on the right.

Lemma. *Orthogonality.* $GH = 0$, and $w \in C \iff wH = 0$.

Definition. The vector wH is called the *syndrome* of w.

If $w = c + e$, where $c \in C$ was sent and e is the error vector, then

$$wH = (c + e)H = eH .$$

Thus, the syndrome depends only on the error.

Theorem. Parity-check matrix decoding corrects every single error if and only if all rows of H are nonzero and no row is a scalar multiple of another row.

Corollary. For a binary code, the condition is that the rows of H be nonzero and distinct.

The single-error decoding procedure is:

1. Compute wH.
2. If $wH = 0$, assume that no error occurred.
3. If $wH = sH_i$ for a unique row H_i and a unique nonzero scalar s, subtract s from the i^{th} component of w.
4. If there is no such unique choice, do not decode by this procedure.

⋆ A zero syndrome means that the received word is a code word. It does not prove that no error occurred: a nonzero error vector that is itself a code word has zero syndrome.

The *Hamming* $(7,4)$ *code* has standard generator and parity-check matrices

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}, \qquad H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The rows of H are precisely the seven nonzero binary triples. This code has minimum distance 3 and corrects every single error. For example, 1000 is encoded as 1000110. If 1100110 is received, its syndrome is 101, the second row of H, so the second component is corrected.

28.3 Coset Decoding

The code C is a subgroup of the additive group F^n. Hence, the cosets of C partition all possible received words.

Definition. A *coset leader* is a vector of minimum Hamming weight in its coset. A *standard array* lists C as its first row, with 0 first, and each other coset as a row $e + C$, with its chosen leader e first and $e + c$ beneath the code word c.

⋆ For a code over a field of order q, the standard array has q^{n-k} rows and q^k columns. A coset may have several vectors of minimum weight; one must choose a leader.

Definition. In *coset decoding*, a received word $w = e + c$ in the row with leader e is decoded as $c = w - e$.

Theorem. Coset decoding is nearest-neighbor decoding: the selected code word has minimum distance from the received word.

Theorem. Two vectors belong to the same coset of C if and only if they have the same syndrome; i.e.,

$$u + C = v + C \iff uH = vH\,.$$

Thus, the standard array can be replaced by a table of syndromes and their coset leaders:

1. Compute the syndrome wH.
2. Look up the leader e with $eH = wH$.
3. Decode w as $w - e$.

⋆ Algebraically, the syndrome map $F^n \to F^{n-k}$ is an onto linear mapping with kernel C. The first isomorphism theorem gives $F^n/C \cong F^{n-k}$ as additive groups (and as vector spaces).

> "Damn it, if the machine can detect an error, why can't it locate the position of the error and correct it?"
>
> — Richard W. Hamming

29 An Introduction To Galois Theory

ft. Évariste Galois, Niels Abel

29.1 Automorphisms and Fixed Fields

Definition. A *field automorphism* of a field E is a ring isomorphism from E onto itself. If $F \subseteq E$, the *Galois group of E over F* is

$$\mathsf{Gal}(E/F) = \{\phi \in \mathsf{Aut}(E) : \phi(a) = a \ \forall a \in F\}.$$

Definition. If $H \leq \mathsf{Gal}(E/F)$, the *fixed field of H* is

$$E^H = \{a \in E : \phi(a) = a \ \forall \phi \in H\}.$$

Theorem. $\mathsf{Gal}(E/F)$ is a group under function composition, and E^H is a subfield of E containing F.

$\star$ The slash in E/F denotes an extension, not a factor ring. An automorphism in $\mathsf{Gal}(E/F)$ fixes F *pointwise*, not merely as a set.

Theorem. Let $f(x) \in F[x]$ and let $a \in E$ be a zero of $f(x)$. If $\phi \in \mathsf{Gal}(E/F)$, then $\phi(a)$ is also a zero of $f(x)$.

Corollary. If E is the splitting field of a polynomial with n distinct zeros over F, then $\mathsf{Gal}(E/F)$ is isomorphic to a subgroup of S_n.

$\star$ An automorphism of $F(a_1, \ldots, a_n)$ fixing F is completely determined by its values on the a_is. These values must preserve every algebraic relation among the generators; an arbitrary permutation of the zeros need not extend to an automorphism.

For example, $\mathsf{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}_2$, with the nonidentity automorphism sending $\sqrt{2}$ to $-\sqrt{2}$. However, $\mathsf{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is trivial: the other two zeros of $x^3 - 2$ are not in this real field.

29.2 Fundamental Theorem of Galois Theory

Theorem. *Fundamental thm of Galois Theory.* Let F have characteristic 0 or be a finite field, and let E be the splitting field of a nonconstant polynomial in $F[x]$. Put $G = \mathsf{Gal}(E/F)$. There is an inclusion-reversing bijection

$$K \longmapsto \mathsf{Gal}(E/K), \qquad H \longmapsto E^H$$

between the intermediate fields $F \subseteq K \subseteq E$ and the subgroups $H \leq G$. Moreover,

1) $[E : K] = |\mathsf{Gal}(E/K)|$.
2) $[K : F] = |G : \mathsf{Gal}(E/K)|$.
3) $K = E^{\mathsf{Gal}(E/K)}$.

4) $H = \mathsf{Gal}(E/E^H)$.

5) If K is a splitting field over F, then $\mathsf{Gal}(E/K) \triangleleft G$, and

$$\mathsf{Gal}(K/F) \cong G/\mathsf{Gal}(E/K)\,.$$

⋆ The isomorphism in property 5 comes from restriction: $\phi \mapsto \phi|_K$. Its kernel consists of the automorphisms fixing K pointwise.

Corollary. Under the hypotheses of the theorem, $|\mathsf{Gal}(E/F)| = [E : F]$ and $E^G = F$.

The correspondence turns the subgroup lattice upside down. A larger subgroup imposes more conditions on a fixed element, and therefore has a smaller fixed field. Degrees of field extensions correspond to indices of subgroups.

Definition. An algebraic extension E/F is *normal* if every irreducible polynomial in $F[x]$ with a zero in E splits over E. It is *separable* if the minimal polynomial of every element of E has distinct zeros. An extension that is both normal and separable is called *Galois*.

⋆ The fundamental theorem holds for every finite Galois extension. The hypotheses above ensure normality because E is a splitting field, and separability because F is perfect. More generally, under the correspondence,

$$H \triangleleft G \iff E^H/F \text{ is Galois}\,,$$

and then $\mathsf{Gal}(E^H/F) \cong G/H$.

For $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, the signs of the two square roots can be changed independently, so $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Its three subgroups of order 2 correspond to the three quadratic intermediate fields

$$\mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(\sqrt{3}), \quad \mathbb{Q}(\sqrt{6})\,.$$

These are all the proper intermediate fields.

Theorem. Let q be a prime power. Then,

$$\mathsf{Gal}(\mathrm{GF}(q^n)/\,\mathrm{GF}(q)) = \langle\phi\rangle \cong \mathbb{Z}_n, \qquad \phi(a) = a^q\,.$$

⋆ The automorphism ϕ is called the *Frobenius automorphism* over $\mathrm{GF}(q)$. For each divisor d of n, the subgroup $\left\langle \phi^d \right\rangle$ has order n/d and fixed field $\mathrm{GF}(q^d)$.

29.3 Solvability by Radicals

Definition. A polynomial $f(x) \in F[x]$ is *solvable by radicals over* F if it splits in an extension $F(a_1, a_2, \ldots, a_t)$, where

$$a_1^{n_1} \in F, \qquad a_i^{n_i} \in F(a_1, \ldots, a_{i-1}) \quad (2 \le i \le t)$$

for positive integers $n_1, \ldots, n_t$.

This formalizes obtaining the zeros by a finite number of field operations and extractions of roots, starting with elements of F.

Definition. A group G is *solvable* if there is a finite series

$$\{e\} = H_0 \triangleleft H_1 \triangleleft \ldots \triangleleft H_k = G$$

such that H_{i+1}/H_i is Abelian for every i.

$\star$ Each H_i need only be normal in H_{i+1}; it need not be normal in all of G.

Theorem. Abelian groups, dihedral groups, and finite groups of prime-power order are solvable.

Theorem. A subgroup or factor group of a solvable group is solvable.

Theorem. If $N \triangleleft G$ and both N and G/N are solvable, then G is solvable.

Corollary. A finite group is solvable if and only if all its composition factors are cyclic groups of prime order.

Corollary. A non-Abelian simple group is not solvable. In particular, A_5 and S_5 are not solvable.

Theorem. Let F be a field of characteristic 0 and let $a \in F$. If E is the splitting field of $x^n - a$ over F, then $\mathsf{Gal}(E/F)$ is solvable.

Theorem. *Galois.* Let F have characteristic 0, let $f(x) \in F[x]$ be nonconstant, and let E be its splitting field over F. Then, $f(x)$ is solvable by radicals over F if and only if $\mathsf{Gal}(E/F)$ is solvable.

$\star$ This is the connection between solving polynomial equations and the structure of groups. The quadratic, cubic, and quartic formulas correspond to the solvability of subgroups of S_2, S_3, and S_4.

29.4 Insolvability of a Quintic

Theorem. The polynomial $f(x) = 3x^5 - 15x + 5$ is not solvable by radicals over $\mathbb{Q}$.

Proof sketch. Let E be its splitting field over $\mathbb{Q}$ and let $G = \mathsf{Gal}(E/\mathbb{Q}) \leq \mathsf{S}_5$.

1. Eisenstein's criterion with $p = 5$ shows that $f(x)$ is irreducible. Hence, $5 \mid [E : \mathbb{Q}] = |G|$, and Cauchy's theorem gives a 5-cycle in G.
2. The values of f at $-2, -1, 0, 1, 2$ show that it has a zero in each of $(-2, -1)$, $(0, 1)$, and $(1, 2)$. Since $f'(x) = 15(x^4 - 1)$ has only two real zeros, Rolle's theorem shows that f has exactly three real zeros.
3. Complex conjugation fixes these three zeros and interchanges the remaining two. Thus, G contains a 2-cycle.
4. A 5-cycle together with any 2-cycle generates S_5. Consequently, $G = \mathsf{S}_5$, which is not solvable.

⋆ The fourth step can be seen by conjugating the 2-cycle by powers of the 5-cycle. The resulting transpositions connect all five symbols, and the transpositions along a connected graph generate its full symmetric group.

⋆ There is no formula by radicals for the general quintic. Particular quintics can still be solvable by radicals; for example, $x^5 - 2$ is.

> "Seeing much, suffering much, and studying much are the three pillars of learning."
>
> — Benjamin Disraeli

30 Cyclotomic Extensions

ft. Carl Friedrich Gauss

30.1 Cyclotomic Polynomials

Definition. Let $\omega = e^{2\pi\iota/n}$ be a primitive n^{th} root of unity. The field $\mathbb{Q}(\omega)$ is called the n^{th} *cyclotomic extension* of $\mathbb{Q}$.

Definition. The n^{th} *cyclotomic polynomial* is

$$\Phi_n(x) = \prod_{\substack{1\le k\le n\\ \gcd(k,n)=1}} (x - \omega^k)\,.$$

⋆ The primitive n^{th} roots of unity are precisely the generators of the cyclic group $\langle\omega\rangle$. Thus, $\Phi_n(x)$ is monic of degree $\varphi(n)$.

Theorem. For every positive integer n,

$$x^n - 1 = \prod_{d|n} \Phi_d(x)\,,$$

where the product runs over the positive divisors of n.

Corollary. $\sum_{d|n} \varphi(d) = n$.

Theorem. $\Phi_n(x) \in \mathbb{Z}[x]$ for every positive integer n.

The factorization theorem gives the recursive formula

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n\\ d<n}} \Phi_d(x)}\,.$$

For instance,

$$\Phi_1(x) = x - 1, \quad \Phi_2(x) = x + 1, \quad \Phi_3(x) = x^2 + x + 1, \quad \Phi_4(x) = x^2 + 1\,,$$

and

$$\Phi_6(x) = \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1\,.$$

Corollary. If p is prime and $k \geq 1$, then

$$\Phi_{p^k}(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \ldots + x^{(p-1)p^{k-1}}\,.$$

Theorem. *Gauss.* $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ (and over $\mathbb{Z}$).

Proof sketch. Let $f(x)$ be a monic irreducible factor of $\Phi_n(x)$ with $f(\omega) = 0$, and write $x^n - 1 = f(x)g(x)$ in $\mathbb{Z}[x]$. If $p \nmid n$ is prime and $f(\omega^p) \neq 0$, then $g(\omega^p) = 0$, so $f(x) \mid g(x^p)$. Reducing modulo p gives $\overline{f}(x) \mid \overline{g}(x)^p$. Hence, $\overline{f}$ and $\overline{g}$ have a common irreducible factor, forcing a repeated factor of $x^n - 1$ modulo p. But $x^n - 1$ is relatively prime to its derivative nx^{n-1} since $p \nmid n$. This contradiction shows that $f(\omega^p) = 0$. Iterating over prime factors of integers relatively prime to n shows that every primitive n^{th} root is a zero of f, so $f = \Phi_n$.

Corollary. $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$, and $\left\{1, \omega, \ldots, \omega^{\varphi(n)-1}\right\}$ is a basis for $\mathbb{Q}(\omega)$ over $\mathbb{Q}$.

⋆ Reduction modulo a prime may make a cyclotomic polynomial reducible. For example, over $\mathbb{Z}_2$,

$$x^6 - 1 = (x+1)^2(x^2+x+1)^2\,,$$

whereas over $\mathbb{Z}_3$,

$$x^6 - 1 = (x-1)^3(x+1)^3\,.$$

30.2 Galois Groups of Cyclotomic Extensions

Theorem. Let $n \geq 2$ and let ω be a primitive n^{th} root of unity. Then,

$$\mathsf{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong U(n)\,.$$

The isomorphism sends $k \in U(n)$ to the automorphism ϕ_k given by $\phi_k(\omega) = \omega^k$.

Corollary. Every intermediate field of $\mathbb{Q}(\omega)/\mathbb{Q}$ is Galois over $\mathbb{Q}$.

⋆ This follows because $U(n)$ is Abelian, so every subgroup is normal. In particular, cyclotomic extensions have solvable Galois groups.

For example,

$$\mathsf{Gal}(\mathbb{Q}(e^{2\pi\iota/9})/\mathbb{Q}) \cong U(9) \cong \mathbb{Z}_6\,,$$

and

$$\mathsf{Gal}(\mathbb{Q}(e^{2\pi\iota/15})/\mathbb{Q}) \cong U(15) \cong \mathbb{Z}_4 \times \mathbb{Z}_2\,.$$

30.3 The Constructible Regular n-gons

Lemma. If $\omega = e^{2\pi\iota/n}$, then

$$\cos\frac{2\pi}{n} = \frac{\omega + \omega^{-1}}{2} \in \mathbb{Q}(\omega)\,.$$

Theorem. For $n \geq 3$, the fixed field of complex conjugation in $\mathbb{Q}(\omega)$ is

$$\mathbb{Q}(\omega) \cap \mathbb{R} = \mathbb{Q}(\omega + \omega^{-1}) = \mathbb{Q}\left(\cos\frac{2\pi}{n}\right).$$

Its degree over $\mathbb{Q}$ is $\varphi(n)/2$.

Definition. A prime of the form $2^{2^r} + 1$, where $r \geq 0$, is called a *Fermat prime*.

Theorem. *Gauss–Wantzel.* For $n \geq 3$, a regular n-gon is constructible with an unmarked straightedge and compass if and only if

$$n = 2^k p_1 p_2 \dots p_t\,,$$

where $k \geq 0$ and the p_is are distinct Fermat primes. Equivalently, $\varphi(n)$ is a power of 2.

Proof sketch. A regular n-gon is constructible iff $\cos(2\pi/n)$ is constructible.

1. If it is constructible, the degree condition for constructible numbers shows that $\varphi(n)/2$ is a power of 2. Write $n = 2^k \prod_i p_i^{a_i}$ with the p_is distinct odd primes. Since

$$\varphi(n) = \varphi(2^k) \prod_i p_i^{a_i - 1}(p_i - 1)\,,$$

   each $a_i = 1$ and each $p_i - 1$ is a power of 2. If $2^m + 1$ is prime, then m is itself a power of 2, giving the required form.

2. Conversely, suppose $\varphi(n)$ is a power of 2. The real field $K = \mathbb{Q}(\cos(2\pi/n))$ is Galois over $\mathbb{Q}$ with an Abelian group of order $\varphi(n)/2$. A series of subgroups with successive index 2 corresponds to a tower from $\mathbb{Q}$ to K with successive degree 2. Each step is obtained by adjoining a square root. Hence, every element of K, in particular $\cos(2\pi/n)$, is constructible.

⋆ For example, the regular 17-gon is constructible because $17 = 2^{2^2} + 1$ is prime. The regular 7-gon is not constructible because $\varphi(7) = 6$, and the regular 9-gon is not constructible because $\varphi(9) = 6$. Repeated odd prime factors are not permitted.

"Difficulties should act as a tonic. They should spur us to greater exertion."

— B. C. Forbes