Note for Abstract Algebra

Xin Ye
Purdue University

January 3, 2014

1 Introduction to Groups

1.1 Basic Axioms and Examples

Definition.

(1) A *binary operation* $\star$ on a set G is a function $\star$: $G \times G \to G$. For any $a, b \in G$ we shall write $a \star b$ for $\star(a, b)$.

(2) A binary operation $\star$ on a set G is *associative* if for all $a, b, c \in G$ we have $a \star (b \star c) = (a \star b) \star c$.

(3) If $\star$ is a binary operation on a set G we say element a and b of G *commute* if $a \star b = b \star a$. We say $\star$(or G) is *commutative* if for all $a, b \in G, a \star b = b \star a$.

Definition.

(1) A *group* is an ordered pair $(G, \star)$ where G is a set and $\star$ is a binary operation on G satisfying the following axioms:

(i) $a \star (b \star c) = (a \star b) \star c$, for all $a, b, c \in G$, i.e., $\star$ is *associative*,

(ii) there exists an element e in G, called an *identity* of G, such that for all $a \in G$ we have $a \star e = e \star a = a$,

(iii) for each $a \in G$ there is an element a^{-1} of G, called an *inverse* of a, such that $a \star a^{-1} = a^{-1} \star a = e$.

(2) The group $(G, \star)$ is called *abelian* (or *commutative*) if $a \star b = b \star a$ for all $a, b \in G$.

Proposition 1. If G is a group under the operation $\star$, then

(1) the identity of G is unique

(2) for each $a \in G$, a^{-1} is uniquely determined

(3) $(a^{-1})^{-1} = a$ for all $a \in G$

(4) $(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$

(5) for any $a_1, a_2, \ldots, a_n \in G$ the value of $a_1 \star a_2 \star \cdots \star a_n$ is independent of how the expression is bracketed (this is called the $generalized\ associative\ law$).

Proposition 2. Let G be a group and let $a, b \in G$. The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, the left and right cancellation laws holds in G, i.e.,

(1) if $au = av$, then $u = v$, and

(2) if $ub = vb$, then $u = v$.

Definition. For G a group and $x \in G$ define the *order* of x to be the smallest positive integer n such that $x^n = 1$, and denote this integer by $|x|$. In this case x is said to be of order n. If no positive power of x is the identity, the order of x is defined to be infinity and x is said to be of infinite order.

Definition. Let $G = \{g_1, g_2, \ldots g_n\}$ be a finite group with $g_1 = 1$. The *multiplication table* or *group table* of G is the $n \times n$ matrix whose i, j entry is the group element $g_i g_j$.

1.2 Dihedral Groups

1.3 Symmetric Groups

1.4 Matrix Groups

Definition.

(1) A *field* is a set F together with two binary operations + and $\cdot$ on F such that $(F, +)$ is an abelian group (call its identity 0) and $(F - \{0\}, \cdot)$ is also an abelian group, and the following *distributive* law holds:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \text{ for all } a, b, c \in F.$$

(2) For any field F let $F^\times = F - \{0\}$.

1.5 The Quaternion Group

1.6 Homomorphisms and Isomorphisms

Definition. Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\varphi : G \to H$ such that

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y), \text{ for all} x, y \in G$$

is called a *homomorphism*.
Definition. The map $\varphi : G \to H$ is called an *isomorphism* and G and H are said to be *isomorphic* or of the same *isomorphism type*, written $G \cong H$, if

(1) φ is a homomorphism (i.e., $\varphi(xy) = \varphi(x)\varphi(y)$), and

(2) φ is a bijection.

1.7 Group Actions

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

(1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G$, $a \in A$, and

(2) $1 \cdot a = a$, for all $a \in A$.

2 Subgroups

2.1 Definition and Examples

Definition. Let G be a group. The subset H of G is a *subgroup* of G if H is nonempty and H is closed under products and inverses (i.e., $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$.
Proposition 1. *(The Subgroup Criterion)* A subset H of a group G is a subgroup if and only if

(1) $H \neq \emptyset$, and

(2) for all $x, y \in H$, $xy^{-1} \in H$.

Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

2.2 Centralizers and Normalizers, Stabilizers and Kernels

Definition. Define $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the *centralizer* of A in G. Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of elements in G which commute with every element of A.
Definition. Define $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$, the set of elements commuting with all the elements of G. This subset of G is called the *center* of G.
Definition. Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. define the *normalizer* of A in G to be the set $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$.

2.3 Cyclic Groups and Cyclic Subgroups

Definition. A group H is *cyclic* if H can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n \mid n \in \mathbb{Z}\}$ (where as usual the operation is multiplication).
Proposition 2. If $H = \langle x \rangle$, then $|H| = |x|$ (where if one side of this equality is infinite, so is the other). More specifically

(1) if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all the distinct elements of H, and

(2) if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$ in $\mathbb{Z}$.

Proposition 3. Let G be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, the $x^d = 1$, there $d = (m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m.
Proposition 4. Any two cyclic groups of the same order are isomorphic. More specifically,

(1) if $n \in \mathbb{Z}^+$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, then the map

$$\begin{aligned} \varphi : \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$

is well defined and is an isomorphism.

(2) if $\langle x \rangle$ is an infinite cyclic group, the map

$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$

is well defined and is an isomorphism.

Proposition 5. Let G be a group. Let $x \in G$ and let $a \in \mathbb{Z} - \{0\}$.

(1) If $|x| = \infty$, then $|x^a| = \infty$.

(2) If $|x| = n < \infty$, then $|x^a| = \dfrac{n}{(n, a)}$.

(3) In particular, if $|x| = n < \infty$ and a is a positive integer dividing n, then $|x^a| = \dfrac{n}{a}$.

Proposition 6. Let $H = \langle x \rangle$.

(1) Assume $|x| = \infty$. Then $H = \langle x^a \rangle$ if and only if $a = \pm 1$.

(2) Assume $|x| = n < \infty$. Then $H = \langle x^a \rangle$ if and only if $(a, n) = 1$. In particular, the number of generators of H is $\varphi(n)$ (where φ is Euler's φ-function).

Theorem 7. Let $H = \langle x \rangle$ be a cyclic group.

(1) Every subgroup of H is cyclic. More precisely, if $K \leq H$, then $K = \{1\}$ or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.

(2) If $|H| = \infty$, then for any distinct nonnegative integers a and b, $\langle x^a \rangle \neq \langle x^b \rangle$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{|m|} \rangle$, where $|m|$ denotes the absolute value of m, so that the nontrivial subgroups of H correspond bijectively with the integers $1, 2, 3, \ldots$.

(3) If $|H| = n < \infty$, then for each positive integer a dividing n there is a unique subgroup of H of order a. This subgroup is the cyclic group $\langle x^d \rangle$, where $d = \dfrac{n}{a}$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, so that the subgroups of H correspond bijectively with the positive divisors of n.

2.4 Subgroups Generated by Subsets of a Group

Proposition 8. If $\mathcal{A}$ is any nonempty collection of subgroups of G, then the intersection of all members of $\mathcal{A}$ is also a subgroups of G.
Definition. If A is any subset of the group G define

$$\langle A\rangle = \bigcap_{\substack{A\subseteq H\\ H\leq G}} H$$

This is called the *subgroup of G generated by A*
Proposition 9. $\bar{A} = \langle A\rangle$.

2.5 The Lattice of Subgroups of a group

3 Quotient Groups and Homomorphisms

3.1 Definitions and Examples

Definition. If φ is a homomorphism $\varphi : G \to H$, the *kernel* of φ is the set

$$\{g \in G \mid \varphi(g) = 1\}$$

and will be denoted by kerφ (here 1 is the identity of H).
Proposition 1. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism.

(1) $\varphi(1_G) = 1_H$, where 1_G and 1_H are the identities of G and H, respectively.

(2) $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.

(3) $\varphi(g^n) = \varphi(g)^n$ for all $n \in \mathbb{Z}$.

(4) kerφ is a subgroup of G.

(5) im(φ), the image of G under φ, is a subgroup of H.

Definition. Let $\varphi : G \to H$ be a homomorphism with kernel K. The *quotient group* or *factor group*, G/K (read G *modulo* K or simply G *mod* K), is the group whose elements are the fibers of φ with group operation defined above: namely if X is the fiber above a and Y is the fiber above b then the product of X with Y is defined to be the fiber above the product ab.
Proposition 2. Let $\varphi : G \to H$ be a homomorphism of groups with kernel K. Let $X \in G/K$ be the fiver above a, i.e., $X = \varphi^{-1}(a)$. Then

(1) For any $u \in X$, $X = \{uk \mid k \in K\}$

(2) For any $u \in X$, $X = \{ku \mid k \in K\}$.

Definition. For any $N \leq G$ and any $g \in G$ let

$$gN = \{gn \mid n \in N\} \text{ and } Ng = \{ng \mid n \in N\}$$

called respectively a *left coset* and a *right coset* of N in G. Any element of a coset is called a *representative* for the coset.
Theorem 3. Let G be a group and let K be the kernel of some homomorphism from G to another group. Then the set whose element are the left cosets of K in G with operation defined by

$$uK \diamond vK = (uv)K$$

forms a group, G/K. In particular, this operation is well defined in the sense that if $u_1$is any element in uK and v_1 is any element in vK, then $u_1v_1 \in uvK$, i.e., $u_1v_1K = uvK$ so that the multiplication does not depend on the choice of representatives for the cosets. The same statement is true with "right coset" in place of "left coset".
Proposition 4. Let N be any subgroup of the group G. The set of left cosets of N in G form a partition of G. Furthermore, for all $u, v \in G$, $uN = vN$ if and only if $v^{-1}u \in N$ and in particular, $uN = vN$ if and only if u and v are representatives of the same coset.
Proposition 5. Let G be a group and let N be a subgroup of G.

(1) The operation on the set of left cosets of N in G described by

$$uN \cdot vN = (uv)N$$

is well defined if and only if $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$.

(2) If the above operation is well defined, then it makes the set of left cosets of N in G into a group. In particular the identity of this group is the coset $1N$ and the inverse of gN is the coset $g^{-1}N$ i.e., $(gN)^{-1} = g^{-1}N$.

Definition. The element gng^{-1} is called the *conjugate* of $n \in N$ by g. The set $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is called the *conjugate* of N by g. The element g is said to *normalize* N if $gNg^{-1} = N$. A subgroup N of a group G is called normal if every element of G normalizes N, i.e., if $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup of G we shall write $N \trianglelefteq G$.
Theorem 6. Let N be a subgroup of the group G. The following are equivalent:

(1) $N \trianglelefteq G$

(2) $N_G(N) = G$ (recall $N_G(N)$ is the normalizer in G of N)

(3) $gN = Ng$ for all $g \in G$

(4) the operation on left cosets of N in G described in Proposition 5 makes the set of left cosets into a group

(5) $gNg^{-1} \subseteq N$ for all $g \in G$.

Theorem 7. A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism.
Definition. Let $N \trianglelefteq G$. The homomorphism $\pi : G \to G/N$ defined by $\pi(g) = gN$ is called the *natural projection (homomorphism)* of G onto G/N. If $\bar{H} \leq G/N$ is a subgroup of G/N, the *complete preimage* of $\bar{H}$ in G is the preimage of $\bar{H}$ under the natural projection homomorphism.

3.2 More on Cosets and Lagrange's Theorem

Theorem 8. *(Lagrange's Theorem)* If G is a finite group and H is a subgroup of G, then the order of H divides the order of G (i.e., $|H| \mid |G|$) and the number of left cosets of H in G equals $\dfrac{|G|}{|H|}$.
Definition. If G is a group (possibly infinite) and $H \leq G$, the number of left cosets of H in G is called the index of H in G and is denoted by $|G : H|$.
Corollary 9. If G is a finite group and $x \in G$, then the order of x divides the order of G. In particular $x^{|G|} = 1$ for all x in G.
Corollary 10. If G is a group of prime order p, then G is cyclic, hence $G \cong Z_p$.
Theorem 11. *(Cauchy's Theorem)* If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.
Theorem 12. (Sylow) If G is a finite group of order $p^\alpha m$, where p is a prime and p dose not divide m, then G has a subgroup of order p^α.
Definition. Let H and K be subgroups of a group and define

$$HK = \{hk \mid h \in H,\ k \in K\}$$

Proposition 13. If H and K are finite subgroups of a group then

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

Proposition 14. If H and K are subgroups of a group, HK is a subgroup if and only if $HK = KH$.
Corollary 15. If H and K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G. In particular, if $K \trianglelefteq G$ then $HG \leq G$ for any $H \leq G$.
Definition. If A is any subset of $N_G(K)$ (or $C_G(K)$), we shall say A *normalizes* K (*centralizes* K, respectively).

3.3 The Isomorphism Theorems

Theorem 16. *(The First Isomorphism Theorem)* If $\varphi : G \to H$ is a homomorphism of groups, then $\ker\varphi \trianglelefteq G$ and $G/\ker\varphi \cong \varphi(G)$.
Corollary 17. Let $\varphi : G \to H$ be a homomorphism of groups.

(1) φ is injective if and only if $\ker\varphi = 1$.

(2) $|G : \ker\varphi| = |\varphi(G)|$.

Theorem 18. *(The Second or Diamond Isomorphism Theorem)* Let G be a group, let A and B be subgroups of G and assume $A \leq N_G(B)$. Then AB is a subgroup of G, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.
Theorem 19. *(The Third Isomorphism Theorem)* Let G be a group and let H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and

$$(G/H)/(K/H) \cong G/K$$

Theorem 20. *(The Fourth or Lattice Isomorphism Theorem)* Let G be a group and let N be a normal subgroup of G. Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\overline{A} = A/N$ of G/N. In particular, every subgroup of $\overline{G}$ is of the form A/N for some subgroup A of G containing N (namely, its preimage in G under the natural projection homomorphism from G to G/N). This bijection has the following properties: for all $A, B \leq G$ with $N \leq A$ and $N \leq B$,

(1) $A \leq B$ if and only if $\overline{A} \leq \overline{B}$,

(2) if $A \leq B$, then $|B : A| = \left|\overline{B} : \overline{A}\right|$,

(3) $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$,

(4) $\overline{A \cap B} = \overline{A} \cap \overline{B}$, and

(5) $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$.

3.4 Composition Series and the Hölder Program

Proposition 21. If G is a finite abelian group and p is a prime dividing $|G|$, then G contains an element of order p.
Definition. A (finite or infinite) group G is called *simple* if $|G| > 1$ and the only normal subgroup of G are 1 and G.
Definition. In a group G a sequence of subgroups

$$1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{k-1} \leq N_k = G$$

is called a *composition series* if $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is a simple group, $0 \leq i \leq k-1$. If the above sequence is a composition series, the quotient groups N_{i+1}/N_i are called *composition factors* of G.
Theorem 22. (Jordan-Hölder) Let G be a finite group with $G \neq 1$. Then

(1) G has a composition series and

(2) The composition factors in a composition series are unique, namely, if $1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{k-1} \leq N_r = G$ and $1 = M_0 \leq M_1 \leq M_2 \leq \cdots \leq M_{k-1} \leq M_s = G$ are two composition series for G, then $r = s$ and there is permutation, π, of $1, 2, \ldots, r$ such that

$$M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1},\ 1 \leq i \leq r$$

The Hölder Prgram
Theorem. There is a list consisting of 18 (infinite) families of simple groups and 26 simple groups not belonging to these families (the *sporadic* simple groups) such that every finite simple group is isomorphic to one of the groups in the list.
Theorem. (Feit-Thompson) If G is a simple group of odd order, then $G \cong Z_p$ for some prime p.
Definition. A group of G is *solvable* if there is a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = G$$

such that G_{i+1}/G_i is abelian for $i = 0, 1, \ldots, s-1$.
Theorem. The finite group G is solvable if and only if for every divisor n of $|G|$ such that $(n, \frac{|G|}{n}) = 1$, G has a subgroup of order n.

3.5 Transpositions and the Alternating Group

Transpositions and Generation of S_n
Definition. A 2-cycle is called a *transposition*.

every element of S_n may be written as a product of transpositions

The Alternating Group
Definition.

(1) $\epsilon(\sigma)$ is called the *sign* of σ.

(2) σ is called an *even permutation* if $\epsilon(\sigma) = 1$ and an *odd permutation* if $\epsilon(\sigma) = -1$.

Proposition 23. The map $\epsilon : S_n \to \{\pm 1\}$ is a homomorphism (where $\{\pm 1\}$ is a multiplicative version of the cyclic group of order 2).
Proposition 24. Transpositions are all odd permutations and ϵ is a surjective homomorphism.
Definition. The *alternating group of order* n, denoted by A_n, is the kernel of the homomorphism ϵ (i.e., the set of even permutations).

an m-cycle is an odd permutation if and only if m is even.

Proposition 25. The permutation σ is odd if and only if the number of cycles of even length in its cycle decomposition is odd.

A_n is non-abelian simple group for all $n \geq 5$.

4 Group Actions

4.1 Group Actions and Permutation Representations

Definition.

(1) The *kernel* of the actioin is the set of elements of G that act trivially on every element of A: $\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$.

(2) For each $a \in A$ the *stabilizer* of a in G is the set of elements of G that fix the element a: $\{g \in G \mid g \cdot a = a\}$ and is denoted by G_a.

(3) An action is *faithful* if its kernel is the identity.

Proposition 1. For any group G and any nonempty set A there is a bijection between the actions of G on A and the homomorphisms of G into S_A.
Definition. If G is a group, a *permutation representation* of G is any homomorphism of G into the symmetric group S_A for some nonempty set A. We shall say a given action of G on A *affords* or *induces* the associated permutation representation of G.
Proposition 2. Let G be a group acting on the nonempty set A. The relation on A defined by

$$a \sim b \text{ in and only if } a = g \cdot b \text{ for some } g \in G$$

is an equivalence relation. For each $a \in A$, the number of elements in the equivalence class containing a is $|G : G_a|$, the index of the stabilizer of a.
Definition. Let G be a group acting on the nonempty set A.

(1) The equivalence class $\{g \cdot a \mid g \in G\}$ is called the *orbit* of G containing a.

(2) The action of G on A is called *transitive* if there is only one orbit, i.e., given any two elements $a, b \in A$ there is some $g \in G$ such that $a = g \cdot b$.

4.2 Groups Acting on Themselves by Left Multiplication–Cayley's Theorem

Theorem 3. Let G be a group, let H be a subgroup of G and let G act by left multiplication on the set A of left cosets of H in G. Let π_H be the associated permutation representation afforded by this action. Then

(1) G acts transitively on A

(2) the stabilizer in G of the point $1H \in A$ is the subgroup H

(3) the kernel of the action (i.e., the kernel of π_H) is $\cap_{x \in G} xHx^{-1}$, and kerπ_H is the largest normal subgroup of G contained in H.

Corollary 4. *(Cayley's Theorem)* Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n, then G is isomorphic to a subgroup of S_n.
Corollary 5. If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.

4.3 Groups Acting on Themselves by Conjugation–The Class Equation

Definition. Two elements a and b of G are said to be *conjugate in* G if there is some $g \in G$ such that $b = gag^{-1}$ (i.e., if and only if they are in the same orbit of G acting on itself by conjugation). The orbits of G acting on itself by conjugation are called the *conjugacy classed of* G.
Definition. Two subsets S and T of G are said to be *conjugate in* G if there is some $g \in G$ such that $T = gSg^{-1}$ (i.e., if and only if they are in the same orbit of G acting on its subsets by conjugation).
Proposition 6. The number of conjugates of a subset S in a group G is the index of the normalizer of S, $|G : N_G(S)|$. In particular, the number of conjugates of an element s of G is the index of the centralizer of s, $|G : C_G(s)|$.
Theorem 7. *(The Class Equation)* Let G be a finite group and let $g_1, g_2, \ldots, g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$

Theorem 8. If p is a prime and P is a group of prime power order p^α for some $\alpha \leq 1$, then P has a nontrivial center: $Z(P) \neq 1$.
Corollary 9. If $|P| = p^2$ for some prime p, then P is abelian. More precisely, P is isomorphic to either Z_{p^2} or $Z_p \times Z_p$.
Proposition 10. Let σ, τ be elements of the symmetric group S_n and suppose σ has cycle decompostion

$$(a_1 a_2 \ldots a_{k_a})(b_1 b_2 \ldots b_{k_2}) \ldots$$

Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a_1)\tau(a_2)\ldots\tau(a_{k_1}))(\tau(b_1)\tau(b_2)\ldots\tau(b_{k_2}))\ldots$$

that is, $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each entry i in the cycle decomposition for σ by the entry $\tau(i)$.
Definition.

(1) If $\sigma \in S_n$ is the product of disjoint cycles of lengths $n_1, n_2, \ldots, n_r$ with $n_1 \leq n_2 \leq \cdots \leq n_r$ (including its 1-cycles) then the integers $n_1, n_2, \ldots, n_r$ are called the *cycle type* of σ.

(2) If $n \in \mathbb{Z}^+$, a *partition* of n is any nondecreasing sequence of positive integers whose sum is n.

Proposition 11. Two elements of S_n are conjugate in S_n if and only if they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n.
Theorem 12. A_5 is a simple group.

4.4 Automorphisms

Definition. Let G be a group. An isomorphism from G onto itself is called an *automorphism* of G. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$.
Proposition 13. Let H be a normal subgroup of the group G. Then G acts by conjugation on H as automorphisms of H. More specifically, the action of G on H by conjugation is defined for each $g \in G$ by

$$h \mapsto ghg^{-1} \text{ for each } h \in H.$$

For each $g \in G$, conjugation by g is an automorphism of H. The permutation representation afforded by is a homomorphism of G into $\mathrm{Aut}(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.
Corollary 14. If K is any subgroup of the group G and $g \in G$, then $K \cong gKg^{-1}$. Conjugate elements and conjugate subgroups have the same order.
Corollary 15. For any subgroup H of a group G, the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$.
Definition. Let G be a group and let $g \in G$. Conjugation by g is called an *inner automorphism* of G and the subgroup of $\mathrm{Aut}(G)$ consisting of all inner automorphisms is denoted by $\mathrm{Inn}(G)$.

By Corollary 15, $\mathrm{Inn}(G) \cong G/Z(G)$.
Definition. A subgroup H of a group G is called *characteristic* in G, denoted H char G, if every automorphism of G maps H to itself, i.e., $\sigma(H) = H$ for all $\sigma \in \mathrm{Aut}(G)$.

Results concerning characteristic subgroups are

(1) characteristic subgroups are normal,

(2) if H is the unique subgroup of G of a given order, then H is characteristic in G, and

(3) if K char H and $H \trianglelefteq G$, then $K \trianglerighteq G$ (so although "normality" is not transitive property, a characteristic subgroup of a normal subgroup is normal).

Proposition 16. The automorphism group of the cyclic group of order n is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, an abelian group of order $\phi(n)$ (where ϕ is Euler's function).
Proposition 17.

(1) If p is an odd prime and $n \in \mathbb{Z}^+$, then the automorphism group of the cyclic group of order p is cyclic of order $p-1$. More generally, the automorphism group of the cyclic group of order p^n is cyclic of order $p^{n-1}(p-1)$ (cf. Corollary 20, Section 9.5).

(2) For all $n \geq 3$ the automorphism group of the cyclic group of order 2^n is isomorphic to $Z_2 \times Z_{2^{n-2}}$, and in particular is not cyclic but has a cyclic subgroup of index 2 (cf. Corollary 20, Section 9.5).

(3) Let p be a prime and let V be an abelian group (written additively) with the property that $pv = 0$ for all $v \in V$. If $|V| = p^n$, then V is an n-dimensional vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The automorphisms of V are precisely the nonsingular linear transformations from V to itself, that is

$$\text{Aut}(V) \cong GL(V) \cong GL_n(\mathbb{F}_p).$$

In particular, the order of Aut(V) is as given in Section 1.4 (cf. the examples in Section 10.2 and 11.1).

(4) For all $n \neq 6$ we have $\text{Aut}(S_n) = \text{Inn}(S_n) \cong S_n$ (cf. Exercise 18). For $n = 6$ we have $|\text{Aut}(S_6) : \text{Inn}(S_6)| = 2$ (cf. the following Exercises 19 and also Exersice 10 in Section 6.3).

(5) $\text{Aut}(D_8) \cong D_8$ and $\text{Aut}(Q_8) \cong S_4$ (cf. the following Exercises 4 and 5 and also Exercise 9 in Section 6.3).

4.5 The Sylow Theorems

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

(1) A group of order p^α for some $\alpha \geq 1$ is called a *p-group*. Subgroups of G which are p-groups are called *p-subgroups*.

(2) If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a *Sylow p-subgroup* of G.

(3) The set of Sylow p-subgroups of G will be denoted by $Syl_p(G)$ and the number of Sylow p-subgroups of G will be denoted by $n_p(G)$ (or just n_p when G is clear from the context).

Theorem 18. *(Sylow's Theorem)* Let G be a group of order $p^\alpha m$, where p is a prime not dividing m.

(1) Sylow p-subgroups of G exist, i.e., $Syl_p(G) \neq \emptyset$.

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

(3) The number of Sylow p-subgroups of G is of the form $1 + kp$, i.e.,

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

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

Lemma 19. Let $P \in Syl_p(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$.
Corollary 20. let P be a Sylow p-subgroup of G. Then the following are equivalent:

(1) P is the unique Sylow p-subgroup of G, i.e., $n_p = 1$

(2) P is normal in G

(3) P is characteristic in G

(4) All subgroups generated by elements of p-power order are p-groups, i.e., if X is any subset of G such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p-group.

Proposition 21. If $|G| = 60$ and G has more than one Sylow 5-subgroup, then G is simple.
Corollary 22. A_5 is simple.
Proposition 23. If G is a simple group of order 60, then $G \cong A_5$.

4.6 The Simplicity of A_n

7 Introduction to Rings

7.1 Basic Definition and Examples

Definition.

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

(i) $(R, +)$ is an *abelian* group,

(ii) $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$,

(iii) the *distributive laws* hold in R: for all $a, b, c \in R$

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

(2) The ring R is *commutative* if multiplication is commutative.

(3) The ring R is said to have an *identity* (or *contain a* 1) if there is an element $1 \in R$ with

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

Definition. A ring R with identity 1, where $1 \neq 0$, is called a *division ring* (or *skew field*) if every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$ such that $ab = ba = 1$. A commutative division ring is called a *field*.
Proposition 1. Let R be a ring. Then

(1) $0a = a0 = 0$ for all $a \in R$.

(2) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$ (recall $-a$ is the additive inverse of a).

(3) $(-a)(-b) = ab$ for all $a, b \in R$.

(4) if R has an identity 1, then the identity is unique and $-a = (-a)a$.

Definition. Let R be a ring.

(1) A nonzero element a of R is called a *zero divisor* if there is a nonzero element b in R such that either $ab = 0$ or $ba = 0$.

(2) Assume R has an identity $1 \neq 0$. An element u of R is called a *unit* in R if there is some v in R such that $uv = vu = 1$. The set of units in R is denoted $R^\times$.

Definition. A commutative ring with identity $1 \neq 0$ is called an *integral domain* if it has no zero divisors.
Proposition 2. Assume a, b and c are elements of any ring with a not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$ (i.e., if $a \neq 0$ we can cancel the a's). In particular, if a, b, c are any elements in an integral domain and $ab = ac$, then either $a = 0$ or $b = c$.
Corollary 3. Any finite integral domain is a field.
Definition. A *subring* of the ring R is a subgroup of R that is closed under multiplication.

7.2 Examples: Polynomial Rings, Matrix Rings, and Group Rings

Proposition 4. Let R be an integral domain and let $p(x)$,$q(x)$ be nonzero elements of $R[x]$. Then

(1) degree $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$,

(2) the units of $R[x]$ are just the units of R,

(3) $R[x]$ is an integral domain.

7.3 Ring Homomorphism and Quetient Rings

Definition. Let R and S be rings.

(1) A *ring homomorphism* is a map $\varphi : R \to S$ satisfying

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$ (so φ is a group homomorphism on the additive groups) and

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

(2) The *kernel* of the ring homomorphism φ, denoted kerφ, is the set of elements of R that map to 0 in S (i.e., the kernel of φ viewed as a homomorphism of additve groups).

(3) A bijective ring homomorphism is called an *isomorphism*.

Proposition 5. Let R and S be rings and let$\varphi : R \to S$ be a homomorphism.

(1) The image of φ is a subring of S.

(2) The kernel of φ is a subring of R. Furthermore, if $\alpha \in$ kerφ then $r\alpha$ and $\alpha r \in$ kerφ for every $r \in R$, i.e., kerφ is closed under multiplication by elements from R.

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

(1) $rI = \{ra \mid a \in I\}$ and $Ir = \{ar \mid a \in I\}$.

(2) A subset I of R is a *left ideal* of R if

(i) I is a subring of R, and

(ii) I is closed under left multiplication by elements from R, i.e., $rI \subseteq I$ for all $r \in R$.

Similarly I is a *right ideal* if (i) holds and in place of (ii) one has

(iii) I is closed under right multiplication by elements from R, i.e., $Ir \subseteq I$ for all $r \in R$.

(3) A subset I that is both a left ideal and a right ideal is called an *ideal* (or, for added emphasis, a *two-sided ideal*) of R.

Proposition 6. Let R be a ring and let I be an ideal of R. Then the (additive) quotient group R/I is a ring under the binary operations:

$$(r+I) + (s+I) = (r+s) + I \text{ and } (r+I) \times (s+I) = (rs) + I$$

for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well defined, then I is an ideal of R.

Definition. When I is an ideal of R, the ring R/I with the operations in the previous proposition is called the *quotient ring* of R by I.

Theorem 7.

(1) *(The First Isomomorphism Theorem for Rings)* If $\varphi : R \to S$ is a homomorphism of rings, then the kernel of φ is an ideal of R, the image of φ is a subring of S and $R/$kerφ is isomorphic as a ring to $\varphi(R)$.

(2) If I is any ideal of R, then the map

$$R \to R/I \text{ defined by } r \mapsto r + I$$

is a surjective ring homomorphism with kernel I (this homomorphism is called the *natural projection* of R onto R/I). Thus every ideal is the kernel of a ring homomorphism and vice versa.

Theorem 8. Let R be a ring.

(1) *(The Second Isomorphism Theorem for Rings)* Let A be a subring and let B be an ideal of R. Then $A + B = \{a + b \mid a \in A,\ b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and $(A+B)/B \cong A/(A \cap B)$.

(2) *(The Third Isomorphism Theorem for Rings)* Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.

(3) *(The Fourth or Lattice Isomorphism Theorem for Rings)* Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings A of R that contain I and the set of subrings of R/I. Furthermore, A (a subring containing I) is an ideal of R if and only if A/I is an ideal of R/I.

Definition. Let I and J be ideals of R.

(1) Define the *sum* of I and J by $I + J = \{a + b \mid a \in I,\ b \in J\}$.

(2) Define the *product* of I and J, denoted by IJ, to be the set of all finite sums of elements of the form ab with $a \in I$ and $b \in J$.

(3) For any $n \leq 1$, define the n^{th} *power* of I, denoted by I^n, to be the set consisting of all finite sums of elements of the form $a_1 a_2 \cdots a_n$ with $a_i \in I$ for all i. Equivalently, I^n is defined inductively by defining $I^1 = I$, and $I^n = II^{n-1}$ for $n = 2, 3, \ldots$.

7.4 Properties of Ideals

Throughout this section R is a ring with identity $1 \neq 0$.
Definition. Let A be any subset of the ring R.

(1) Let (A) denote the smallest ideal of R containing A, called *the ideal generated by* A.

(2) Let RA denote the set of all finite sums of elements of the form ra with $r \in R$ and $a \in A$ i.e., $RA = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$ (where the convention is $RA = 0$ if $A = \emptyset$).
Similarly, $AR = \{a_1 r_1 + a_2 r_2 + \cdots + a_n r_n \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$ and $RAR = \{r_1 a_1 r_1' + r_2 a_2 r_2' + \cdots + r_n a_n r_n' \mid r_i, r_i' \in R, a_i \in A, n \in \mathbb{Z}^+\}$

(3) An ideal generated by a single element is called a *principal ideal*.

(4) An ideal generated by a finite set is called a *finitely generated ideal*.

Proposition 9. Let I be an ideal of R.

(1) $I = R$ if and only if I contains a unit.

(2) Assume R is commutative. Then R is a field if and only if its only ideals are 0 and R.

Corollary 10. If R is a field then any nonzero ring homomorphism from R into another ring is an injection.
Definition. An ideal M in an arbitrary ring S is called a *maximal ideal* if $M \neq S$ and the only ideals containing M are M and S.
Proposition 11. In a ring with identity every proper ideal is contained in a maximal ideal.
Proposition 12. Assume R is commutative. The ideal M is a maximal ideal if and only if the quotient ring R/M is a field.
Definition. Assume R is commutative. An ideal P is called a *prime ideal* if $P \neq R$ and whenever the product ab of two elements $a, b \in R$ is an element of P, then at least one of a and b is an element of P.
Proposition 13. Assume R is commutative. Then the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.
Corollary 14. Assume R is commutative. Every maximal ideal of R is a prime ideal.

7.5 Rings of Fractions

7.6 The Chinese Remainder Theorem

Throughout this section all rings are commutative with an identity $1 \neq 0$.
Definition. The ideals A and B of the ring R are said to be *comaximal* if $A + B = R$.
Theorem 17. *(Chinese Remainder Theorem)* Let $A_1, A_2, \ldots, A_k$ be ideals in R. The map

$$R \to R/A_1 \times R/A_2 \times \cdots \times R/A_k \text{ defined by } r \mapsto (r + A_1, r + A_2, \ldots, r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap \cdots \cap A_k$. If for each $i, j \in \{1, 2, \ldots, k\}$ with $i \neq j$ the ideals A_i and A_j are comaximal, then this map is surjective and $A_1 \cap A_2 \cap \cdots \cap A_k = A_1 A_2 \cdots A_k$, so

$$R/(A_1 A_2 \cdots A_k) = R/(A_1 \cap A_2 \cap \cdots \cap A_k) \cong R/A_1 \times R/A_2 \times \cdots \times R/A_k.$$

Corollary 18. Let n be a positive integer and let $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ be its factorization into powers of distinct primes. Then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}),$$

as rings, so in particular we have the following isomorphism of multiplicative groups:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times.$$

8 Euclidean Domains, Principlal Ideal Domains, and Unique Factorization Domains

8.1 Euclidean Domains

Definiation. Any function $N : R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a *norm* on the integral domain R. If $N(a) > 0$ for $a \neq 0$ define N to be a *positive norm*.
Definiation. The integral domain R is said to be a *Euclidean Domain* (or possess a *Division Algorithm*) if there is a norm N on R such that for any two elements a and b of R with $b \neq 0$ there exist elements q and r in R with

$$a = qb + r \text{ with } r = 0 \text{ or } N(r) < N(b).$$

The element q is called the *quotient* and the element r the *remainder* of the division.
Proposition 1. Every ideal in a Euclidean Domian is principal. More precisely, if I is any nonzero ideal in the Euclicdean Domian R then $I = (d)$, where d is any nonzero element of I of minimum norm.
Definiation. Let R be a commutative ring and let $a, b \in R$ with $b \neq 0$.

(1) a is said to be a *multiple* of b if there exists an element $x \in R$ with $a = bx$. In this case b is said to *divide* a or be a *divisor* of a, written $b \mid a$.

(2) A *greatest common divisor* of a and b is a nonzero element d such that

(i) $d \mid a$ and $d \mid b$, and

(ii) if $d' \mid a$ and $d' \mid b$ then $d' \mid d$.

A greatest common divisor of a and b will be denoted by g.c.d(a, b), or (abusing the notation) simply (a, b).

(3) The defining properties (i) and (ii) of a greatest common divisor of a and b translated into the language of ideals therefore become:
if I is the ideal of R generated by a and b, then d is a greatest common divisor of a and b if

(i) I is contained in the principal ideal (d), and

(ii) if (d') is any principal ideal containing I then $(d) \subseteq (d')$.

Proposition 2. If a and b are nonzero elements in the commutative ring R such that the ideal generated by a and b is a principal ideal (d), then d is a greatest common divisor of a and b.
Proposition 3. Let R be an integral domain. If two elements d and d' of R generate the same principal ideal, i.e., $(d) = (d')$, then $d' = ud$ for some unit u in R. In particular, if d and d' are both greatest common divisors of a and b, then $d' = ud$ for some unit u.
Theorem 4. Let R be a Euclidean Domain and let a and b be nonzero elements of R. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for a and b. Then

(1) d is a greatest common divisor of a and b, and

(2) the principal ideal (d) is the ideal generated by a and b. In particular, d can be written as an *R-linear combination* of a and b, i.e., there are elements x and y in R such that

$$d = ax + by.$$

For any integral domain let $\tilde{R} = R^\times \cup \{0\}$ denote the collection of units of R together with 0. An element $u \in R - \tilde{R}$ is called a *universal side divisor* if for every $x \in R$ there is some $z \in \tilde{R}$ such that u divides $x - z$ in R.
Proposition 5. Let R be an integral domain that is not a field. If R is a Euclidean Domain then there are universal side divisors in R.

8.2 Principal Ideal Domains (P.I.D.s)

Definition. A *Principal Ideal Domain* (P.I.D.) is an integral domain in which every ideal is principal.
Proposition 6. Let R be a Principal Ideal Domain and let a and b be nonzero elements of R. Let d be a generator for the principal ideal generated by a and b. Then

(1) d is a greatest common divisor of a and b

(2) d can be written as an *R-linear combination* of a and b, i.e., there are elements x and y in R with

$$d = ax + by$$

(3) d is unique up to multiplication by a unit of R.

Proposition 7. Every nonzero prime ideal in a Principal Ideal Domain is a maximal ideal.
Corollary 8. If R is any commutative ring such that the polynomial ring $R[x]$ is a Principal Ideal Domain (or a Euclidean Domain), then R is necessarily a field.
Definition. Define N to be a *Dedekind-Hasse norm* if N is a positive norm and for every nonzero $a, b \in R$ either a is an element of the ideal (b) or there is a nonzero element in the ideal (a, b) of norm strictly smaller than the norm of b (i.e., either b divides a in R or there exist $s, t \in R$ with $0 < N(sa - tb) < N(b)$).
Proposition 9. The integral domain R is a P.I.D. if and only if R has a Dedekind-Hasse norm.

8.3 Unique Factorization Domains (U.F.D.s)

Definition. Let R be an integral domain.

(1) Suppose $r \in R$ is nonzero and is not a unit. Then r is called *irreducible* in R if whenever $r = ab$ with $a, b \in R$, at least one of a or b must be a unit in R. Otherwise r is said to be *reducible*.

(2) The nonzero element $p \in R$ is called *prime* in R if the ideal (p) generated be p is a prime ideal. In other words, a nonzero element p is a prime if it is not a unit and whenever $p \mid ab$ for any $a, b \in R$, then either $p \mid a$ or $p \mid b$.

(3) Two elements a and b of R differing by a unit are said to be *associate* in R (i.e., $a = ub$ for some unit u in R).

Proposition 10. In an integral domain a prime element is always irreducible.
Proposition 11. In a Principal Ideal Domain a nonzero element is a prime if and only if it is irreducible.
Definition. A *Unique Factorization Domain* (U.F.D.) is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following two properties:

(i) r can be written as a finite product of irreducibles p_i of R (not necessarily distinct): $r = p_1 p_2 \cdots p_n$ and

(ii) the decomposition in (i) is *unique up to associates*: namely, if $r = q_1 q_2 \cdots q_m$ is another factorization of r into irreducibles, then $m = n$ and there is some renumbering of the factors so that p_i is associate to q_i for $i = 1, 2, \ldots, n$.

Proposition 12. In a Unique Factorization Domain a nonzero element is a prime if and only if it is irreducible.
Proposition 13. Let a and b be two nonzero elements of the Unique Factorization Domain R and suppose

$$a = up_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \text{ and } b = vp_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$$

are prime factorizations for a and b, where u and v are units, the primes $p_1, p_2, \ldots, p_n$ are *distinct* and the exponents e_i and f_i are ≥ 0. Then the element

$$d = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_n^{\min(e_n, f_n)}$$

(where $d = 1$ if all the exponents are 0) is a greatest common divisor of a and b.
Theorem 14. Every Principal Ideal Domain is a Unique Factorization Domain. In particular, every Euclidean Domain is a Unique Factorization Domain.
Theorem 15. The integers $\mathbb{Z}$ are a Unique Factorization Domain.
Corollary 16. Let R be a P.I.D. Then there exists a multiplicative Dedekind-Hasse norm on R.
Lemma 17. The prime number $p \in \mathbb{Z}$ divides an integer of the form $n^2 + 1$ if and only if p is either 2 or is an odd prime congruent to 1 modulo 4.
Proposition 18.

(1) *(Fermat's Theorem on sums of squares)* The prime p is the sum of two integer squares, $p = a^2 + b^2$, $a, b \in \mathbb{Z}$, if and only if $p = 2$ or $p \equiv 1 \bmod 4$. Except for interchanging a and b or changing the signs of a and b, the representation of p as a sum of two squares is unique.

(2) THe irreducible elements in the Gaussian integers $\mathbb{Z}[i]$ are as follows:

(a) $1 + i$ (which has norm 2),

(b) the primes $p \in \mathbb{Z}$ with $p \equiv 3 \bmod 4$ (which have norm p^2), and

(c) $a + bi, a - bi$, the distinct irreducible factors of $p = a^2 + b^2 = (a + bi)(a - bi)$ for the primes $p \in \mathbb{Z}$ with $p \equiv 1 \bmod 4$ (both of which have norm p).

Corollary 19. Let n be a positive integer and write

$$n = 2^k p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

where $p_1, \ldots, p_r$ are distinct primes congruent to 1 modulo 4 and $q_1, \ldots, q_s$ are distinct primes congruent to 3 modulo 4. Then n can be written as a sum of two squares in $\mathbb{Z}$, i.e., $n = A^2 + B^2$ with $A, B \in \mathbb{Z}$, if and only if each b_i is even. Futhermore, if this condition on n is satisfied, then the number of representations of n as a sum of two squares is $4(a_1 + 1)(a_2 + 1) \cdots (a_r + 1)$.
Summary. In summary, we have the following inclusions among classes of commutatve rings with identity:

fields $\subset$ *Euclidean Domains* $\subset$ *P.I.D.s* $\subset$ *U.F.D.s* $\subset$ *integral domains*

9 Polynomial Rings

9.1 Definitions and Basic Properties

Proposition 1. Let R be an integral domain. Then

(1) degree $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$, if $p(x), q(x)$ are nonzero.

(2) the units of $R[x]$ are just the units of R

(3) $R[x]$ is an integral domain.

Proposition 2. Let I be an ideal of the ring R and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I (the set of polynomials with coefficients in I). Then

$$R[x]/(I) \cong (R/I)[x].$$

In particular, if I is a prime ideal of R then (I) is a prime ideal of $R[x]$.
Definition. The *polynomial ring in the variables* $x_1, x_2, \ldots, x_n$ *with coefficients in* R, denoted $R[x_1, x_2, \ldots, x_n]$, is defined inductively by

$$R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]$$

9.2 Polynomial Rings Over Fields I

Theorem 3. Let F be a field. The polynomial ring $F[x]$ is a Euclidean Domain. Specifically, if $a(x)$ and $b(x)$ are two polynomials in $F[x]$ with $b(x)$ nonzero, then there are *unique* $q(x)$ and $r(x)$ in $F[x]$ such that

$$a(x) = q(x)b(x) + r(x) \text{ with } r(x) = 0 \text{ or degree } r(x) < \text{degree } b(x)$$

Corollary 4. If F is a field, then $F[x]$ is a Principal Ideal Domain and a Unique Factorization Domain.

9.3 Polynomial Rings That Are Unique Factorization Domains

Proposition 5. *(Gauss' Lemma)* Let R be a Unique Factorization Domain with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some nonconstant polynomials $A(x), B(x) \in F[x]$, then there are nonzero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.
Corollary 6. Let R be a Unique Factorization Domain, let F be its field of fractions and let $p(x) \in R[x]$. Suppose the greatest common divisor of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ if and only if it is irruducible in $F[x]$. In particular if $p(x)$ is a monic polynomial that is irreducible in $R[x]$, then $p(x)$ is irruducible in $F[x]$.
Theorem 7. R is a Unique Factorization Domain if and only if $R[x]$ is a Unique Factorization Domain.
Corollary 8. If R is a Unique Factorization Domain, then a polynomial ring in an arbitrary number of variables with coefficients in R is also a Unique Factorization Domain.

9.4 Irreducibility Criteria

Proposition 9. Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in F, i.e., there is an $\alpha \in F$ with $p(\alpha) = 0$.
Proposition 10. A polynomial of degree two or three over a field F is reducible if and only if it has a root in F.
Proposition 11. Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial of degree n with integer coefficients. If $r/s \in \mathbb{Q}$ is in lowest terms (i.e., r and s are relatively prime integers) and r/s is a root of $p(x)$, then r divides the constant term and s divides the leading coefficient of $p(x)$: $r \mid a_0$ and $s \mid a_n$. In particular, if $p(x)$ is a *monic* polynomial with integer coefficients and $p(d) \neq 0$ for all integers d dividing the constant term of $p(x)$, then $p(x)$ has no roots in $\mathbb{Q}$.
Proposition 12. Let I be a proper ideal in the integral domain R and let $p(x)$ be a nonconstant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.
Proposition 13. *(Eisenstein's Criterion)* Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $R[x]$ (here $n \geq 1$). Suppose $a_{n-1}, \ldots, a_1, a_0$ are all elements of P and suppose a_0 is not an element of P^2. Then $f(x)$ is irreducible in $R[x]$.
Corollary 14. *(Eisenstein's Criterion for $\mathbb{Z}[x]$)* Let p be a prime in $\mathbb{Z}$ and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $n \geq 1$. Suppose p divides a_i for all $i \in \{0, 1, \ldots, n-1\}$ but that p^2 does not divide a_0. Then $f(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

13 Field Theory

13.1 Basic Theory of Field Extensions

Definition. The *characteristic* of a field F, denoted $\text{ch}(F)$, is defined to be the smallest positive integer p such that $p \cdot 1_F = 0$ if such a p exists and is defined to be 0 otherwise.
Proposition 1. The characteristic of a field F, $\text{ch}(F)$, is either 0 or a prime p. If $\text{ch}(F) = p$ then for any $\alpha \in F$,

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

Definition. The *prime subfield* of a field F is the subfield of F generated by the multiplicative identity 1_F of F. It is (isomorphic to) either $\mathbb{Q}$ (if $\text{ch}(F) = 0$) or $\mathbb{F}_p$ (if $\text{ch}(F) = p$).
Definition. If K is a field containing the subfield F, then K is said to be an *extension field* (or simply an *extension*) of F, denoted K/F or by the diagram

In particular, every field F is an extension of its prime subfield. The field F is sometimes called the *base field* of the extension.
Definition. The *degree* (or *relative degree* or *index*) of a field entension K/F, denoted $[K : F]$, is the dimension of K as a vector space over F (i.e., $[K : F] = \dim_F K$). The extension is said to be *finite* if $[K : F]$ is finite and is said to be *infinite* otherwise.
Proposition 2. Let $\varphi : F \to F'$ be a homomorphism of fields. Then φ is either identically 0 or is injective, so that the imiage of φ is either 0 or isomorphic to F.
Theorem 3. Let F be a field and let $p(x) \in F\,[x]$ be an irreducible polynomial. Then there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root. Identifying F with this isomorphic copy shows that there exists an extension of F in which $p(x)$ has a root.
Theorem 4. Let $p(x) \in F[x]$ be an irreducible polynomial of degree n over the field F and let K be the field $F[x]/(p(x))$. Let $\theta = x \bmod (p(x)) \in K$. Then the elements

$$1, \theta, \theta^2, \ldots, \theta^{n-1}$$

are a basis for K as a vector space over F, so the degree of the extension is n, i.e., $[K : F] = n$. Hence

$$K = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\}$$

consists of all polynomials of degree $< n$ in θ.
Corollary 5. Let K be as in Theorem 4, and let $a(\theta), b(\theta) \in K$ be two polynomials of degree $< n$ in θ. Then addition in K is defined simply by usual polynomial addition and multiplication in K is defined by

$$a(\theta)b(\theta) = r(\theta)$$

where $r(x)$ is the remainder (of degree $< n$) obtained after dividing the polynomial $a(x)b(x)$ by $p(x)$ in $F[x]$.
Definition. Let K be an extension of the field F and let $\alpha, \beta, \cdots \in K$ be a collection of elements of K. Then the smallest subfield of K containing both F and the elements $\alpha, \beta, \ldots$, denoted $F(\alpha, \beta, \ldots)$ is called the field *generated by* $\alpha, \beta, \ldots$ *over* F.
Definition. If the field K is generated by a single element α over F, $K = F(\alpha)$, then K is said to be a *simple* extension of F and the element α is called a *primitive element* for the extension.

Theorem 6. Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Suppose K is an extension field of F containing a root α of $p(x)$: $p(\alpha) = 0$. Let $F(\alpha)$ denote the subfield K generated over F be α. Then

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

Corollary 7. Suppose in Theorem 6 that $p(x)$ is of degree n. Then

$$F(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\} \subseteq K.$$

Theorem 8. Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be an irreducible polynomial and let $p'(x) \in F'[x]$ be the irreducible polynomial obtained be applying the map φ to the coefficients of $p(x)$. Let α be a root of $p(x)$ (in some extension of F) and let β be a root of $p'(x)$ (in some extension of F'). Then there is an isomorphism

$$\begin{aligned} \sigma : F(\alpha) &\xrightarrow{\sim} F'(\beta) \\ \alpha &\mapsto \beta \end{aligned}$$

mapping α to β and extending φ, i.e., such that σ restricted to F is the isomorphism φ.

13.2 Algebraic Extensions

Let F be a field and let K be an extension of F.
Definition. The element $\alpha \in K$ is said to be *algebraic* over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic over F (i.e., is not the root of any nonzero polynomial with coefficients in F) then α is said to be *transcendental* over F. The extension is said to be *algebraic* if every element of K is algebraic over F.
Proposition 9. Let α be algebraic over F. Then there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$.
Corollary 10. If L/F is an extension of fields and α is algebraic over both F and L, then $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in $L[x]$.
Definition. The polynomial $m_{\alpha,F}(x)$ (or just $m_\alpha(x)$ if the field F is understood) in Proposition 9 is called the *minimal polynomial* for α over F. The *degree* of $m_\alpha(x)$ is called the *degree* of α.
Proposition 11. Let α be algebraic over the field F and let $F(\alpha)$ be the field generated be α over F. Then

$$F(\alpha) \cong F[x]/(m_\alpha(x))$$

So that in particular

$$[F(\alpha) : F] = \deg m_\alpha(x) = \deg \alpha,$$

i.e., the degree of α over F is the degree of the extension it generates over F.
Proposition 12. The element α is algebraic over F if and only if the simple extension $F(\alpha)/F$ is finite. More precisely, if α is an element of an extension of degree n over F then α satisfies a polynomial of degree at most n over F and if α satisfies a polynomial of degree n over F then the degree of $F(\alpha)$ over F is at most n.
Corollary 13. If the extension K/F is finite, then it is algebraic.
Theorem 14. Let $F \subseteq K \subseteq L$ be fields. Then

$$[L : F] = [L : K][K : F],$$

i.e., extension degrees are multiplicative, where if one side of the equation is infinite, the other side is also infinite. Pictorially,

$$\overbrace{\underbrace{F \subseteq}_{[K:F]} K \underbrace{\subseteq L}_{[L:K]}}^{[L:F]}$$

Corollary 15. Suppose L/F is a finite extension and let K be any subfield of L containing F, $F \subseteq K \subseteq L$. Then $[K : F]$ divides $[L : F]$.
Definition. An extension K/L is *finitely generated* if there are elements $\alpha_1, \alpha_2, \ldots, \alpha_k$ in K such that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_k)$.
Lemma 16. $F(\alpha, \beta) = (F(\alpha))(\beta)$, i.e., the field generated over F by α and β is the field generated by β over the field $F(\alpha)$ generated by α.
Theorem 17. The extension K/F is finite if and only if K is generated by a finite number of algebraic elements over F. More precisely, a field generated over F by a finite number of algebraic elements of degrees $n_1, n_2, \ldots, n_k$ is algebraic of degree $\leq n_1 n_2 \cdots n_k$.
Corollary 18. Suppose α and β are algebraic over F. Then $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ (for $\beta \neq 0$), (in particular α^{-1} for $\alpha \neq 0$) are all algebraic.

Corollary 19. Let L/F be an arbitrary extension. Then the collection of elements of L that are algebraic over F form a subfield K of L.
Theorem 20. If K is algebraic over F and L is algebraic over K, then L is algebraic over F.
Definition. Let K_1 and K_2 be two subfields of a field K. Then the *composite field* of K_1 and K_2, denoted K_1K_2, is the smallest subfield of K containing both K_1 and K_2. Similarly, the composite of any collection of subfields of K is the smallest subfield containing all the subfields.
Proposition 21. Let K_1 and K_2 be two finite extensions of a field F contained in K. Then

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

with equality if and only if an F-basis for one of the fields remains linearly independent over the other field. If $\alpha_1, \alpha_2, \ldots, \alpha_n$ and $\beta_1, \beta_2, \ldots, \beta_m$ are bases for K_1 and K_2 over F, respectively, then the elements $\alpha_i\beta_j$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$ span K_1K_2 over F.
Corollary 22. Suppose that $[K_1 : F] = n$, $[K_2 : F] = m$ in proposition 21, where n and m are relatively prime: $(n, m) = 1$. Then $[K_1K_2 : F] = [K_1 : F][K_2 : F] = nm$.

13.3 Classical Straightedge and Compass Constructions

13.4 Splitting Fields and Algebraic Closures

Definition. The extension field K of F is called a *splitting field* for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors (or *splits completely*) in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.
Theorem 25. For any field F, if $f(x) \in F[x]$ then there exists an extension K of F which is a splitting field for $f(x)$.
Definition. If K is an algebraic extension of F which is the splitting field over F for a collection of polynomials $f(x) \in F[x]$ then K is called a *normal* extension of F.
Proposition 26. A splitting field of a polynomial of degree n over F is of degree at most $n!$ over F.
Examples: (Splitting Field of $x^n - 1$: Cyclotomic Fields)
Definition. A generator of the cyclic group of all n^{th} roots of unity is called a *primitive* n^{th} root of unity. Let ζ_n denote a primitive n^{th} root.
Definition. The field $\mathbb{Q}(\zeta_n)$ (the splitting field of $x^n - 1$) is called the *cyclotomic field of n^{th} roots of unity*.
Examples: (Splitting Field of $x^p - 2$, p a prime)
The splitting field of $x^p - 2$ is $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ where ζ_p is a primitive p^{th} root of unity. And

$$[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] = p(p-1)$$

Theorem 27. Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $f(x) \in F[x]$ be a polynomial and let $f'(x) \in F'[x]$ be the polynomial obtained by applying φ to the coefficients of $f(x)$. Let E be a splitting field for $f(x)$ over F and let E' be a splitting field for $f'(x)$ over F'. Then the isomorphism φ extends to an isomorphism $\sigma : E \xrightarrow{\sim} E'$, i.e., σ restricted to F is the isomorphism φ.
Corollary 28. *(Uniqueness of Splitting Fields)* Any two splitting fields for a polynomial $f(x) \in F[x]$ over a field F are isomorphic.
Definition. The field $\overline{F}$ is called an *algebraic closure* of F if $\overline{F}$ is algebraic over F and if every polynomial $f(x) \in F[x]$ splits completely over $\overline{F}$ (so that $\overline{F}$ can be said to contain all the elements algebraic over F.)
Definition. A field K is said to be *algebraically closed* if every polynomial with coefficients in K has a root in K.
Proposition 29. Let $\overline{F}$ be an algebraic closure of F. Then $\overline{F}$ is algebraically closed.
Proposition 30. For any field F there exists an algebraically closed field K containing F.
Proposition 31. Let K be an algebraically closed field and let F be a subfield of K. Then the collection of elements $\overline{F}$ of K that are algebraic over F is an algebraic closure of F. An algebraic closure of F is unique up to isomorphism.
Theorem. *(Fundamental Theorem of Algebra)* The field $\mathbb{C}$ is algebraically closed.
Corollary 32. The field $\mathbb{C}$ contains an algebraic closure for any of its subfields. In particular, $\overline{\mathbb{Q}}$, the collection of complex numbers algebraic over $\mathbb{Q}$, is an algebraic closure of $\mathbb{Q}$.

13.5 Separable and Inseparable Extensions

Definition. A polynomial over F is called *separable* if it has no multiple roots (i.e., all its roots are distinct). A polynomial which is not separable is called *inseparable*.

Definition. The *derivative* of the polynomial

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

is defined to be the polynomial

$$D_x f(x) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1 \in F[x].$$

Proposition 33. A polynomial $f(x)$ has a multiple root α if and only if α is also a root of $D_x f(x)$, i.e., $f(x)$ and $D_x f(x)$ are both divisible by the minimal polynomial for α. In particular, $f(x)$ is separable if and only if it is relatively prime to its derivative: $(f(x), D_x f(x)) = 1$.

Corollary 34. Every irreducible polynomial over a field of characteristic 0 (for example, $\mathbb{Q}$) is separable. A polynomial over such a field is separable if and only if it is the product of distinct irreducible polynomials.

Proposition 35. Let F be a field of charateristic p. Then for any $a, b \in F$,

$$(a+b)^p = a^p + b^p, \text{ and } (ab)^p = a^p b^p.$$

Put another way, the p^{th}-power map defined by $\varphi(a) = a^p$ is an injective field homomorphism from F to F.

Definition. The map in Proposition 35 is called the *Frobenius endomorphism* of F.

Corollary 36. Suppose that $\mathbb{F}$ is a finite field of characteristic p. Then every element of $\mathbb{F}$ is a p^{th} power in $\mathbb{F}$ (notationally, $\mathbb{F} = \mathbb{F}^p$).

Proposition 37. Every irreducible polynomial over a finite field $\mathbb{F}$ is separable. A polynomial in $\mathbb{F}[x]$ is separable if and only if it is the product of distinct irreducible polynomials in $\mathbb{F}[x]$.

Definition. A field K of characteristic p is called *perfect* if every element of K is a p^{it} power in K, i.e., $K = K^p$. Any field of characteristic 0 is also called perfect.

Fact: Every irreducible polynomial over a perfect field is separable.

Proposition 38. Let $p(x)$ be an irreducible polynomial over a field F of characteristic p. Then there is a unique integer $k \geq 0$ and a unique irreducible separable polynomial $p_{\text{sep}(x)} \in F[x]$ such that

$$p(x) = p_{\text{sep}}(x^{p^k}).$$

Definition. Let $p(x)$ be an irreducible polynomial over a field of characteristic p. The degree of $p_{\text{sep}(x)}$ in the last proposition is called the *separable degree* of $p(x)$, denoted $\deg_s p(x)$. The integer p^k in the proposition is called the *inseparable degree* of $p(x)$, denoted $\deg_i p(x)$.

$$\deg p(x) = \deg_s p(x) \deg_i p(x)$$

Definition. The field is said to be *separable* (or *separable algebraic*) over F if every element of K is the root of a separable polynomial over F (equivalently, the minimal polynomial over F of every element of K is separable). A field which is not separable is *inseparable*.

Corollary 39. Every finite extension of a perfect field is separable. In particular, every finite extension of either $\mathbb{Q}$ or a finite field is separable.

14 Galois Theory

14.1 Basic Definitions

Definition.

(1) An isomorphism σ of K with itself is called an *automorphism* of K. The collection of automorphisms of K is denoted $\text{Aut}(K)$. If $\alpha \in K$ we shall write $\sigma\alpha$ for $\sigma(\alpha)$.

(2) An automorphism $\sigma \in \text{Aut}(K)$ is said to *fix* an element $\alpha \in K$ if $\sigma\alpha = \alpha$. If F is a subset of K (for example, a subfield), then an automorphism σ is said to *fix* F if it fixes all the elements of F, i.e., $\sigma a = a$ for all $a \in F$.

Definition. Let K/F be an extension of fields. Let $\text{Aut}(K/F)$ be the collection of automorphisms of K which fix F.

Proposition 1. $\text{Aut}(K)$ is a group under composition and $\text{Aut}(K/F)$ is a subgroup.

Proposition 2. Let K/F be a field extension and let $\alpha \in K$ be algebraic over F. Then for any $\sigma \in \text{Aut}(K/F)$, $\sigma\alpha$ is a root of the minimal polynomial for α over F, i.e., $\text{Aut}(K/F)$ permutes the roots of irruducible polynomials. Equivalently, any polynomial with coefficients in F having α as a root also has $\sigma\alpha$ as a root.

Proposition 3. Let $H \leq \text{Aut}(K)$ be a subgroup of the group of automorphisms of K. Then the collection F of elements of K fixed by all the elements of H is a subfield of K.

Definition. If H is a subgroup of the group of automorphisms of K, the subfield of K fixed by all the elements of H is called the *fixed field* of H.

Proposition 4. The association of groups to fields and fields to groups defined above is inclusion reversing, namely

(1) if $F_1 \subseteq F_2 \subseteq K$ are two subfields of K then $\text{Aut}(K/F_2) \leq \text{Aut}(K/F_1)$, and

(2) if $H_1 \leq H_2 \leq \text{Aut}(K)$ are two subgroups of automorphisms with associated fixed fields F_1 and F_2, respectively, then $F_2 \subseteq F_1$.

Proposition 5. Let E be the splitting field over F of the polynomial $f(x) \in F[x]$. Then

$$|\text{Aut}(E/F)| \leq [E : F]$$

with equality if $f(x)$ is separable over F.
Definition. Let K/F be a finite extension. Then K is said to be *Galois* over F and K/F is a *Galois* extension if $|\text{Aut}(E/F)| = [E : F]$. If K/F is Galois the group of automorphisms $\text{Aut}(K/F)$ is called the *Galois group* of K/F, denoted $\text{Gal}(K/F)$.
Corollary 6. If K is the splitting field over F of a separable polynomial $f(x)$ then K/F is Galois.
Definition. If $f(x)$ is a separable polynomial over F, then the *Galois group of* $f(x)$ *over* F is the Galois group of the splitting field of $f(x)$ over F.

14.2 The Fundamental Theorem of Galois Theory

Definition. A *character* χ of a group G with values in a field L is a homomorphism from G to the multiplicative group of L:

$$\chi : G \to L^\times$$

i.e., $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in G$ and $\chi(g)$ is nonzero element of L for all $g \in G$.
Definition. The characters $\chi_1, \chi_2, \ldots, \chi_n$ of G are said to be *linearly independent* over L if they are linearly independent as functions on G, i.e., if there is no trivial relation

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0 \ (a_1, a_2, \ldots, a_n \in L \ \text{ not all } 0)$$

as a function on G.
Theorem 7. *(Linear Independence of Characters)* If $\chi_1, \chi_2, \ldots, \chi_n$ are distinct characters of G with values in L then they are linearly independent over L.
Corollary 8. If $\sigma_1, \sigma_2, \ldots, \sigma_n$ are distinct embeddings of a field K into a field L, then they are linearly independent as functions on K. In particular distinct automorphisms of a field K are linearly independent as functions on K.
Theorem 9. Let $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be a subgroup of automorphisms of a field K and let F be the fixed field. Then

$$[K : F] = n = |G| .$$

Corollary 10. Let K/F be any finite extension. Then

$$|\text{Aut}(K/F)| \leq [k : F]$$

with equality if and only if F is the fixed field of $\text{Aut}(K/F)$. Put another way, k/F is Galois if and only if F is the fixed field of $\text{Aut}(K/F)$.
Corollary 11. let G be a finite subgroup of automorphisms of a field K and let F be the fixed field. Then every automorphism of K fixing F is contained in G, i.e., $\text{Aut}(K/F) = G$, so that K/F is Galois, with Galois group G.
Corollary 12. If $G_1 \neq G_2$ are distinct finite subgroups of automorphisms of a field K then their fixed fields are also distinct.
Theorem 13. The extension K/F is Galois if and only if K is the splitting field of some separable polynomial over F. Furthermore, if this is the case then every irreducible polynomial with coefficients in F which has a root in K is separable and has all its roots in K (so particular K/F is a separable extension).
Definition. Let K/F be a Galois extension. If $\alpha \in K$ the elements $\sigma\alpha$ for σ in $\text{Gal}(K/F)$ are called the *conjugates* (or *Galois conjugates*) of α over F. If E is a subfield of K containing F, the field $\sigma(E)$ is called the *conjugate field* of E over F.
Theorem 14. *(Fundamental Theorem of Galois Theory)*

14.3 Finite Fields

Proposition 15. Any finite field is isomorphic to $\mathbb{F}_{p^n}$ for some prime p and some integer $n \geq 1$. The field $\mathbb{F}_{p^n}$ is the splitting field over $\mathbb{F}_p$ of the polynomial $x^{p^n} - x$, the cyclic Galois group of order n generated by the Frobenius automorphism σ_p. The subfields of $\mathbb{F}_{p^n}$ are all Galois over $\mathbb{F}_p$ and are in one to one correspondence with the divisors d of n. They are the fields $\mathbb{F}_{p^d}$, the fixed fields of σ_p^d.
Corollary 16. The irreducible polynomial $x^4 + 1 \in \mathbb{Z}[x]$ is reducible modulo every prime p.
Proposition 17. The finite field $\mathbb{F}_{p^n}$ is simple. In particular, there exists an irreducible polynomial of degree n over $\mathbb{F}_p$ for every $n \geq 1$.
Proposition 18. The polynomial $x^{p^n} - x$ is precisely the product of all the distinct irreducible polynomials in $\mathbb{F}_p[x]$ of degree d where d runs through all divisors of n.

14.4 Composite Extensions and Simple Extensions

Proposition 19. Suppose K/F is a Galois extension and F'/F is any extension. Then KF'/F' is a Galois extension, with Galois group

$$\text{Gal}(KF'/F') \cong \text{Gal}(K/K \cap F')$$

isomorphic to a subgroup of $\text{Gal}(K/F)$.
Corollary 20. Suppose K/F is a Galois extension and F'/F is any finite extension. Then

$$[KF' : F] = \frac{[K : F][F' : F]}{[K \cap F' : F]}$$

Proposition 21. Let K_1 and K_2 be Galois extensions of a field F. Then

(1) The intercection $K_1 \cap K_2$ is Galois over F.

(2) The composite K_1K_2 is Galois over F. The Galois group is isomorphic to the subgroup

$$H = \{(\sigma, \tau) \mid \sigma \mid_{K_1 \cap K_2} = \tau \mid_{K_1 \cap K_2}\}$$

of the direct product $\text{Gal}(K_1/F) \times \text{Gal}(K_2/F)$ consisting of elements whose restrictions to the intersection $K_1 \cap K_2$ are equal.

Corollary 22. Let K_1 and K_2 be Galois extensions of a field F with $K_1 \cap K_2 = F$. Then

$$\text{Gal}(K_1K_2/F) \cong \text{Gal}(K_1/F) \times \text{Gal}(K_2/F).$$

Conversely, if K is Galois over F and $G = \text{Gal}(K/F) = G_1 \times G_2$ is the product of two subgroups G_1 and G_2, then K is composite of two Galois extensions K_1 and K_2 of F with $K_1 \cap K_2 = F$.
Corollary 23. Let E/F be any finite separable extension. Then E is contained in an extension K which is Galois over F and is minimal in the sense that in a fixed algebraic closure of K any other Galois extension of F containing E contains K.
Definition. The Galois extension K of F containing E in the previous corollary is called the *Galois closure* of E over F.
Proposition 24. Let K/F be a finite extension. Then $K = F(\theta)$ if and only if there exist only finitely many subfields of K containing F.
Theorem 25. *(The primitive Element Theorem)* If K/F is finite and separable, then K/F is simple. In particular, any finite extension of fields of characteristic 0 is simple.

14.5 Cylotomic Extensions and Abelian Extensions over $\mathbb{Q}$

Theorem 26. The Galois group of the cyclotomic field $\mathbb{Q}(\zeta_n)$ of n^{th} roots of unity is isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. The isomorphism is given explicitly by the map
Corollary 27. Let
Definition. The extension K/F is called an *abelian* extension if K/F is Galois and $\text{Gal}(K/F)$ is an abelian group.
Corollary 28. Let G be any finite abelian group. Then there is a subfield K of a cyclotomic field with $\text{Gal}(K/\mathbb{Q}) \cong G$.
Theorem. *(Kronecker-Weber)* Let K be a finite abelian extension of $\mathbb{Q}$. Then K is contained in a cyclotomic extension of $\mathbb{Q}$.

14.6 Galois Groups of Polynomials