

Incomplete Notes on Fraleigh's Abstract Algebra (4th ed.)

Afra Zomorodian

December 12, 2001

Contents

1	A Few Preliminaries	2
1.1	Mathematics and Proofs	2
1.2	Sets and Equivalence Relations	2
1.3	Mathematical Induction	3
1.4	Complex and Matrix Arithmetic	3
2	Introduction to Groups	4
2.1	Binary Operations	4
2.2	Groups	4
2.3	Subgroups	5
2.4	Groups of Permutations	6
2.5	Orbits, Cycles, and the Alternating Group	7
2.6	Cyclic Groups	8
2.7	Cosets and the Theorem of Lagrange	8
2.8	Direct Products and Finitely Generated Abelian Groups	9
3	Homomorphisms and Factor Groups	11
3.1	Homomorphisms	11
3.2	Isomorphism and Cayley's Theorem	12
3.3	Factor Groups	13
3.4	Factor-Group Computations and Simple Groups	14
3.5	Series of Groups	14
3.6	Groups in Geometry, Analysis, and Art	15
4	Advanced Group Theory	16
4.1	Isomorphism Theorems: Proof of the Jordan-Hölder Theorem	16
4.2	Group Action on a Set	17
4.3	Application of G -Sets to Counting	17
4.4	Sylow Theorems	17
4.5	Applications of the Sylow Theory	18
4.6	Free Abelian Groups	19
4.7	Free Groups	20
4.8	Group Presentations	21

5	Introduction to Rings and Fields	22
5.1	Rings and Fields	22
5.2	Integral Domains	23
5.3	Fermat's and Euler's Theorems	24
5.4	The Field of Quotients of an Integral Domain	25
5.5	Rings of Polynomials	26
5.6	Factorization of Polynomials over a Field	27
5.7	Noncommutative Examples	28
6	Factor Rings and Ideals	29
6.1	Homomorphisms and Factor Rings	29
6.2	Prime and Maximal Ideals	31
7	Factorization	33
7.1	Unique Factorization Domains	33
7.2	Euclidean Domains	34
7.3	Gaussian Integers and Norms	35
8	Extension Fields	36
8.1	Introduction to Extension Fields	36
8.2	Vector Spaces	37
8.3	Additional Algebraic Structures	39
8.4	Algebraic Extensions	40
8.5	Geometric Constructions	42
8.6	Finite Fields	42
9	Automorphisms and Galois Theory	43
9.1	Automorphisms of Fields	43

1 A Few Preliminaries

1.1 Mathematics and Proofs

Mathematics is an *axiomatic* study. Abstract algebra is the most axiomatic as it is the most efficient presentation (proofs are for structures satisfying *axioms*.) *Abstract* means that algebra is studied by properties abstracted from subject. Proofs are the right tricks gained through experience. Useful definitions, once understood, lead to interesting results. Definitions are iff. Hypotheses must be used in proofs so they're not redundant. Counterexamples disprove theorems. Never take quantifying words or phrases for granted. For existence and uniqueness proofs, show existence, then assume 2 exist and show equality.

1.2 Sets and Equivalence Relations

THE NOTION OF A SET

It is impossible to define every concept as our language is finite. We have to have primitive undefined concepts.

- A **set** is a well-defined collection of objects. We assume:
 1. Set S is made up of **elements** $a \in S$.
 2. There is only one empty set \emptyset .
 3. We may describe a set by characterizing it ($\{x \mid P(x)\}$) or by enumerating elements ($\{1, 2, 3\}$).
 4. A set S is **well-defined** if for each object a , either $a \in S$ or $a \notin S$.

- A set B is a **subset** of a set A ($B \subseteq A$ or $A \supseteq B$), if every element of B is in A . $B \subset A$ or $A \supset B$ will be used for $B \subseteq A$ but $B \neq A$.
- If A is any set, then A is the **improper subset** of A . Any other subset is **proper**.

PARTITIONS AND EQUIVALENCE RELATIONS

- A **partition of a set** is a decomposition of the set into subsets (**cells**) such that every element of the set is in *one and only one* of the subsets.
- **(Theorem)** Let S be a nonempty set and let \sim be a relation between elements of S that satisfies the following properties for all $a, b, c \in S$:
 1. (Reflexive) $a \sim a$.
 2. (Symmetric) If $a \sim b$, then $b \sim a$.
 3. (Transitive) If $a \sim b$ and $b \sim c$, $a \sim c$.

Then, \sim yields a natural partition of S , where:

$$\bar{a} = \{x \in S \mid x \sim a\}$$

Note that \bar{a} represents the subset to which a belongs to. The relation \sim is then called an **equivalence relation** on S . Each cell \bar{a} in the natural partition given by an equivalence relation is an **equivalence class**. Explanation: reflexive property means each element is in at least some partition. Symmetric and transitive properties allow the “flowing” of elements among unfinished partitions (so no element could be in two different partitions, they just merge!)

- Let h and k be two integers in \mathbb{Z} and n any positive integer. We define h *congruent to k modulo n* , written $h \equiv k \pmod{n}$, if $h - k$ is evenly divisible by n , so that $h - k = ns$ for some $s \in \mathbb{Z}$. Equivalence classes for congruence modulo n are **residue classes modulo n** .

1.3 Mathematical Induction

- **Induction Axiom:** Let S be a subset of \mathbb{Z}^+ satisfying
 1. $1 \in S$, and
 2. if $k \in S$, then $(k + 1) \in S$.

Then $S = \mathbb{Z}^+$.

- **Mathematical Induction:** Let $P(n)$ be a statement. If
 1. $P(1)$ is true, and
 2. if $P(k)$ is true, then $P(k + 1)$ is true.

Then, $P(n)$ is true for all $n \in \mathbb{Z}^+$.

- **Strong Induction:** replace rule two by: if $P(m)$ is true for $1 \leq m \leq k$, then $P(k + 1)$ is true.

1.4 Complex and Matrix Arithmetic

COMPLEX NUMBERS:

- The set \mathbb{C} of **complex numbers** is defined by

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$$

- The **norm, absolute value, or modulus** of $a + bi$ is $|a + bi| = \sqrt{a^2 + b^2}$.

- $z = a + bi$ may be written in polar coordinates as $z = |z|(\cos \theta + i \sin \theta)$.
- Geometrically, addition is vector addition and multiplication is multiplying the norms and adding the polar angles.
- $a - bi$ is the **conjugate** of $a + bi$. To divide complex numbers, we multiply the quotient by the conjugate of the denominator.

MATRICES:

- A **matrix** is an array of numbers. We denote a matrix with m rows and n columns and type \mathbb{X} numbers as $M_{m \times n}(\mathbb{X})$.
- Matrix multiplication is not commutative but associative.
- Square matrices can be **invertible**. Otherwise, they're **singular**.

2 Introduction to Groups

2.1 Binary Operations

- A **binary operation $*$ on a set S** is a rule that assigns to each ordered pair (a, b) of elements of S some element in S . Note: it must assign a single element to each pair (otherwise it's either *not defined* or *not well-defined*) and it must assign an element which is in S for the operation to be **closed**. Examples: $+$ is not a binary operation on $M(\mathbb{R})$, \cdot is on $M_4(\mathbb{C})$.
- A binary operation $*$ on a set S is **commutative** iff $a * b = b * a$ for all $a, b \in S$. The table for $*$ will be symmetric with respect to the upper-left to lower-right diagonal.
- A binary operation $*$ on a set S is **associative** iff $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

2.2 Groups

Solving equations gave rise to need for new types of numbers:

1. $5 + x = 2$ for \mathbb{Z}^-
2. $2x = 3$ for \mathbb{Q}
3. $x^2 = -1$ for \mathbb{C}

Analysis of solving linear additive and multiplicative equations motivated basic properties for groups.

- A **group** $\langle G, * \rangle$ is a set G , together with a binary operation $*$ on G , such that the following axioms are satisfied:
 - \mathcal{G}_1 : The binary operation $*$ is associative
 - \mathcal{G}_2 : There is an element e in G such that $e * x = x * e = x$ for all $X \in G$ (This element e is an **identity** element for $*$ on G .)
 - \mathcal{G}_3 : For each $a \in G$, there is an element $a' \in G$ with the property that $a' * a = a * a' = e$ (The element a' is an **inverse of a with respect to the operation $*$**).
- **(Theorem)** If G is a group with binary operation $*$, then the **left and right cancellation laws** hold in G , that is, $a * b = a * c$ implies $b = c$, and $b * a = c * a$ implies $b = c$ for $a, b, c \in G$. (Proof follows axioms)
- **(Theorem)** If G is a group with binary operation $*$, and if a and b are any elements of G , then the linear equations $a * x = b$ and $y * a = b$ have unique solutions in G . (Proof by existence, then cancellation laws.)

- A group G is **abelian** if its binary operation $*$ is commutative. Subset S of $M_2(\mathbb{R})$ consisting of all *invertible* matrices is a nonabelian group with matrix multiplication as operation.
- **(Theorem)** In a group, the identity and inverses are unique.
- In a group G , we have $(ab)' = b'a'$ for all $a, b \in G$.
- One-sided definitions are OK for group definition, as long the same side is used for both identity and inverses.
- In finite groups, each element b of a group must appear once and only once in each row and column of its table.
- Finite group structures for groups of size 2, 3, 4. Note: three exist for 4, but only two structures.

$*$	e	a
e	e	a
a	a	e

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

\mathbb{Z}_4	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

V	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

2.3 Subgroups

NOTATION AND TERMINOLOGY

- The operation is often denoted as $+$ or juxtaposition. $+$ is used for commutative operations.
- 0 or 1 is used to denote identity.
- a^{-1} or $-a$ is used to denote inverse.
- **(Theorem)** If G is a finite group, then the **order** $|G|$ of G is the number of elements in G . In general, for any finite set S , $|S|$ is the number of elements in S .
- We use the word “under” for operations: the group \mathbb{R} under addition.

SUBSETS AND SUBGROUPS

- Let G be a group and let S be a subset of G . If for every $a, b \in S$ it is true that the product ab computed in G is also in S , then S is closed under the group operation of G . The binary operation on S thus defined is the **induced operation on S from G** .
- If a subset H of a group G is closed under the binary operation of G and if H itself is a group, then H is a **subgroup of G** . We shall let $H \leq G$ or $G \geq H$ denote that H is a subgroup of G , and $H < G$ or $G > H$ shall mean $H \leq G$ but $H \neq G$.
- If G is a group, then the subgroup consisting of G itself is the **improper subgroup of G** . All other subgroups are **proper subgroups**. The subgroup $\{e\}$ is the **trivial subgroup** of G . All other subgroups are **nontrivial**.
- **(Theorem)** A subset H of a group G is a subgroup of G iff:
 1. H is closed under the binary operation of G ,
 2. the identity e of G is in H ,
 3. for all $a \in H$ it is true that $a^{-1} \in H$ also.

Note: condition 2 eliminates \emptyset . A closed nonempty finite subset is always a subgroup.

CYCLIC SUBGROUPS

- **(Theorem)** Let G be a group and let $a \in G$. Then

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G and is the smallest subgroup of G that contains a , that is, every subgroup containing a contains H (Note the difference between *minimal* and *smallest*. A *minimal* subset doesn't have any subsets with the same property, while the *smallest* subset is the smallest and is unique.)

- The group H of above theorem is the **cyclic subgroup of G generated by a** , and will be denoted by $\langle a \rangle$.
- An element a of a group G **generates G** and is a **generator for G** if $\langle a \rangle = G$. A group G is **cyclic** if it has a generator.

2.4 Groups of Permutations

FUNCTIONS AND PERMUTATIONS

- A **function** or **mapping ϕ from a set A into a set B** is a rule that assigns to each element a of A exactly one element b of B . We say that ϕ **maps a into b** , and that ϕ **maps A into B** . We denote this by:

$$\phi(a) = b$$

The element b is the **image of a under ϕ** . We show the map as:

$$\phi : A \rightarrow B$$

The set A is the **domain of ϕ** , the set B is the **codomain of ϕ** , and the set $\phi(A) = \{\phi(a) \mid a \in A\}$ is the **image of A under ϕ** .

- If ϕ and ψ are functions with $\phi : A \rightarrow B$ and $\psi : B \rightarrow C$, then there is a natural function mapping A into C , the **composite function**, consisting of ϕ followed by ψ . We write:

$$\psi(\phi(a)) = c,$$

and denote the composite function by $\psi\phi$ (read from right to left.)

- A function from a set A into a set B is **one to one (injection)** if each element B has at most one element mapped into it, and it is **onto B (surjection)** if each element of B has at least one element of A mapped into it. If it is both, it's a **bijection**. In other words, to say an function is one-to-one is to say each $b \in B$ has *at most one arrow* coming into it, while onto means that *every $b \in B$ has at least one arrow* coming into it:

1. To show that ϕ is one-to-one, you show that $\phi(a_1) = \phi(a_2)$ implies $a_1 = a_2$.

2. To show that ϕ is onto B , you show that for each $b \in B$, there exists $a \in A$ such that $\phi(a) = b$.

- A **permutation of a set A** is a function from A into A that is both one to one and onto. In other words, a permutation of A is a one-to-one function from A onto A . We write:

$$\phi : A \xrightarrow[\text{onto}]{1-1} A$$

PERMUTATION GROUPS

- Function composition is a binary operation on the collection of all permutations of a set A . We call this operation **permutation multiplication**.
- **(Theorem)** Let A be a nonempty set, and let S_A be the collection of all permutations of A . Then, S_A is a group under permutation multiplication. $\iota(a) = a$ acts as identity for group.

- Let A be the finite set $\{1, 2, \dots, n\}$. The group of all permutations of A is the **symmetric group on n letters**, is denoted by S_n , and has $n!$ elements.
- Examples: S_3 has minimal order for any nonabelian group and corresponds to the **group D_3 (dihedral group) of the symmetries of an equilateral triangle**. Group D_4 has 8 elements, is the **group of the symmetries of the square or octic group**, and is nonabelian.

2.5 Orbits, Cycles, and the Alternating Group

Note: Orbits are sets ($\{1, 2, 5\}$). Cycles are permutation and should be written in the cycle notation. Transpositions are 2-cycles.

ORBITS

- Let σ be a permutation of a set A . The equivalence classes in A determined by the equivalence relation below are the **orbits of σ** :

$$a, b \in A, \quad a \sim b \quad \text{iff} \quad b = \sigma^n(a), \quad \text{for some } n \in \mathbb{Z}$$

CYCLES

- A permutation $\sigma \in S_n$ is a **cycle** if it has at most one orbit containing more than one element. The **length** of a cycle is the number of elements in its largest orbit. We use a single-row **cycle notation** as below, where the set on which the cycle acts must be made clear by context (μ below acts on S_8 , for example):

$$\mu = (1, 3, 6)$$

- **(Theorem)** Every permutation σ of a finite set is a product of disjoint cycles.
- Multiplication of disjoint cycles is commutative. Therefore, representation of a permutation as a product of disjoint cycles, none of which is the identity permutation, is unique up to the order of the factors (here order just means order in list!)

EVEN AND ODD PERMUTATIONS

- A cycle of length 2 is a **transposition**.
- Any cycle is a product of transpositions: $(a_1, a_2, \dots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \dots (a_1, a_2)$.
- Any permutation of a finite set of at least two elements is a product of transpositions (corollary to theorem above.) Example: in S_n for $n \geq 2$, the identity permutation is the product $(1, 2)(1, 2)$.
- **(Lemma)** Let $\sigma \in S_n$ and let τ be a transposition in S_n . The number of orbits of σ and the number of orbits of $\tau\sigma$ differ by 1. (bridge building)
- **(Theorem)** No permutation in S_n can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions. (induction on transpos.)
- A permutation of a finite set is **even** or **odd** according to whether it can be expressed as a product of even or odd number of transpositions, respectively.

THE ALTERNATING GROUP

- If $n \geq 2$, then the collection of all even permutations of $1, 2, \dots, n$ forms a subgroup of order $n!/2$ of the symmetric group S_n . We call this subgroup the **alternating group A_n on n letters**.

2.6 Cyclic Groups

Recall from section 1.3 definitions about cyclic groups.

- Let $a \in G$. If cyclic subgroup $\langle a \rangle$ is finite, then the **order of a** is the order $|\langle a \rangle|$. Otherwise, we say that a is of **infinite order**.

ELEMENTARY PROPERTIES

- **(Theorem)** Every cyclic group is abelian.
- **(Division algorithm for \mathbb{Z})** If m is a positive integer and n is any integer, then there exist unique integers q and r such that

$$n = mq + r \quad \text{and} \quad 0 \leq r < m$$

q is **quotient** and r is the nonnegative **remainder** when n is divided by m (Proof by diagram.)

- **(Theorem)** A subgroup of a cyclic group is cyclic.
- **(Corollary)** The subgroups of \mathbb{Z} under addition are precisely the groups $n\mathbb{Z}$ under addition for $n \in \mathbb{Z}$.
- Let $r, s \in \mathbb{Z}^+$. The positive generator d of the cyclic group

$$H = \{nr + ms \mid n, m \in \mathbb{Z}\}$$

under addition is the **greatest common divisor (gcd)** of r and s .

- Two positive integers are **relatively prime** if their gcd is 1.
- If r and s are relatively prime and r divides sm , then r must divide m .

THE CLASSIFICATION OF CYCLIC GROUPS

- **(Case I)** G has infinite number of elements. All infinite cyclic groups are isomorphic. We use $\langle \mathbb{Z}, + \rangle$ as prototype.
- **(Case II)** G has finite order. The distinct elements are $e, a, a^2, \dots, a^{m-1}$ and a is of order m . All cyclic groups of the same finite order are isomorphic.
- Let n be a fixed positive integer and let h and k be any integers. The remainder r when $h+k$ is divided by n in accord with the division algorithm is the **sum of h and k modulo n** .
- **(Theorem)** The set $\{0, 1, 2, \dots, n-1\}$ is a cyclic group \mathbb{Z}_n of elements under addition modulo n .

SUBGROUPS OF FINITE CYCLIC GROUPS

- **(Theorem)** Let G be a cyclic group with n elements and generated by a . Let $b \in G$ and let $b = a^s$. Then b generates a cyclic subgroup H of G containing n/d elements, where d is the gcd of n and s .
- **(Corollary)** If a is a generator of a finite cyclic group G of order n , then the other generators of G are the elements of the form a^r , where r is relatively prime to n .

2.7 Cosets and the Theorem of Lagrange

COSETS

- **(Theorem)** Let H be a subgroup of G . Let the relation \sim_L be defined on G by

$$a \sim_L b \quad \text{if and only if} \quad a^{-1}b \in H$$

Let \sim_R be defined by

$$a \sim_R b \quad \text{if and only if} \quad ab^{-1} \in H$$

Then \sim_L and \sim_R are both equivalence relations on G .

- $a^{-1}b \in H \Rightarrow a^{-1}b = h \in H \Rightarrow b = ha$. Similar for other case.
- Let H be a subgroup of group G . For $a \in G$, the subset $aH = \{ah \mid h \in H\}$ of G is the **left coset** of H containing a , while $Ha = \{ha \mid h \in H\}$ is the **right coset** of H containing a .
- For an abelian subgroup H of G , the partition of G into left cosets of H and the partition into right cosets are the same.
- The partition of \mathbb{Z} into cosets of $n\mathbb{Z}$ is the partition of \mathbb{Z} into residue classes modulo n (\sim_R). We call this partition *cosets modulo $n\mathbb{Z}$* .
- Left cosets of a subgroup H of a group G give rise to a coset group when the partition of G into left cosets of H is the same as the partition into right cosets of H (proof in Ch. 2)

THEOREM OF LAGRANGE

- Every coset (left or right) of a subgroup H of a group G has the same number of elements as H (proof by 1-1 onto map.)
- **(Theorem of Lagrange)** Let H be a subgroup of a finite group G . Then the order of H is a divisor of the order of G (Converse isn't true, e.g. A_4 has no subgroup of order 6.) Proof by counting.
- **(Corollary)** Every group of prime order is cyclic.
- *Never underestimate a theorem that counts something!*
- There is essentially one group structure of a given prime order p (as all cyclic and isomorphic to \mathbb{Z}_p .)
- **(Theorem)** The order of an element of a finite group divides the order of the group.
- Let H be a subgroup of a group G . The number of left cosets of H in G is the **index** ($G : H$) of H in G . If G is finite, then $(G : H) = |G|/|H|$.
- **(Theorem)** Suppose H and K are subgroups of a group G such that $K \leq H \leq G$, and suppose $(H : K)$ and $(G : H)$ are both finite. Then $(G : K)$ is finite, and $(G : K) = (G : H)(H : K)$.

2.8 Direct Products and Finitely Generated Abelian Groups

DIRECT PRODUCTS

- The **Cartesian product of sets** S_1, S_2, \dots, S_n is the set of all ordered n -tuples (a_1, a_2, \dots, a_n) , where $a_i \in S_i$. The Cartesian product is denoted by either

$$S_1 \times S_2 \times \dots \times S_n$$

or by

$$\prod_{i=1}^n S_i .$$

- **(Theorem)** Let G_1, G_2, \dots, G_n be groups. For (a_1, a_2, \dots, a_n) and (b_1, b_2, \dots, b_n) in $\prod_{i=1}^n G_i$, define $(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n)$ to be $(a_1b_1, a_2b_2, \dots, a_nb_n)$. Then $\prod_{i=1}^n G_i$ is a group, the **direct product of the groups G_i** , under this binary operation (multiplication by components.) If each G_i is commutative, we often use $\bigoplus_{i=1}^n G_i$ as notation and refer to it as the **direct sum of the groups G_i** .
- **(Theorem)** The group $\mathbb{Z}_n \times \mathbb{Z}_m$ is isomorphic to \mathbb{Z}_{mn} iff m and n are relatively prime. This may be extended to more than two factors via induction (orders must be pairwise relatively prime.)
- Let r_1, r_2, \dots, r_n be positive integers. Their **least common multiple (lcm)** is the positive generator of the cyclic group of all common multiples of the r_i , that is, the cyclic group of all integers divisible by each r_i for $i = 1, 2, \dots, n$.

- **(Theorem)** Let $(a_1, a_2, \dots, a_n) \in \prod_{i=1}^n G_i$. If a_i is of finite order r_i in G_i , then the order of (a_1, a_2, \dots, a_n) in $\prod_{i=1}^n G_i$ is equal to the least common multiple of all the r_i .
- We consider $\prod_{i=1}^n G_i$ to be the **internal direct product** of the subgroups

$$\overline{G}_i = \{(e_1, e_2, \dots, e_{i-1}, a_i, e_{i+1}, \dots, e_n) \mid a_i \in G_i\}$$

GENERATORS OF A GROUP

- Let $\{S_i \mid i \in I\}$ be a collection of sets. Here I may be any set of indices. The **intersection** $\bigcap_{i \in I} S_i$ of the sets S_i is the set of all elements that are in all the sets S_i ; that is,

$$\bigcap_{i \in I} S_i = \{x \mid x \in S_i \text{ for all } i \in I\}$$

If I is finite, $I = \{1, 2, \dots, n\}$, we may denote $\bigcap_{i \in I} S_i$ by

$$S_1 \cap S_2 \cap \dots \cap S_n$$

- **(Theorem)** The intersection of subgroups H_i of a group G for $i \in I$ is again a subgroup of G .
- Let G be a group and let $a_i \in G$ for $i \in I$. The smallest subgroup of G containing $\{a_i \mid i \in I\}$ is the **subgroup generated by** $\{a_i \mid i \in I\}$. If this subgroup is all of G , then $\{a_i \mid i \in I\}$ **generates** G and the a_i are the **generators of** G . If there is a finite set $\{a_i \mid i \in I\}$ that generates G , then G is **finitely generated**.
- **(Theorem)** If G is a group and $a_i \in G$ for $i \in I$, then the subgroup H of G generated by $\{a_i \mid i \in I\}$ has as elements precisely those elements of G that are finite products of integral powers of the a_i , where powers of a fixed a_i may occur several times in the product. Examples: S_3 is generated by ρ_1 and μ_1 . $\mathbb{Z} \times \mathbb{Z}_2$ is generated by $\{(1, 0), (0, 1)\}$.

THE STRUCTURE OF FINITELY GENERATED ABELIAN GROUPS

- **(Fundamental Theorem of Finitely Generated Abelian Groups)** Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \dots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z},$$

where the p_i are primes, not necessarily distinct. The direct product is unique except for possible arrangement of factors; that is, the number (**Betti number** of G) of factors of \mathbb{Z} is unique and the prime powers $(p_i)^{r_i}$ are unique (Proof in 3.6.)

APPLICATIONS

All proven using the fundamental theorem above.

- A group G is **decomposable** if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise, G is **indecomposable**.
- **(Theorem)** The finite indecomposable abelian groups are exactly the cyclic groups with order a power of a prime.
- **(Theorem)** If m divides the order of a finite abelian group G , then G has a subgroup of order m .
- **(Theorem)** If m is a square-free integer, that is, m is not divisible by the square of any prime, then every abelian group of order m is cyclic.

3 Homomorphisms and Factor Groups

3.1 Homomorphisms

STRUCTURE-RELATING MAPS

- A map ϕ of a group G into a group G' is a **homomorphism** if

$$\phi(ab) = \phi(a)\phi(b)$$

for all $a, b \in G$. For any groups G and G' , there's always at least one homomorphism $\phi : G \rightarrow G'$, namely the **trivial homomorphism** defined by $\phi(g) = e'$ for all $g \in G$, where e' is the identity in G' .

- Examples: evaluation homomorphisms, determinant, projection map, reduction modulo n .

PROPERTIES OF HOMOMORPHISMS

- Let ϕ be a mapping of a set X into a set Y , and let $A \subseteq X$ and $B \subseteq Y$. The **image** $\phi(A)$ of A in Y under ϕ is $\{\phi(a) \mid a \in A\}$. The set $\phi(X)$ is sometimes called the **range of ϕ** . The **inverse image** $\phi^{-1}(B)$ of B in X is $\{x \in X \mid \phi(x) \in B\}$.
- **(Theorem)** Let ϕ be a homomorphism of a group G into a group G' .
 1. If e is the identity in G , then $\phi(e)$ is the identity e' in G' .
 2. If $a \in G$, then $\phi(a^{-1}) = \phi(a)^{-1}$.
 3. If H is a subgroup of G , then $\phi(H)$ is a subgroup of G' .
 4. If K' is a subgroup of G' , then $\phi^{-1}(K')$ is a subgroup of G .

Loosely speaking, ϕ preserves the identity, inverses, and subgroups.

- Let $\phi : G \rightarrow G'$ be a homomorphism of groups. The subgroup $\phi^{-1}(\{e'\})$, consisting of all elements of G mapped by ϕ into the identity e' of G' , is the **kernel of ϕ** , denoted by $\text{Ker}(\phi)$. Note: as $\{e'\}$ is a subgroup of G' , the above theorem shows that the kernel is a subgroup of G .
- **(Theorem)** Let $\phi : G \rightarrow G'$ be a group homomorphism, and let $H = \text{Ker}(\phi)$. Let $a \in G$. Then the set

$$\phi^{-1}\{\phi(a)\} = \{x \in G \mid \phi(x) = \phi(a)\}$$

is the left coset aH of H , and is also the right coset Ha of H . Consequently, the two partitions of G into left cosets and into right cosets of H are the same.

- **(Corollary)** A group homomorphism $\phi : G \rightarrow G'$ is a one-to-one map iff $\text{Ker}(\phi) = \{e\}$.
- A subgroup H of a group G is **normal** if its left and right cosets coincide, that is, if $gH = Hg$ for all $g \in G$. Note: all subgroups of abelian groups are normal, so is the kernel of a homomorphism by theorem above.
- A homomorphism $\phi : G \rightarrow G'$ that is one-to-one is called a **monomorphism** (like injection.)
- A homomorphism that maps G onto G' is called an **epimorphism** (like surjection.)

3.2 Isomorphism and Cayley's Theorem

DEFINITION AND ELEMENTARY PROPERTIES

- An **isomorphism** $\phi : G \rightarrow G'$ is a homomorphism that is one to one and onto G' . The usual notation is $G \simeq G'$. Note: this is just an extension of our idea of renaming elements to get another group.
- ϕ^{-1} is the **inverse map to** ϕ and is well defined for bijections.
- **(Theorem)** Let \mathcal{G} be any collection of groups, and define $G \simeq G'$ for G and G' in \mathcal{G} if there exists an isomorphism $\phi : G \rightarrow G'$. Then \simeq is an equivalence relation.

HOW TO SHOW THAT GROUPS ARE ISOMORPHIC

- **Step 1.** Define the function ϕ that gives the isomorphism of G with G' , i.e. describe, in some fashion, what $\phi(x)$ is to be in G' for every $x \in G$.
- **Step 2.** Show that ϕ is a one-to-one function.
- **Step 3.** Show that ϕ is onto G' .
- **Step 4.** Show that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$ by computation.
- **(Theorem)** Any infinite cyclic group G is isomorphic to the group \mathbb{Z} of integers under addition.
- There is only one group of order 1, one group of order 2, and one group of order 3 up to isomorphism. There are two groups of order 4 up to isomorphism, namely \mathbb{Z}_4 and the Klein 4-group V . There are at least two groups of order 6 up to isomorphism, namely \mathbb{Z}_6 and S_3 .

HOW TO SHOW THAT GROUPS ARE NOT ISOMORPHIC

- Show there are no one-to-one functions. For finite groups, for example, the orders could be different.
- Show one group has a **structural property** that the other doesn't: cyclic, abelian, order, finiteness, number of elements with certain order, solutions for equations (e.g. $x^2 = a$ has solutions in one group but not another.)
- $\mathbb{Z} \not\simeq \mathbb{Q}$ under addition because \mathbb{Z} is cyclic and \mathbb{Q} is not.
- $\mathbb{Q}^* \not\simeq \mathbb{R}^*$ under multiplication as $x^3 = 2$ has a solution in \mathbb{R}^* but not in \mathbb{Q}^* .

CAYLEY'S THEOREM

- Steps for Cayley's proof:
 - **Step 1.** Find a set G' of permutations that is a candidate for forming a group under permutation multiplication isomorphic to G .
 - **Step 2.** Prove that G' is a group under permutation multiplication.
 - **Step 3.** Define a mapping $\phi : G \rightarrow G'$ and show that ϕ is an isomorphism of G with G' .
- **(Cayley's Theorem)** Every group is isomorphic to a group of permutations.
- The group $G' = \{\lambda_a \mid a \in G\}$ where $\lambda_a(x) = ax$ is the **left regular representation** of G , and the group $G'' = \{\rho_a \mid a \in G\}$ where $\rho_a(x) = xa$ is the **right regular representation** of G (ρ for right, λ for left multiplication.)

3.3 Factor Groups

FACTOR GROUPS FROM HOMOMORPHISMS

- **(Theorem)** Let $\phi : G \rightarrow G'$ be a group homomorphism with kernel H . Then the cosets of H form a group, G/H , whose binary operation defines the product $(aH)(bH)$ of two cosets by choosing elements a and b from the cosets, and letting $(aH)(bH) = (ab)H$. Also, the map $\mu : G/H \rightarrow \phi(G)$ defined by $\mu(aH) = \phi(a)$ is an isomorphism.
- Note: elements of G/H are aH where $a \in G$. Identity is H and $(aH)^{-1} = a^{-1}H$.
- A thing is **well-defined** if it is independent of any choices made in its computation.

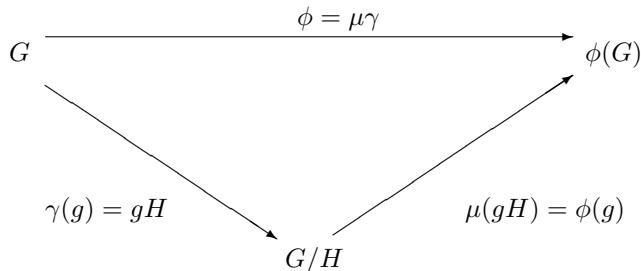
FACTOR GROUPS FROM NORMAL SUBGROUPS

- **(Theorem)** Let H be a subgroup of a group G . Then left coset multiplication is well-defined by the equation

$$(aH)(bH) = (ab)H$$
 iff left and right cosets coincide, so that $aH = Ha$ for all $a \in G$.
- **(Corollary)** Let H be a subgroup of G whose left and right cosets coincide. Then the cosets of H form a group G/H under the binary operation $(aH)(bH) = (ab)H$.
- The group G/H above is the **factor group** (or **quotient group**) of G **modulo** H . The elements in the same coset of H are said to be **congruent modulo** H .
- The following three conditions are equivalent characterizations for a normal subgroup H of a group G :
 1. $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.
 2. $gHg^{-1} = H$ for all $g \in G$.
 3. $gH = Hg$ for all $g \in G$.
- An isomorphism $\phi : G \rightarrow G'$ is an **automorphism** of G . The automorphism $i_g : G \rightarrow G$ where $i_g(x) = gxg^{-1}$ is the **inner automorphism of G by g** .
- The equivalence of conditions 1 and 3 above shows that the normal subgroups of a group G are precisely those that are **invariant** under all inner automorphisms of G .

FUNDAMENTAL HOMOMORPHISM THEOREM

- **(Theorem)** Let H be a normal subgroup of G . Then, $\gamma : G \rightarrow G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H . Note: this is the converse of a homomorphism giving rise to a natural factor group, namely $G/\text{Ker}(G)$.
- **(Fundamental Homomorphism Theorem)** Let $\phi : G \rightarrow G'$ be a group homomorphism with kernel H . Then $\phi(G)$ is a group, and the map $\mu : G/H \rightarrow \phi(G)$ given by $\mu(gH) = \phi(g)$ is an isomorphism. If $\gamma : G \rightarrow G/H$ is the homomorphism given by $\gamma(g) = gH$, then for each $g \in G$, we have $\phi(g) = \mu\gamma(g)$. Note: μ is the **natural** or **canonical isomorphism**. γ is the corresponding homomorphism.



3.4 Factor-Group Computations and Simple Groups

- Two extreme examples:
 1. $N = \{0\}$ is the trivial subgroup of \mathbb{Z} and is normal. $\mathbb{Z}/\{0\} \simeq \mathbb{Z}$, there's no collapsing, and each $x \in \mathbb{Z}$ is simply renamed $\{x\}$ in $\mathbb{Z}/\{0\}$.
 2. $n\mathbb{R} = \{nr \mid r \in \mathbb{R}\}$ is a subgroup of \mathbb{R} under addition and is normal as \mathbb{R} is abelian. As $n\mathbb{R} = \mathbb{R}$, $\mathbb{R}/n\mathbb{R}$ is the trivial group consisting only of the identity. Everything is collapsed.

Note: neither is important as the factor group gives no information about the structure of the original group.

- **(Theorem)** Let $G = H \times K$ be the direct product of groups H and K . Then $\overline{H} = \{(h, e) \mid h \in H\}$ is a normal subgroup of G . Also, G/\overline{H} is isomorphic to K in a natural way. Similarly, $G/\overline{K} \simeq H$ in a natural way. Note: intuitively, we collapse one of the factors to the identity.
- **(Theorem)** A factor group of a cyclic group is cyclic.

SIMPLE GROUPS

- A group is **simple** if it has no proper nontrivial normal subgroups.
- **(Theorem)** The alternating group A_n is simple for $n \geq 5$.
- **(Theorem)** Let $\phi : G \rightarrow G'$ be a group homomorphism. If N is a normal subgroup of G , then $\phi(N)$ is a normal subgroup of $\phi(G)$. Also, if N' is a normal subgroup of $\phi(G)$, then $\phi^{-1}(N')$ is a normal subgroup of G (homomorphisms preserve normal subgroups between group and its image).
- A **maximal normal subgroup of a group** G is a normal subgroup M not equal to G such that there is no proper normal subgroup N of G properly containing M .
- **(Theorem)** M is a maximal normal subgroup of G iff G/M is simple.

COMMUTATOR SUBGROUPS

- The set of all commutators $aba^{-1}b^{-1}$ of a group G generates a normal subgroup G' (the **commutator subgroup**) of G , and G/G' is abelian. Furthermore, G/N is abelian iff $G' \leq N$.

3.5 Series of Groups

SUBNORMAL AND NORMAL SERIES

- A **subnormal** (or **subvariant**) **series of a group** G is a finite sequence H_1, H_2, \dots, H_n of subgroups of G such that $H_i < H_{i+1}$ and H_i is a normal subgroup of H_{i+1} with $H_0 = \{e\}$ and $H_n = G$. A **normal** (or **invariant**) **series of** G is a finite sequence H_1, H_2, \dots, H_n of normal subgroups of G such that $H_i < H_{i+1}$, $H_0 = \{e\}$, and $H_n = G$. Note: for abelian groups, subnormal and normal series coincide. A normal series is always subnormal, but converse may not be true.
- A subnormal (normal) series $\{K_j\}$ is a **refinement of a subnormal (normal) series** $\{H_i\}$ of a group G if $\{H_i\} \subseteq \{K_j\}$, that is, if each H_i is one of the K_j . Note: refinements are larger!
- Two subnormal (normal) series $\{H_i\}$ and $\{K_j\}$ of the same group G are **isomorphic** if there is a one-to-one correspondence between the collections of factor groups $\{H_{i+1}/H_i\}$ and $\{K_{j+1}/K_j\}$ such that the corresponding factor groups are isomorphic.

THE JORDAN-HÖLDER THEOREM

- **(Schreier theorem)** Two subnormal (normal) series of a group G have isomorphic refinements. Proof in 3.1.

- A subnormal series $\{H_i\}$ of a group G is a **composition series** if all the factor groups H_{i+1}/H_i are simple. A normal series $\{H_i\}$ of G is a **principal** or **chief series** if all the factor groups H_{i+1}/H_i are simple. Note: again, for abelian groups, composition and principal series coincide. Also, every principal series is a composition series for any group, as normals are subnormal.
- To form a composition series for a group G , we just hunt for a maximal normal subgroup H_{n-1} of G , then for a maximal normal subgroup of H_{n-1} , and so on. If this terminates in a finite number of steps, we have a composition series (note that the series and no further refinement.) To form a principal series, do the same but H_{n-1} must be normal in G .
- (**Jordan-Hölder theorem**) Any two composition (principal) series of a group G are isomorphic.
- Regard composition series as a type of factorization of the group into simple factor groups, analogous to the factorization of a positive integer into primes.
- (**Theorem**) If G has a composition (principal) series, and if N is a proper normal subgroup of G , then there exists a composition (principal) series containing N .
- A group is **solvable** if it has a composition series $\{H_i\}$ such that all factor groups H_{i+1}/H_i are abelian. By Jordan-Hölder, every composition series of a solvable group must have abelian factor groups.
- The group A_5 of order 60 is the smallest group that is not solvable (note $\{e\} < A_5 < S_5$ is a composition series and $A_5/\{e\}$ is isomorphic to A_5 which is not abelian.)

THE CENTER AND THE ASCENDING CENTRAL SERIES

- The **center of a group** G is the set of all $a \in G$ such that $ax = xa$ for all $x \in G$, that is, the set of all elements of G that commute with every element of G .
- (**Theorem**) The center of a group is a normal subgroup of the group.
- For G , let $Z(G)$ be the center. Then $Z(G/Z(G))$ is normal in $G/Z(G)$ by above and if $\gamma : G \rightarrow G/Z(G)$ is the canonical homomorphism, then $Z_1(G) = \gamma^{-1}[Z(G/Z(G))]$ is a normal subgroup of G . We can then form $Z_2(G) = \gamma_1^{-1}[Z(G/Z_1(G))]$ and so on.

- The series

$$\{e\} \leq Z(G) \leq Z_1(G) \leq Z_2(G) \leq \dots$$

is the **ascending central series of the group** G .

- Example: For D_4 , $\{\rho_0\} \leq \{\rho_0, \rho_2\} \leq D_4 \leq D_4 \leq \dots$

3.6 Groups in Geometry, Analysis, and Art

Note: chapter not essential so only interesting useful facts are included.

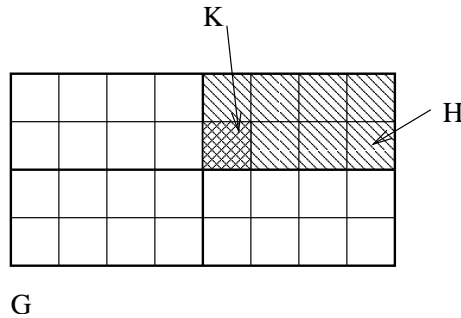
- By a **transformation of a set** A , a geometer means a permutation of the set, that is, a one-to-one function of A onto itself. Recall that the transformations of a set form a group under transformation (permutation) multiplication (simply function composition.)
- A **geometry** is the study of those properties of space (set) that remain invariant under some fixed subgroup of the full transformation group.
- If A is a set on which an idea of distance is defined, a transformation ϕ of A is an **isometry** if $d(x, y) = d(\phi(x), \phi(y))$, that is, if ϕ preserves distance.
- The **Euclidean geometry** of the line, plane, 3-space, and so on is exactly the study of those properties left invariant under the group of isometries (a subgroup of the transformation group.)
- **Topology** is the study of properties of continuous spaces that are invariant under the group of bicontinuous transformations.

4 Advanced Group Theory

4.1 Isomorphism Theorems: Proof of the Jordan-Hölder Theorem

THE ISOMORPHISM THEOREMS

- **(First isomorphism theorem)** Let $\phi : G \rightarrow G'$ be a homomorphism with kernel K , and let $\gamma_K : G \rightarrow G/K$ be the canonical homomorphism. There is a unique isomorphism $\psi : G/K \rightarrow \phi(G)$ such that $\phi(x) = \psi(\gamma_K(x))$ for each $x \in G$ (this is the fundamental theorem from 2.3.)
- Recall: $H, N \leq G$, then $HN = \{hn \mid h \in H, n \in N\}$.
- The **join** $H \vee N$ of $H, N \leq G$ is the intersection of all subgroups of G that contain HN ; that is, $H \vee N$ is the smallest subgroup of G containing HN .
- **(Lemma)** If N is a normal subgroup of G , and if H is any subgroup of G , then $H \vee N = HN = NH$. Furthermore, if H is also normal in G , then HN is normal in G .
- **(Second isomorphism theorem)** Let H be a subgroup of G and let N be a normal subgroup of G . Then $(HN)/N \simeq H/(H \cap N)$.
- If $K \leq H \leq G$, and K and H are both normal in G , then H/K is a normal subgroup of G/K (subgroup follows from H being a subgroup, $(gK)(hK)(g^{-1}K) = (ghg^{-1})K = h_1K \in H/K$ as H is normal.)
- **(Third isomorphism theorem)** Let H and K be normal subgroups of a group G with $K \leq H$. Then $G/H \simeq (G/K)/(H/K)$ (Note: easy way to remember is to see that the K factors “cancel.”)



THE ZASSENHAUS (BUTTERFLY) LEMMA

- **(Zassenhaus Lemma)** Let H and K be subgroups of a group G and let H^* and K^* be normal subgroups of H and K respectively. Then
 1. $H^*(H \cap K^*)$ is a normal subgroup of $H^*(H \cap K)$.
 2. $K^*(H^* \cap K)$ is a normal subgroup of $K^*(H \cap K)$.
 3. $H^*(H \cap K)/H^*(H \cap K^*) \simeq K^*(H \cap K)/K^*(H^* \cap K)$
 $\simeq (H \cap K)/[(H^* \cap K)(H \cap K^*)]$.

PROOF OF THE SCHREIER THEOREM

The proof proceeds by showing isomorphism between specific refinements of two subnormal (normal) series using the Zassenhaus lemma. Note that the isomorphism shown is between the factor groups as required and this is shown via the third assertion of the Zassenhaus lemma.

4.2 Group Action on a Set

THE NOTION OF A GROUP ACTION

- We may view a binary operation on S as a function mapping $S \times S$ into S (more sophisticated view.)
- Let X be a set and G a group. An **action of G on X** is a map $* : G \times X \rightarrow X$ such that
 1. $ex = x$ for all $x \in X$,
 2. $(g_1)(g_2)(x) = g_1(g_2x)$ for all $x \in X$ and for all $g_1, g_2 \in G$.

Under these conditions, X is a **G -set**.

- We can show that every G -set is isomorphic to a disjoint union of left coset G -sets.

ISOTROPY SUBGROUPS

- Let X be a G -set. Define $X_g = \{x \in X \mid gx = x\}$ and $G_x = \{g \in G \mid gx = x\}$. X_g consists of elements unaffected by action g . G_x consists of actions that don't affect element x .
- **(Theorem)** Let X be a G -set. Then G_x is a subgroup of G for each $x \in X$. We call G_x the **isotropy subgroup of x** (or the stabilizer of x in G .)

ORBITS

- **(Theorem)** Let X be a G -set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ iff there exists $g \in G$ such that $gx_1 = x_2$. Then \sim is an equivalence relation on S .
- Let X be a G -set. Each cell in the partition of the equivalence relation described in the above theorem is an **orbit in X under G** . If $x \in X$, the cell containing x is the **orbit of x** . We let this cell be Gx .
- **(Theorem)** Let X be a G -set and let $x \in X$. Then $|Gx| = (G : G_x)$.
- Note: proof shows that the elements of G carrying x into g_1x are precisely the elements of the left coset g_1G_x .

4.3 Application of G -Sets to Counting

- **(Burnside Theorem)** Let G be a finite group and X a finite G -set. If r is the number of orbits in X under G , then

$$r \cdot |G| = \sum_{g \in G} |X_g|.$$

- **(Corollary)** If G is a finite group and X is a finite G -set, then

$$(\text{number of orbits in } X \text{ under } G) = \frac{1}{|G|} \cdot \sum_{g \in G} |X_g|.$$

4.4 Sylow Theorems

p -GROUPS

Throughout this section, p is a prime integer.

- Let X be a finite G -set with r orbits under G . Let $\{x_1, x_2, \dots, x_r\}$ be representative elements from each orbit, where the first s belong to one element orbits. If we let X_G be the union of all one element orbits, $X_G = \{x \in X \mid gx = x, \forall g \in G\}$, then $|X_G| = s$ and

$$|X| = \sum_{i=1}^r |G_{x_i}| = |X_G| + \sum_{i=s+1}^r |G_{x_i}|$$

- **(Theorem)** Let G be a group of order p^n and let X be a finite G -set. Then, $|X| \equiv |X_G| \pmod{p}$.

- A group G is a **p -group** if every element in G has order a power of the prime p . A subgroup of a group G is a **p -subgroup of G** if the subgroup is itself a p -group.
- **(Cauchy's Theorem)** Let G be a finite group and let p divide $|G|$. Then G has an element of order p and, consequently, a subgroup of order p .
- **(Corollary)** Let G be a finite group. Then G is a p -group iff $|G|$ is a power of p .

THE SYLOW THEOREMS

- Let G be a group and let \mathcal{S} be the collection of all subgroups of G . We make \mathcal{S} a G -set by letting G act on \mathcal{S} by **conjugation**: $H \in \mathcal{S}$ then $H \leq G$ and g acting on H yields gHg^{-1} . $G_H = \{g \in G \mid gHg^{-1} = H\}$ is the isotropy subgroup of H in G . H is a normal subgroup of G_H so G_H is the largest subgroup of G having H as a normal subgroup (in a sense, we define a group by taking those elements which qualify H as a normal subgroup.)
- The subgroup $G_H = \{g \in G \mid gHg^{-1} = H\}$ is the **normalizer of H in G** and will be denoted $N[H]$. Again, $H \leq N[H]$ and is normal in $N[H]$.
- Explanation: the isotropy group of H in G when the group action is conjugation becomes the normalizer.
- **(Lemma)** Let H be a p -subgroup of a finite group G . Then

$$(N[H] : H) \equiv (G : H) \pmod{p}.$$

- **(Corollary)** Let H be a p -subgroup of a finite group G . If p divides $(G : H)$, then $N[H] \neq H$.
- **(First Sylow Theorem)** Let G be a finite group and let $|G| = p^n m$ where $n \geq 1$ and where p doesn't divide m . Then
 1. G contains a subgroup of order p^i for each i where $1 \leq i \leq n$,
 2. Every subgroup H of G of order p^i is a normal subgroup of a subgroup of order p^{i+1} for $1 \leq i < n$.
- A **Sylow p -subgroup** P of a group G is a maximal p -subgroup of G , that is, a p -subgroup contained in no larger p -subgroup. Note: first Sylow theorem implies that the Sylow p -subgroups are precisely those subgroups of order p^n (as Cauchy's corollary implies they are p -groups.) Every conjugate of a Sylow p -subgroup is also a Sylow p -subgroup.
- **(Second Sylow Theorem)** Let P_1 and P_2 be Sylow p -subgroups of a finite group G . Then P_1 and P_2 are conjugate subgroups of G . Note: in particular, $P_1 = x^{-1}P_2x$, where $xP_1 \in \mathcal{L}_{P_2}$ and \mathcal{L} is the collection of left cosets of P_1 .
- **(Third Sylow Theorem)** If G is a finite group and p divides $|G|$, then the number of Sylow p -subgroups is congruent to 1 modulo p and divides $|G|$ (proof also tells us that $\mathcal{L}_P = \{P\}$ where \mathcal{L} is set of all Sylow p -subgroups.)
- *Never underestimate a theorem that counts something, even modulo p .*

4.5 Applications of the Sylow Theory

APPLICATIONS TO p -GROUPS AND THE CLASS EQUATION

- **(Theorem)** Every group of prime power order (that is, every finite p -group) is solvable. (Proof from 3rd Sylow)

- If we let G act on G by conjugation, then $G_G = Z(G)$, that is, the union of one-element orbits in G is the same as the center of G . We let $c = |Z(G)|$ and $n_i = |Gx_i|$. Then, $|X| = |X_G| + \sum_{i=s+1}^r |Gx_i|$ of last section becomes the **class equation**

$$|G| = c + n_{c+1} + \cdots + n_r$$

where n_i is the number of elements in the i th orbit of G under conjugation by itself. Note that n_i divides $|G|$ for $c+1 \leq i \leq r$ as we know $|Gx_i| = (G : Gx_i)$. Each orbit in G under conjugation by G is a **conjugate class in G** .

- **(Theorem)** The center of a nontrivial p -group G is nontrivial. (Proof using class eqn and $e \in Z(G)$.)
- **(Lemma)** Let G be a group containing normal subgroups H and K such that $H \cap K = \{e\}$ and $H \vee K = G$. Then G is isomorphic to $H \times K$. (build isomorphism)
- **(Theorem)** For a prime number p , every group G of order p^2 is abelian.

FURTHER APPLICATIONS

- **(Theorem)** If p and q are distinct primes with $p < q$, then every group G of order pq has a single subgroup of order q and this subgroup is normal in G . Hence G is not simple. If q is not congruent to 1 modulo p , then G is abelian and cyclic. (there is one Sylow p -subgroup and one q -subgroup and $G \simeq Z_q \times Z_p$ by above lemma.)
- **(Lemma)** If H and K are finite subgroups of a group G , then

$$|HK| = \frac{(|H|)(|K|)}{|H \cap K|}.$$

Note: lemma says that a finite group can't have large subgroups with small intersections or the order of the product would exceed the order of the group.

- A subgroup H of index 2 in a finite group G is always normal. (2 cosets, H and not in H).

4.6 Free Abelian Groups

FREE ABELIAN GROUPS

- **(Theorem)** Let X be a subset of a nonzero abelian group G . The following conditions on X are equivalent.
 1. Each nonzero element a in G can be *uniquely* expressed in the form $a = n_1x_1 + n_2x_2 + \cdots + n_rx_r$ for $n_i \neq 0$ in \mathbb{Z} and distinct $x_i \in X$.
 2. X generates G , and $n_1x_1 + n_2x_2 + \cdots + n_rx_r = 0$ for $n_i \in \mathbb{Z}$ and $x_i \in X$ iff $n_1 = n_2 = \cdots = n_r = 0$.
- An abelian group having a nonempty generating set X satisfying the conditions in above theorem is a **free abelian group**, and X is a **basis** for the group. (Note: it is "free" of relations.)
- Example: the finite direct product of the group \mathbb{Z} with itself are free abelian groups with the natural bases.
- **(Theorem)** If G is a nonzero free abelian group with a basis of r elements, then G is isomorphic to $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ for r factors.
- **(Theorem)** Let $G \neq \{0\}$ be a free abelian group with a finite basis. Then every basis of G is finite, and all bases have the same number of elements. (size is $\log_2 |G/2G|$).
- If G is a free abelian group, the **rank** of G is the number of elements in a basis for G . (All bases have the same number of elements.)

PROOF OF THE FUNDAMENTAL THEOREM
Refer to Section 1.8

- **(Theorem)** Let G be a finitely generated abelian group with generating set $\{a_1, a_2, \dots, a_n\}$. Let

$$\phi : \mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z} \rightarrow G$$

(n factors of \mathbb{Z}) to be defined by $\phi(h_1, h_2, \dots, h_n) = h_1 a_1 + h_2 a_2 + \dots + h_n a_n$. Then ϕ is a homomorphism onto G . (easily seen)

- **(Theorem)** If $X = \{x_1, x_2, \dots, x_r\}$ is a basis for a free abelian group G and $t \in \mathbb{Z}$, then for $i \neq j$, the set

$$Y = \{x_1, x_2, \dots, x_{j-1}, x_j + t x_i, x_{j+1}, \dots, x_r\}$$

is also a basis for G . This is a “replacement property.” Note: you just add a different basis element.

- **(Theorem)** Let G be a nonzero free abelian group of finite rank n , and let K be a nonzero subgroup of G . Then K is free abelian of rank $s \leq n$. Furthermore, there exists a basis $\{x_1, x_2, \dots, x_n\}$ for G and positive integers d_1, d_2, \dots, d_s where d_i divides d_{i+1} for $i = 1, \dots, s-1$ such that $\{d_1 x_1, d_2 x_2, \dots, d_s x_s\}$ is a basis for K .

- **(Theorem)** Every finitely generated abelian group is isomorphic to a group of the form

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_r} \times \mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z},$$

where m_i divides m_{i+1} for $i = 1, \dots, r-1$.

- Mostly done: prime-power decomposition exists by breaking groups into prime-power factors. Betti number is the rank of the free abelian group G/T where T is the torsion subgroup of G and this rank is invariant and so unique. Uniqueness of torsion coefficients and prime-powers is harder to show.

4.7 Free Groups

WORDS AND REDUCED WORDS

- let A be any set of elements a_i for $i \in I$. We may think of A as an **alphabet** and of the a_i as **letters** in the alphabet. Any symbol of the form a_i^n with $n \in \mathbb{Z}$ is a **syllable** and a finite string w of syllables written in juxtaposition is a **word**. The **empty word** 1 does not have any syllables.
- The **elementary contractions** let us modify words naturally: replace $a_i^m a_i^n$ by a_i^{m+n} , and drop a_i^0 . We get a **reduced word** when no more elementary contractions are possible. Note: formally, elementary contractions are manipulations of integer exponents.

FREE GROUPS

- Let the set of all reduced words formed from alphabet A be $F[A]$. Define $w_1 \cdot w_2$ be the reduced form of the word obtained by juxtaposition $w_1 w_2$ of the two words. Then, $F[A]$ is the **free group generated** by A .
- If G is a group with a set $A = a_i$ of generators, and if G is isomorphic to $F[A]$ under a map $\phi : G \rightarrow F[A]$ such that $\phi(a_i) = a_i$, then G is **free on** A , and the a_i are **free generators of** G . A group is **free** if it is free on some nonempty set A .
- \mathbb{Z} is free on one generator. Clearly, all free groups are infinite.
- **(Theorem)** If a group G is free on A and also on B then the sets A and B have the same number of elements; that is, any two sets of free generators of a free group have the same cardinality. (no proof)
- If G is free on A , the number of elements in A is the **rank of the free group** G .

- **(Theorem)** Two free groups are isomorphic iff they have the same rank.
- **(Theorem)** A nontrivial proper subgroup of a free group is free. Note: rank of subgroup might be higher than group.

HOMOMORPHISMS OF FREE GROUPS

- **(Theorem)** Let G be generated by $A = \{a_i \mid i \in I\}$ and let G' be any group. If a'_i for $i \in I$ are any elements in G' , not necessarily distinct, then there is at most one homomorphism $\phi : G \rightarrow G'$ such that $\phi(a_i) = a'_i$. If G is free on A , then there is exactly one such homomorphism. (homomorphism is completely determined by its values on generating set.)
- Note: in particular, a homomorphism of a cyclic group is completely determined by its value on a single generator of a group.
- **(Theorem)** Every group G' is a homomorphic image of a free group G .
- If G is free abelian with given basis X form the free group $F[X]$, form the factor group of $F[X]$ modulo its commutator subgroup, and you have a group isomorphic to G .

4.8 Group Presentations

DEFINITION

- Let A be a set and let $\{r_i\} \subseteq F[A]$. Let R be the least normal subgroup of $F[A]$ containing the r_i . An isomorphism ϕ of $F[A]/R$ onto a group G is a **presentation of G** . The sets A and $\{r_i\}$ give a **group presentation**. The set A is the set of **generators for the presentation** and each r_i is a **relator**. Each $r \in R$ is a **consequence of $\{r_i\}$** . An equation $r_i = 1$ is a **relation**. A **finite presentation** is one in which both A and $\{r_i\}$ are finite sets.
- If a group presentation has generators x_j and relators r_i , we use $(x_j : r_i)$ or $(x_j : r_i = 1)$ as notation.
- Note: $\prod_j x_j (r_{i_j}^{n_j}) x_j^{-1}$ will have to be equal to 1 in the new group. All these finite products do form a normal subgroup.

ISOMORPHIC PRESENTATIONS

- Example: $(a : a^6 = 1)$ and $(a, b : a^2, b^3, aba^{-1}b^{-1})$ are both isomorphic to \mathbb{Z}_6 .
- When two different presentations give isomorphic groups, we have **isomorphic presentations**.
- The presentation isomorphism problem, whether a group given by a presentation is finite, free, abelian, or trivial, as well as the word problem of determining whether a given word r is a consequence of a given set of relators are unsolvable.
- Every group has a presentation (see last theorem in 3.7.)

APPLICATIONS

- Groups of order 10 are isomorphic to \mathbb{Z}_{10} or D_5 .
- Groups of order 8 are isomorphic to $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4$ or the quaternion group.
- Exercise 11: $(a, b : a^m = 1, b^n = 1, ba = a^r b)$ gives a group of order mn iff $r^n \equiv 1 \pmod{m}$.

5 Introduction to Rings and Fields

5.1 Rings and Fields

DEFINITIONS AND BASIC PROPERTIES

- A **ring** $\langle R, +, \cdot \rangle$ is a set R together with two binary operations $+$ and \cdot , which we call addition and multiplication, defined on R such that the following axioms are satisfied:
 - \mathcal{R}_1 $\langle R, + \rangle$ is an abelian group.
 - \mathcal{R}_2 Multiplication is associative.
 - \mathcal{R}_3 For $a, b, c \in R$. the **left distributive law**, $a(b + c) = (ab) + (ac)$, and the **right distributive law**, $(a + b)c = (ac) + (bc)$, hold.
- Note: \cdot is a binary operation, so R is closed under it.
- Examples: $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$, and $\langle \mathbb{C}, +, \cdot \rangle$. Let R be any ring. Then, $M_n(R)$ is a ring. $\langle F, +, \cdot \rangle$ is a ring. $\langle \mathbb{Z}_n, +, \cdot \rangle$ is a ring where \cdot is **multiplication modulo n** .
- Notation: 0 as additive identity of ring. $n > 0$, $na = a + a + \cdots + a$. with n summands. $n < 0$, $na = (-a) + (-a) + \cdots + (-a)$ with $|n|$ summands. $0 \cdot a = 0$ where $0 \in \mathbb{Z}$ on the left and $0 \in R$ on the right.
- By convention, multiplication comes before addition. We incorrectly refer to a ring $\langle R, +, \cdot \rangle$ as R .
- **(Theorem)** If R is a ring with additive identity 0 , then for any $a, b \in R$ we have
 1. $0a = a0 = 0$,
 2. $a(-b) = (-a)b = -(ab)$,
 3. $(-a)(-b) = ab$.

HOMOMORPHISMS AND ISOMORPHISMS

- Let R and R' be rings. A map $\phi : R \rightarrow R'$ is a **homomorphism** if the following two properties are satisfied for all $a, b \in R$:
 1. $\phi(a + b) = \phi(a) + \phi(b)$.
 2. $\phi(ab) = \phi(a)\phi(b)$.
- Note: ϕ is a group homomorphism, so all results on group homomorphisms are valid for the additive structure of the rings. In particular, ϕ is one to one iff $\text{Ker}(\phi) = \{a \in R \mid \phi(a) = 0'\}$ is just the subset $\{0\}$ of R .
- Example: For $\langle F, +, \cdot \rangle$, $\phi_a : F \rightarrow \mathbb{R}$, for $a \in \mathbb{R}$, $\phi_a(f) = f(a)$ is the **evaluation homomorphism**.
- An **isomorphism** $\phi : R \rightarrow R'$ from a ring R to a ring R' is a homomorphism that is one to one and onto R' . The rings R and R' are **isomorphic**.
- We refer to $\langle n\mathbb{Z}, +, \cdot \rangle$ as $n\mathbb{Z}$.

MULTIPLICATIVE QUESTIONS; FIELDS

- A ring in which the multiplication is commutative is a **commutative ring**. A ring R with a multiplicative identity 1 such that $1x = x1 = x$ for all $x \in R$ is a **ring with unity**. A multiplicative identity in a ring is **unity**.
- We exclude the ring $\{0\}$ as the **trivial ring**. It is the only ring with a zero multiplicative identity.

- **(Theorem)** If R is a ring with unity, then this unity 1 is the only multiplicative identity (we assume it to be nonzero.)
- If R_i are rings, the ring $R_1 \times R_2 \times \cdots \times R_n$ is the **direct product** of the rings R_i , where operations are by components.
- A **multiplicative inverse** of an element a in a ring R with unity 1 is an element a^{-1} such that $aa^{-1} = a^{-1}a = 1$ (it is unique.)
- Let R be a ring with unity. An element u in R is a **unit of R** if it has a multiplicative inverse in R . If every nonzero element of R is a unit, then R is a **division ring**. A **field** is a commutative division ring. A noncommutative division ring is a **skew ring**.
- Exercise 25: collection U of all units in a ring with unity is a group under multiplication (in particular, closed.)
- Examples: \mathbb{Z} is not a field, \mathbb{Q} and \mathbb{R} are.
- A **subring of a ring** is a subset of the ring that is a ring under the induced operations from the whole ring; a **subfield** is defined similarly for a subset of a field.

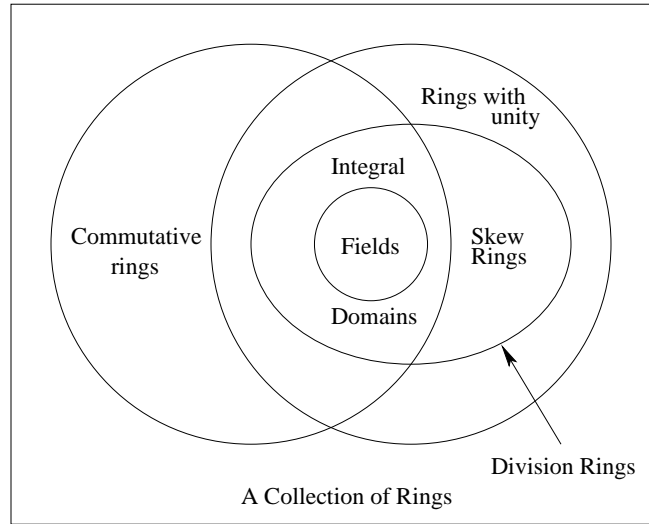
5.2 Integral Domains

DIVISORS OF ZERO AND CANCELLATION

- If a and b are two nonzero elements of a ring R such that $ab = 0$, then a and b are **divisors of 0** (or **0 divisors**). In particular, a is a **left divisor of 0** and b is a **right divisor of 0**.
- **(Theorem)** In the ring \mathbb{Z}_n , the divisors of 0 are precisely those elements that are not relatively prime to n .
- **(Corollary)** If p is a prime, then \mathbb{Z}_p has no divisors of 0.
- The (multiplicative) **cancellation laws** hold in R if $ab = ac$ with $a \neq 0$ implies $b = c$, and $ba = ca$ with $a \neq 0$ implies $b = c$.
- **(Theorem)** The cancellations laws hold in R iff R has no left or right divisors of 0.
- In a ring R with no divisors of 0, $ax = b, a \neq 0$ has one solution. If R has unity and a is a unit in R with multiplicative inverse a^{-1} , then solution is $a^{-1}b$. If ring is commutative, $ba^{-1} = a^{-1}b$ and we may use quotient b/a as notation. In a field F , we define a **quotient** b/a as the solution x in F of the equation $ax = b$. In particular, the multiplicative inverse of $a \in F$ is $1/a$.

INTEGRAL DOMAINS

- An **integral domain** D is a commutative ring with unity containing no divisors of 0. Example: \mathbb{Z}, \mathbb{Z}_p for p prime. Note: cancellation laws hold.
- **(Theorem)** Every field F is an integral domain. Note: fields are richest (most restrictive).
- **(Theorem)** Every finite integral domain is a field. (show inverses exist by counting.)
- **(Corollary)** If p is a prime, then \mathbb{Z}_p is a field.



THE CHARACTERISTIC OF A RING

- If for a ring R a positive integer n exists such that $n \cdot a = 0$ for all $a \in R$, then the least such positive integer is the **characteristic of the ring R** . If no such positive integer exists, then R is of **characteristic 0**. Note: $n \cdot a$ refers to a sum of n a s.
- Examples: \mathbb{Z}_n is of characteristic n , while $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ all have characteristic 0.
- If R is a ring with unity 1, then R has characteristic $n > 0$ iff n is the smallest positive integer such that $n \cdot 1 = 0$.
- The characteristic of a subdomain is equal to that of the domain. The characteristic of an integral domain is either 0 or a prime p . If it's 0, it is infinite.

5.3 Fermat's and Euler's Theorems

FERMAT'S THEOREM

- The cosets of $\mathbb{Z}/n\mathbb{Z}$ are closed under multiplication by representative. Associative and distributive laws hold. Therefore, the cosets form an isomorphic field to \mathbb{Z}_n .
- **(Fermat's Little Theorem)** If $a \in \mathbb{Z}$ and p is any prime not dividing a , then p divides $a^{p-1} - 1$, that is, $a^{p-1} \equiv 1 \pmod{p}$ for $a \not\equiv 0 \pmod{p}$. (look at isomorphic rings.)
- **(Corollary)** If $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$ for any prime p .
- Primes of the form $2^p - 1$ for p a prime are known as **Mersenne primes**.

EULER'S GENERALIZATION

- **(Theorem)** The set G_n of nonzero elements of \mathbb{Z}_n that are not 0 divisors forms a group under multiplication modulo n .
- Define $\phi(n)$ or the **Euler phi-function** as the number of positive integers less than or equal to n and relatively prime to n . We know that $\phi(n)$ is the number of elements of \mathbb{Z}_n that are not divisors of n .
- **(Euler's Theorem)** If a is an integer relatively prime to n , then $a^{\phi(n)} - 1$ is divisible by n , that is, $a^{\phi(n)} \equiv 1 \pmod{n}$.

APPLICATION TO $ax \equiv b \pmod{m}$

- **(Theorem)** Let m be a positive integer and let $a \in \mathbb{Z}_m$ be relatively prime to m . For each $b \in \mathbb{Z}_m$, the equation $ax = b$ has a unique solution in \mathbb{Z}_m . ($a^{-1}b$)
- **(Corollary)** If a and m are relatively prime integers, then for any integer b , the congruence $ax \equiv b \pmod{m}$ has as solutions all integers in precisely one residue class modulo m .
- **(Theorem)** Let m be a positive integer and let $a, b \in \mathbb{Z}_m$. Let d be the gcd of a and m . The equation $ax = b$ has a solution in \mathbb{Z}_m iff d divides b . When d divides b , the equation has exactly d solutions in \mathbb{Z}_m .
- **(Corollary)** Let d be the gcd of positive integers a and m . The congruence $ax \equiv b \pmod{m}$ has a solution iff d divides b . When this is the case, the solutions are the integers in exactly d distinct residue classes modulo m .
- To solve $ax \equiv b \pmod{m}$:
 1. Find $d = \gcd(a, m)$. If d doesn't divide b , there is no solution. Otherwise, let $a_1 = a/d$, $b_1 = b/d$, and $m_1 = m/d$.
 2. Solve $a_1x \equiv b_1 \pmod{m_1}$ to get s . Note: unique solution in \mathbb{Z}_{m_1} .
 3. Solutions are integers in residue classes $s + km_1 + (m\mathbb{Z})$ for $0 \leq k < d$ (d solutions in \mathbb{Z}_m .)

5.4 The Field of Quotients of an Integral Domain

THE CONSTRUCTION

- Let D be an integral domain we desire to enlarge to a field of quotients F . We take the following steps:
 1. Define what the elements of F are to be. $D \times D = \{(a, b) \mid a, b \in D\}$. Let S be a subset of $D \times D$, $S = \{(a, b) \mid a, b \in D, b \neq 0\}$.
 - Two elements (a, b) and (c, d) in S are **equivalent**, denoted by $(a, b) \sim (c, d)$, iff $ad = bc$.
 - **(Lemma)** The relation \sim between elements of S is an equivalence relation. (uses commutativity of D and cancellation laws!)
 - Let $[(a, b)]$ be the equivalence class of (a, b) in S under \sim .
 We define F to be the set of all equivalence classes $[(a, b)]$ for $(a, b) \in S$.
 2. Define the binary operations of addition and multiplication on F .
 - **(Lemma)** For $[(a, b)]$ and $[(c, d)]$ in F , the equations

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)]$$

and

$$[(a, b)][(c, d)] = [(ac, bd)]$$

give well-defined operations of addition and multiplication on F . (esp. use of D having no 0 divisors)

3. Check all the field axioms to show that F is a field under these operations.
 - (a) Addition is commutative. (abelian)
 - (b) Addition is associative. (group)
 - (c) $[(0, 1)]$ is an identity for addition in F . (group)
 - (d) $[(-a, b)]$ is an additive inverse for $[(a, b)]$ in F . (group)
 - (e) Multiplication in F is associative. (ring)
 - (f) Multiplication in F is commutative.
 - (g) The distributive laws hold in F . (ring)
 - (h) $[(1, 1)]$ is a multiplicative identity in F . (unity)

- (i) If $[(a, b)] \in F$ is not the additive identity, then $a \neq 0$ in D and $[(b, a)]$ is a multiplicative inverse for $[(a, b)]$. (division)

Note: F is also an integral domain as it has no 0 divisors (it inherits that from D).

4. Show that F can be viewed as containing D as an integral subdomain.

- (**Lemma**) The map $i : D \rightarrow F$ given by $i(a) = [(a, 1)]$ is an isomorphism of D with a subdomain of F .

- Note: $[(a, b)] = [(a, 1)][(1, b)] = [(a, 1)]/[(b, 1)] = i(a)/i(b)$ holds in F
- (**Theorem**) Any integral domain D can be enlarged to (or embedded in) a field F such that every element of F can be expressed as a quotient of two elements of D . (Such a field F is a **field of quotients of D**).

UNIQUENESS

- (**Theorem**) Let F be a field of quotients of D and let L be any field containing D . Then there exists a map $\psi : F \rightarrow L$ that gives an isomorphism of F with a subfield of L such that $\psi(a) = a$ for $a \in D$. ($\psi(a) = a, a \in D$ and $\psi(a/Fb) = \psi(a)/_L\psi(b)$).
- (**Corollary 1**) Every field L containing an integral domain D contains a field of quotients of D . (Note: $\psi(F) \leq L$).
- (**Corollary 2**) Any two fields of quotients of an integral domain D are isomorphic (ψ becomes onto.)

5.5 Rings of Polynomials

POLYNOMIALS IN AN INDETERMINATE

- We call a variable an **indeterminate**.
- Let R be a ring. A **polynomial $f(x)$ with coefficients in R** is an infinite formal sum

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n + \cdots,$$

where $a_i \in R$ and $a_i = 0$ for all but a finite number of values of i . The a_i are **coefficients of $f(x)$** . If for some $i > 0$ it is true that $a_i \neq 0$, the largest such value of i is the **degree of $f(x)$** . If no such $i > 0$ exists, then $f(x)$ is of **degree zero**. Addition and multiplication of polynomials are defined in the usual way.

- An element of R is a **constant polynomial**.
- (**Theorem**) The set $R[x]$ of all polynomials in an indeterminate x with coefficients in a ring R is a ring under polynomial addition and multiplication. If R is commutative, then so is $R[x]$, and if R has unity 1, then 1 is also unity for $R[x]$.
- We can form the ring $(R[x])[y]$ which actually is $(R[y])[x]$ so we consider it $R[x, y]$, the **ring of polynomials in two indeterminates x and y with coefficients in R** . We can do n indeterminates similarly.
- If F is a field, then $F[x]$ is an integral domain but not a field. We can construct the field of quotients $F(x)$ of $F[x]$. For n indeterminates, this is the **field of rational functions in n indeterminates over F** .

THE EVALUATION HOMOMORPHISMS

- **(Theorem)** Let F be a subfield of a field E , let α be any element of E , and let x be an indeterminate. The map $\phi_\alpha : F[x] \rightarrow E$ defined by

$$\phi_\alpha(a_0 + a_1x + \cdots + a_nx^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

for $(a_0 + a_1x + \cdots + a_nx^n) \in F[x]$ is a homomorphism of $F[x]$ into E . Also, $\phi_\alpha(x) = \alpha$, and ϕ_α maps F isomorphically by the identity map; that is, $\phi_\alpha(a) = a$ for $a \in F$. The homomorphism ϕ_α is **evaluation at α** . Note: also true if F and E are commutative rings with unity.

- Interesting example: $\phi_\pi : \mathbb{Q}[x] \rightarrow \mathbb{R}$ is an isomorphism, that is, all formal polynomials in π with rational coefficients form a ring isomorphic to $\mathbb{Q}[x]$ in a natural way with $\phi_\pi(x) = \pi$.

THE NEW APPROACH

- Let F be a subfield of a field E and let α be an element of E . Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be in $F[x]$, and let $\phi_\alpha : F[x] \rightarrow E$ be the evaluation homomorphism. Let $f(\alpha)$ denote

$$\phi_\alpha(f(x)) = a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

If $f(\alpha) = 0$, then α is a **zero of $f(x)$** .

OUR BASIC GOAL

- Pythagoreans asserted that all distances are **commensurable**, that is, given distances a and b , there exists a unit distance u such that $a = nu$ and $b = mu$ for integers n and m . This is equivalent to asserting all numbers are rational.
- **(Theorem)** The equation $x^2 = 2$ has no solutions in rational numbers. Thus $\sqrt{2}$ is not a rational number.
- **Our basic goal** is to show that given any polynomial of degree ≥ 1 , where the coefficients of the polynomial may be from any field, we can find (or construct) a zero of this polynomial.

5.6 Factorization of Polynomials over a Field

- Let $E \leq F$ be fields. Suppose $f(x) \in F[x]$ has factors in $F[x]$. Then $f(x) = g(x)h(x)$, $h(x), g(x) \in F[x]$. For $\alpha \in E$, we have

$$f(\alpha) = \phi_\alpha(f(x)) = \phi_\alpha(g(x)h(x)) = \phi_\alpha(g(x))\phi_\alpha(h(x)) = g(\alpha)h(\alpha).$$

Thus, if $\alpha \in E$, then $f(\alpha) = 0$ iff either $g(\alpha) = 0$ or $h(\alpha) = 0$. We reduce the problem to finding a zero of f to finding zeros of factors of f . This is our motivation.

THE DIVISION ALGORITHM IN $F[x]$

- **(Division algorithm for $F[x]$)** Let

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$$

and

$$g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_0$$

be two elements of $F[x]$, with a_n and b_m both nonzero elements of F and $m > 0$. Then there are unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$, with the degree of $r(x)$ less than m , degree of $g(x)$.

- **(Corollary 1)** An element $a \in F$ is a zero of $f(x) \in F[x]$ iff $x - a$ is a factor of $f(x)$ in $F[x]$ (we divide by long division.)

- **(Corollary 2)** A nonzero polynomial $f(x) \in F[x]$ of degree n can have at most n zeros in a field F .

IRREDUCIBLE POLYNOMIALS

- A nonconstant polynomial $f(x) \in F[x]$ is **irreducible over F** or is an **irreducible polynomial in $F[x]$** if $f(x)$ cannot be expressed as a product $g(x)h(x)$ of two polynomials $g(x)$ and $h(x)$ in $F[x]$ both of lower degree than the degree of $f(x)$. Note: f might be irreducible in F but not in $E \geq F$.
- Let $f(x) \in F[x]$, and let $f(x)$ be of degree 2 or 3. Then $f(x)$ is reducible over F iff it has a zero in F .
- **(Theorem)** If $f(x) \in \mathbb{Z}[x]$, then $f(x)$ factors into a product of two polynomials of lower degrees r and s in $\mathbb{Q}[x]$ iff it has such a factorization with polynomials of the same degrees r and s in $\mathbb{Z}[x]$. (Proof in 6.1)
- **(Corollary)** If $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ is in $\mathbb{Z}[x]$ with $a \neq 0$, and if $f(x)$ has a zero in \mathbb{Q} , then it has a zero m in \mathbb{Z} , and m must divide a_0 . Note: therefore, check the divisors of a_0 .
- **(Eisenstein Theorem)** Let $p \in \mathbb{Z}$ be a prime. Suppose that $f(x) = a_nx^n + \dots + a_0$ is in $\mathbb{Z}[x]$, and $a_n \not\equiv 0 \pmod{p}$, but $a_i \equiv 0 \pmod{p}$ for $i < n$, with $a_0 \not\equiv 0 \pmod{p^2}$. Then $f(x)$ is irreducible over \mathbb{Q} . (show in \mathbb{Z} by contradiction)
- **(Corollary)** The cyclotomic polynomial

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

is irreducible over \mathbb{Q} for any prime p . (show $\Phi_p(x + 1)$ is irreducible using Eisenstein)

UNIQUENESS OF FACTORIZATION IN $F[x]$

- For $f(x), g(x) \in F[x]$, we say that $g(x)$ **divides $f(x)$ in $F[x]$** if there exists $q(x) \in F[x]$ such that $f(x) = g(x)q(x)$.
- **(Theorem)** Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides $r(x)s(x)$ for $r(x), s(x) \in F[x]$, then either $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$. (proof in 5.2)
- **(Corollary)** If $p(x)$ is irreducible in $F[x]$ and $p(x)$ divides the product $r_1(x) \cdot \dots \cdot r_n(x)$ for $r_i(x) \in F[x]$, then $p(x)$ divides $r_i(x)$ for at least one i . (induct)
- **(Theorem)** If F is a field, then every nonconstant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials which are unique except for order and for unit (that is, a nonzero constant) factors in F .

5.7 Noncommutative Examples

RINGS OF ENDOMORPHISMS

- Let A be any abelian group. A homomorphism of A into itself is an **endomorphism of A** . We call the set of all endomorphisms of A $\text{Hom}(A)$. Define addition by $\phi, \psi \in \text{Hom}(A)$, $(\phi + \psi)(a) = \phi(a) + \psi(a)$ and multiplication by function composition (which is associative.) With $0(a) = e$ as identity, $(\text{Hom}(A), +)$ forms an abelian group.
- The set A^A of all functions from A into A also forms an abelian group. However, it cannot be made into a ring because the left distributive law does not hold.
- **(Theorem)** The set $\text{Hom}(A)$ of all endomorphisms of an abelian group A forms a ring under homomorphism addition and homomorphism multiplication (function composition.) Note: $\text{Hom}(A)$ need not be commutative, as function composition isn't.
- We can specify an endomorphism by giving its values on the generators of the group.

GROUP RINGS AND GROUP ALGEBRAS

- Let $G = \{g_i \mid i \in I\}$ be any multiplicative group, and let R be any commutative ring with unity. Let $R(G)$ be the set of all formal sums

$$\sum_{i \in I} a_i g_i$$

for $a_i \in R$ and $g_i \in G$, where all but a finite number of a_i are 0. Define the sum of two elements of $R(G)$ by

$$\left(\sum_{i \in I} a_i g_i \right) + \left(\sum_{i \in I} b_i g_i \right) = \sum_{i \in I} (a_i + b_i) g_i$$

Clearly, $(a_i + b_i) = 0$ except for a finite number of indices, so the sum is in $R(G)$. It is immediate that $\langle R(G), + \rangle$ is an abelian group with additive identity $\sum_{i \in I} 0 g_i$. We define multiplication by

$$\left(\sum_{i \in I} a_i g_i \right) \left(\sum_{i \in I} b_i g_i \right) = \sum_{i \in I} \left(\sum_{g_j g_k = g_i} a_j b_k \right) g_i.$$

Again, multiplication is closed on $R(G)$.

- **(Theorem)** If G is any multiplicative group, then $\langle R(G), +, \cdot \rangle$ is a ring.
- $R(G)$ contains G naturally as a multiplicative subsystem. Thus, $R(G)$ is not commutative if G isn't abelian.
- The ring $R(G)$ defined above is the **group ring of G over R** . If F is a field, then $F(G)$ is the **group algebra of G over F** .

THE QUATERNIONS

- The quaternions \mathcal{Q} form a skew field under addition and multiplication.
- **(Wedderburn Theorem)** A finite division ring is a field. (no proof given.)

6 Factor Rings and Ideals

6.1 Homomorphisms and Factor Rings

HOMOMORPHISMS

- A map ϕ of a ring R into a ring R' is a **homomorphism** if

$$\phi(a + b) = \phi(a) + \phi(b)$$

and

$$\phi(ab) = \phi(a)\phi(b)$$

for all element a and b in R . (repeated from 4.1)

PROPERTIES OF HOMOMORPHISMS

- Definitions and theorems are analogs of those in Chapter 2.

- **(Theorem)** Let ϕ be a homomorphism of a ring R into a ring R' . If 0 is the additive identity in R , then $\phi(0) = 0'$ is the additive identity in R' , and if $a \in R$, then $\phi(-a) = -\phi(a)$. If S is a subring of R , then $\phi(S)$ is a subring of R' . Going the other way, if S' is a subring of R' , then $\phi^{-1}(S')$ is a subring of R . Finally, if R has unity 1 and $\phi(1) \neq 0'$, then $\phi(1)$ is unity for $\phi(R)$. Loosely speaking, subrings correspond to subrings, and rings with unity to rings with unity under a ring homomorphism.
- Let a map $\phi : R \rightarrow R'$ be a homomorphism of rings. The subring $\phi^{-1}(\{0'\})$ is the **kernel** of ϕ , denoted by $\text{Ker}(\phi)$. Note: same as kernel for group homomorphism of associated groups.
- **(Theorem)** Let $\phi : R \rightarrow R'$ be a ring homomorphism, and let $H = \text{Ker}(\phi)$. Let $a \in R$. Then $\phi^{-1}\{\phi(a)\} = a + H = H + a$, where $a + H = H + a$ is the coset containing a of the commutative additive group $\langle H, + \rangle$. Note: as abelian, right and left sets always match.
- **(Corollary)** A ring homomorphism $\phi : R \rightarrow R'$ is a one-to-one map iff $\text{Ker}(\phi) = \{0\}$.

ISOMORPHISMS OF RINGS

- An **isomorphism** $\phi : R \rightarrow R'$ is a homomorphism that is one to one and onto R' .
- **(Theorem)** Let \mathcal{R} be any collection of rings, and define $R \simeq R'$ for R and R' in \mathcal{R} if there exists an isomorphism $\phi : R \rightarrow R'$. Then \simeq is an equivalence relation.

FACTOR (QUOTIENT) RINGS

- **(Theorem)** Let $\phi : R \rightarrow R'$ be a ring homomorphism with kernel H . Then the additive cosets of H form a ring R/H whose binary operations are defined by choosing representatives. That is, the sum of two cosets is defined by

$$(a + H) + (b + H) = (a + b) + H$$

and the product of the cosets is define by

$$(a + H)(b + H) = (ab) + H.$$

Also, the map $\mu : R/H \rightarrow \phi(R)$ defined by $\mu(a + H) = \phi(a)$ is an isomorphism.

- **(Theorem)** Let H be a subring of the ring R . Multiplication of additive cosets of H is well defined by the equation

$$(a + H)(b + H) = (ab) + H.$$

iff $ah \in H$ and $hb \in H$ for all $a, b \in R$ and $h \in H$.

- A subring N of a ring R satisfying the properties

$$aN \subseteq N \quad \text{and} \quad Nb \subseteq N \quad \text{for all} \quad a, b \in R$$

is an **ideal**. Note: analogs of normal subgroups.

- **(Corollary)** Let N be an ideal of a ring R . Then, the additive cosets of N form a ring R/N with the binary operations defined by

$$(a + N) + (b + N) = (a + b) + N$$

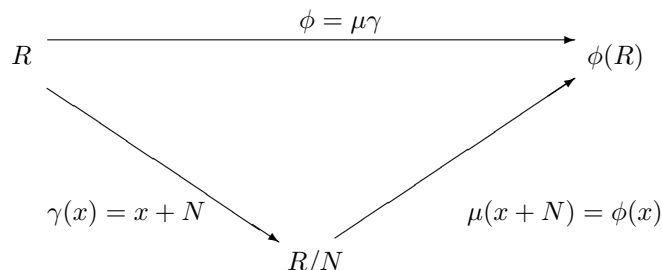
and

$$(a + N)(b + N) = (ab) + N.$$

- The ring R/N in the preceding corollary is the **factor ring** (or **quotient ring**) of R modulo N .

FUNDAMENTAL HOMOMORPHISM THEOREM

- **(Theorem)** Let N be an ideal of a ring R . Then $\gamma : R \rightarrow R/N$ given by $\gamma(x) = x + N$ is a ring homomorphism with kernel N .
- **Fundamental homomorphism theorem** Let $\phi : R \rightarrow R'$ be a ring homomorphism with kernel N . Then $\phi(R)$ is a ring, and the map $\mu : R/N \rightarrow \phi(R)$ given by $\mu(x + N) = \phi(x)$ is an isomorphism. If $\gamma : R \rightarrow R/N$ is the homomorphism given by $\gamma(x) = x + N$, then for each $x \in R$, we have $\phi(x) = \mu\gamma(x)$.



- **(Theorem)** Let $\phi : R \rightarrow R'$ be a homomorphism and let N be an ideal of R . Then $\phi(N)$ is an ideal of $\phi(R)$, although it might not be an ideal of R' . Also, if N' is an ideal of either $\phi(R)$ or R' , then $\phi^{-1}(N')$ is an ideal of R .

6.2 Prime and Maximal Ideals

- A ring might have factor rings with better or worse structure.
- Every ring R has two ideals, the **improper ideal** R and the **trivial ideal** $\{0\}$. A **proper nontrivial ideal of R** is an ideal N such that $N \neq R$ and $N \neq \{0\}$.
- **(Theorem)** If R is a ring with unity and N is an ideal of R containing a unit, then $N = R$. (show that unity is in N)
- **(Corollary)** A field contains no nontrivial ideals.

MAXIMAL AND PRIME IDEALS

- Definitions and theorems are analogs of those in Chapter 2.
- A **maximal ideal of a ring R** is an ideal M different from R such that there is no proper ideal N of R properly containing M .
- **(Theorem)** Let R be a commutative ring with unity. Then M is a maximal ideal of R iff R/M is a field. Note: R/M being a field means that it has no proper nontrivial ideals or it's "simple."
- **(Corollary)** A commutative ring with unity is a field iff it has no proper nontrivial ideals.
- An ideal $N \neq R$ in a commutative ring R is a **prime ideal** if $ab \in N$ implies either $a \in N$ or $b \in N$ for $a, b \in R$.
- **(Theorem)** Let R be a commutative ring with unity, and let $N \neq R$ be an ideal in R . Then R/N is an integral domain iff N is a prime ideal in R . (easy proof)
- **(Corollary)** Every maximal ideal in a commutative ring R with unity is a prime ideal.
- We have demonstrated: for a commutative ring R with unity
 1. An ideal M of R is maximal iff R/M is a field.
 2. An ideal N of R is prime iff R/N is an integral domain.

3. Every maximal ideal of R is a prime ideal.

PRIME FIELDS

- **(Theorem)** If R is a ring with unity 1, then the map $\phi : \mathbb{Z} \rightarrow R$ given by

$$\phi(n) = n \cdot 1$$

for $n \in \mathbb{Z}$ is a homomorphism of \mathbb{Z} into R . Recall: $n \cdot 1 = 1 + 1 + \cdots + 1$ for n summands.

- **(Corollary)** If R is a ring with unity and characteristic $n > 1$, then R contains a subring isomorphic to \mathbb{Z}_n . If R has characteristic 0, then R contains a subring isomorphic to \mathbb{Z} . (proof using theorem in 4.2)
- **(Theorem)** A field F is either of prime characteristic p and contains a subfield isomorphic to \mathbb{Z}_p or of characteristic 0 and contains a subfield isomorphic to \mathbb{Q} . (every field containing an integral domain contains a field of quotients of that domain - 4.4)
- The fields \mathbb{Z}_p and \mathbb{Q} are **prime fields**. Note: these are the fundamental building blocks on which all fields rest.

IDEAL STRUCTURE IN $F[x]$

- If R is a commutative ring with unity and $a \in R$, the ideal $\{ra \mid r \in R\}$ of all multiples of a is the **principal ideal generated by a** and is denoted by $\langle a \rangle$. An ideal N of R is a **principal ideal** if $N = \langle a \rangle$ for some $a \in R$. Note: principal ideals are analogs of cyclic subgroups.
- Example: the ideal $\langle x \rangle$ in $F[x]$ consists of all polynomials with zero constant term.
- **(Theorem)** If F is a field, every ideal in $F[x]$ is principal. (use division algorithm.)
- **(Theorem)** An ideal $\langle p(x) \rangle \neq \{0\}$ of $F[x]$ is maximal iff $p(x)$ is irreducible over F .

APPLICATION TO UNIQUE FACTORIZATION IN $F[x]$

- Note: theorem was given without proof in section 4.6.
- **(Theorem)** Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides $r(x)s(x)$, for $r(x), s(x) \in F[x]$, then either $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$. (easy, using last theorem)

A PREVIEW OF OUR BASIC GOAL

- Outline of the Proof:
 1. Let $p(x)$ be an irreducible factor of $f(x)$ in $F[x]$.
 2. Let E be the field $F[x]/\langle p(x) \rangle$.
 3. Show that no two different elements of F are in the same coset of $F[x]/\langle p(x) \rangle$, and deduce that we may consider F to be isomorphic to a subfield of E .
 4. Let α be the coset $x + \langle p(x) \rangle$. Show that for the evaluation homomorphism $\phi_\alpha : F[x] \rightarrow E$, we have $\phi_\alpha(f(x)) = 0$. That is, α is a zero of $f(x)$ in E .

7 Factorization

7.1 Unique Factorization Domains

- Let D be an integral domain and $a, b \in D$. If there exists $c \in D$ such that $b = ac$, then a **divides** b (or a is a **factor of** b), denoted by $a|b$.
- An element u of an integral domain D is a **unit of** D if u divides 1, that is, if u as a multiplicative inverse in D . Two elements $a, b \in D$ are **associates in** D if $a = bu$, where u is a unit in D .
- Examples: the only units in \mathbb{Z} are 1 and -1. The associates of 26 in \mathbb{Z} are 26 and -26.
- A nonzero element p that is not a unit of an integral domain D is an **irreducible of** D if in any factorization $p = ab$ in D either a or b is a unit. Note: an associate of an irreducible is an irreducible.
- An integral domain D is a **unique factorization domain** (abbreviated UFD) if the following conditions are satisfied:
 1. Every element of D that is neither 0 nor a unit can be factored into a product of a finite number of irreducibles.
 2. If $p_1 \cdots p_r$ and $q_1 \cdots q_s$ are two factorizations of the same element of D into irreducibles, then $r = s$ and the q_j can be renumbered so that p_i and q_i are associates.
- Example: $F[x]$ and \mathbb{Z} are UFDs.
- An integral domain D is a **principal ideal domain** (abbreviated PID) if every ideal in D is a principal ideal.

EVERY PID IS A UFD

- In general, concepts are generalizations of 4.6.
- If $\{A_i \mid i \in I\}$ is a collection of sets, then the **union** $\bigcup_{i \in I} A_i$ **of the sets** A_i is the set of all x such that $x \in A_i$ for at least one $i \in I$.
- **(Lemma)** Let D be a PID. If $N_1 \subseteq N_2 \subseteq \cdots$ is a monotonic ascending chain of ideals N_i , then there exists a positive integer r such that $N_r = N_s$ for all $s \geq r$. Equivalently, every strictly ascending chain of ideals (all inclusions proper) in a PID is of finite length. We express this by saying that the **ascending chain condition** (ACC) holds for ideals in a PID. (proof by showing union of N_i is an ideal whose generator is in N_r)
- For $a, b \in D$,
 1. $\langle a \rangle \subseteq \langle b \rangle$ iff b divides a ,
 2. $\langle a \rangle = \langle b \rangle$ iff a and b are associates.
- **(Theorem)** Let D be a PID. Every element that is neither 0 nor a unit in D is a product of irreducibles. (use ACC to find irreducible factors) Note: this is UFD's condition 1.
- **(Theorem)** An ideal $\langle p \rangle$ in a PID is maximal iff p is an irreducible. (use equivalences above.)
- **(Lemma)** In a PID, if an irreducible p divides ab , then either $p|a$ or $p|b$. (proof: maximal ideal is prime)
- **(Corollary)** If p is an irreducible in a PID and p divides the product $a_1 a_2 \cdots a_n$ for $a_i \in D$, then $p|a_i$ for at least one i . (induct)
- A nonzero nonunit element p of an integral domain D with the property that $p|ab$ implies either $p|a$ or $p|b$ is a **prime**.

- Note: in a PID, irreducibles are primes by above lemma.
- In a UFD, the concepts of prime and irreducible coincide. But in some domains, they don't. Example: subdomain of $F[x, y]$ generated by x^3, xy, y^3 where x^3, xy, y^3 are irreducible but $x^3y^3 = (xy)(xy)(xy)$.
- **(Theorem)** Every PID is a UFD. (use corollary above)
- **(Corollary: Fundamental Theorem of Arithmetic)** The integral domain \mathbb{Z} is a UFD.
- Note: \mathbb{Z} is a PID because all its subgroups are all in the form $n\mathbb{Z}$ (1.6). As \mathbb{Z} is cyclic and therefore abelian, all its subgroups are normal and cyclic and lead to principal ideals.

IF D IS A UFD, THEN $D[x]$ IS A UFD

- Let D be a UFD. A nonconstant polynomial

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

in $D[x]$ is **primitive** if the only common divisors of all the a_i are units of D .

- **(Lemma)** If D is a UFD, then for every nonconstant $f(x) \in D[x]$ we have $f(x) = (c)g(x)$, where $c \in D$, $g(x) \in D[x]$, and $g(x)$ is primitive. The element c is unique up to a unit factor in D and is the **content** of $f(x)$. Also, $g(x)$ is unique up to a unit factor in D . (c is the gcd)
- **(Lemma - Gauss)** If D is a UFD, then a product of two primitive polynomials in $D[x]$ is again primitive. (expand coefficients of product)
- **(Corollary)** If D is a UFD, then a finite product of primitive polynomials in $D[x]$ is again primitive. (induct)
- **(Lemma)** Let D be a UFD and let F be a field of quotients of D . Let $f(x) \in D[x]$, where $(\text{degree } f(x)) > 0$. If $f(x)$ is an irreducible in $D[x]$, then $f(x)$ is also an irreducible in $F[x]$. Also, if $f(x)$ is primitive in $D[x]$ and irreducible in $F[x]$, then $f(x)$ is irreducible in $D[x]$. (get rid of denominator/obvious)
- **(Corollary)** If D is a UFD and F is a field of quotients of D , then a nonconstant $f(x) \in D[x]$ factors into a product of two polynomials of lower degrees r and s in $F[x]$ iff it has a factorization into polynomials of the same degrees r and s in $D[x]$. Note: proof of theorem in 4.6 regarding \mathbb{Z} and \mathbb{Q} .
- **(Theorem)** If D is a UFD, then $D[x]$ is a UFD. (factorize in $F[x]$ and bring back)
- **(Corollary)** If F is a field and x_1, \dots, x_n are indeterminates, then $F[x_1, \dots, x_n]$ is a UFD. (induct)
- Not all UFDs are PIDs. Example: N , the set of polynomials in $F[x, y]$ (a UFD) with constant term 0 is an ideal but is not principal.

7.2 Euclidean Domains

- Here, we abstract out the properties of a division algorithm.
- A **Euclidean valuation on an integral domain** D is a function ν mapping the nonzero elements of D into the nonnegative integers such that the following conditions are satisfied:
 1. For all $a, b \in D$ with $b \neq 0$, there exist q and r in D such that $a = bq + r$, where either $r = 0$ or $\nu(r) < \nu(b)$.
 2. For all $a, b \in D$, where neither a nor b is 0, $\nu(a) \leq \nu(ab)$.

An integral domain D is a **Euclidean domain** if there exists a Euclidean valuation on D .

- Examples: \mathbb{Z} with $\nu(n) = |n|$ and $F[x]$ for a field F with $\nu(f(x)) = (\text{degree } f(x))$

- **(Theorem)** Every Euclidean domain is a PID.
- **(Corollary)** Every Euclidean domain is a UFD.
- Note: not all PIDs are Euclidean domains, however.

ARITHMETIC IN EUCLIDEAN DOMAINS

- The arithmetic structure of a Euclidean domain D is completely determined by the set D and the operations $+$ and \cdot on D (it is intrinsic) and it is not affected by the valuation.
- **(Theorem)** For a Euclidean domain with a Euclidean valuation ν , $\nu(1)$ is minimal among all $\nu(a)$ for nonzero $a \in D$, and $u \in D$ is a unit iff $\nu(u) = \nu(1)$. (use condition 2)
- Examples: For \mathbb{Z} , the minimum ν for nonzero elements is 1 and so the units are 1 and -1.
- Let D be a UFD. An element $d \in D$ is a **greatest common divisor** (abbreviated gcd) **of elements a and b in D** if $d|a$, $d|b$, and also $c|d$ for all c dividing both a and b . Note: we may find gcds by factorization into irreducibles.
- **(Theorem)** If D is a PID and a and b are nonzero elements of D , then there exists a gcd of a and b . Furthermore, each gcd of a and b can be expressed in the form $\lambda a + \mu b$ for some $\lambda, \mu \in D$. (d is the generator of the ideal $\{ra + sb \mid r, s \in D\}$)
- **(Euclidean Algorithm)** Let D be a Euclidean domain with a Euclidean valuation ν , and let a and b be nonzero elements of D . Let r_1 be as in Condition 1 for a Euclidean valuation, that is,

$$a = bq_1 + r_1,$$

where either $r_1 = 0$ or $\nu(r_1) < \nu(b)$. If $r_1 \neq 0$, let r_2 be such that

$$b = r_1q_2 + r_2,$$

where either $r_2 = 0$ or $\nu(r_2) < \nu(r_1)$. In general, let r_{i+1} be such that

$$r_{i-1} = r_iq_{i+1} + r_{i+1},$$

where either $r_{i+1} = 0$ or $\nu(r_{i+1}) < \nu(r_i)$. Then the sequence r_1, r_2, \dots must terminate with some $r_s = 0$. If $r_1 = 0$, then b is the gcd of a and b . If $r_1 \neq 0$ and r_s is the first $r_i = 0$, then a gcd of a and b is r_{s-1} . (show set of common divisors are same)

- Note: to make the Euclidean algorithm run faster, we take the remainder which has the smallest valuation (take negatives, as the divisors are the same.)

7.3 Gaussian Integers and Norms

GAUSSIAN INTEGERS

- Goal is to show other Euclidean domains.
- A **Gaussian Integer** is a complex number $a + bi$, where $a, b \in \mathbb{Z}$. For a Gaussian integer $\alpha = a + bi$, the **norm** $N(\alpha)$ of α is $a^2 + b^2$. We let $\mathbb{Z}[i]$ be the set of all Gaussian integers. Gaussian integers include all the **rational integers**, that is, all the elements of \mathbb{Z} .
- **(Lemma)** In $\mathbb{Z}[i]$, the following properties of the norm function N hold for all $\alpha, \beta \in \mathbb{Z}[i]$:
 1. $N(\alpha) \geq 0$.
 2. $N(\alpha) = 0$ iff $\alpha = 0$.
 3. $N(\alpha\beta) = N(\alpha)N(\beta)$.

- **(Lemma)** $\mathbb{Z}[i]$ is an integral domain. (gets it from \mathbb{Z} using lemma or inherited from \mathbb{C})
- **(Theorem)** The function $\nu(\alpha) = N(\alpha)$ for nonzero $\alpha \in \mathbb{Z}[i]$ is a Euclidean valuation on $\mathbb{Z}[i]$. Thus $\mathbb{Z}[i]$ is a Euclidean domain. (geometrical proof using lines)

MULTIPLICATIVE NORMS

- In *algebraic number theory*, we study a domain of *algebraic integers* by different valuations which help in determining the arithmetic structure of the domain.
- Let D be an integral domain. A **multiplicative norm** N on D is a function mapping D into the integers \mathbb{Z} such that the following conditions are satisfied:
 1. $N(\alpha) \geq 0$.
 2. $N(\alpha) = 0$ iff $\alpha = 0$.
 3. $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in D$.

Note: same as norm, except in an abstract domain.

- **(Theorem)** If D is an integral domain with a multiplicative norm N , then $N(1) = 1$ and $N(u) = 1$ for every unit in D . If, furthermore, every α such that $N(\alpha) = 1$ is a unit in D , then an element π in D , with $N(\pi) = p$ for a prime $p \in \mathbb{Z}$, is an irreducible of D . (p also an irreducible)
- Note: a Euclidean valuation has $N(u) = N(1)$ for all units, so if $N(1) = 1$, it satisfies theorem.
- Example: $\mathbb{Z}[\sqrt{-5}]$ is an integral domain but not a UFD as $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$.

8 Extension Fields

8.1 Introduction to Extension Fields

OUR BASIC GOAL ACHIEVED

- A field E is an **extension field of a field** F if $F \leq E$. Examples: $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$
- **(Theorem - Kronecker)** Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$. ($\alpha = x + \langle p(x) \rangle$ in $E = F[x]/\langle p(x) \rangle \geq F$ and $F \simeq \{a + \langle p(x) \rangle \mid a \in F\}$.)

ALGEBRAIC AND TRANSCENDENTAL ELEMENTS

- An element α of an extension field E of a field F is **algebraic over** F if $f(\alpha) = 0$ for some nonzero $f(x) \in F[x]$. If α is not algebraic over F , then α is **transcendental over** F . Examples: $\sqrt{2}$ and i are algebraic over $\mathbb{Q} \leq \mathbb{C}$, π and e are transcendental over \mathbb{Q} but algebraic over \mathbb{R} (consider $x - \pi = 0$.)
- An element of \mathbb{C} that is algebraic over \mathbb{Q} is an **algebraic number**. A **transcendental number** is an element of \mathbb{C} that is transcendental over \mathbb{Q} . Note: this is connection to number theory concepts.
- **(Theorem)** Let E be an extension field of a field F and let $\alpha \in E$. Let $\phi_\alpha : F[x] \rightarrow E$ be the evaluation homomorphism of $F[x]$ into E such that $\phi_\alpha(a) = a$ for all $a \in F$ and $\phi_\alpha(x) = \alpha$. Then α is transcendental over F iff ϕ_α gives an isomorphism of $F[x]$ with a subdomain of E , that is, iff ϕ_α is a one-to-one map. ($\text{Ker}(\phi_\alpha) = \{0\}$)

THE IRREDUCIBLE POLYNOMIAL FOR α OVER F

- **(Theorem)** Let E be an extension field of F , and let $\alpha \in E$, where α is algebraic over F . Then there is an irreducible polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$. This irreducible polynomial $p(x)$ is uniquely determined up to a constant factor in F and is a polynomial of minimal degree ≥ 1 in $F[x]$ having α as a zero. If $f(\alpha) = 0$ for $f(x) \in F[x]$, with $f(x) \neq 0$, then $p(x)$ divides $f(x)$. ($p(x)$ is the generator of the principal ideal which is the kernel of ϕ_α)

- A polynomial having 1 as the coefficient of the highest power of x appearing is a **monic polynomial**. In $F[x]$ for a field F , we can always achieve this as we have inverses.
- Let E be an extension field of a field F , and let $\alpha \in E$ be algebraic over F . The unique monic polynomial $p(x)$ of above theorem is the **irreducible polynomial for α over F** and will be denoted by $\text{irr}(\alpha, F)$. The degree of $\text{irr}(\alpha, F)$ is the **degree of α over F** , denoted by $\text{deg}(\alpha, F)$.
- Examples: $\text{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$, $\text{deg}(\sqrt{2}, \mathbb{Q}) = 2$, but $\text{irr}(\sqrt{2}, \mathbb{R}) = x - \sqrt{2}$ so $\text{deg}(\sqrt{2}, \mathbb{R}) = 1$.

SIMPLE EXTENSIONS

- Let E be an extension field of a field F , and let $\alpha \in E$. Let ϕ_α be the evaluation homomorphism of $F[x]$ into E with $\phi_\alpha(a) = a$, for all $a \in F$ and $\phi_\alpha(x) = \alpha$.

Case I. *Suppose α is algebraic over F .* Then, the kernel of ϕ_α is $\langle \text{irr}(\alpha, F) \rangle$ (see above theorem) and is a maximal ideal of $F[x]$ as the generator is irreducible. Therefore, $F[x]/\langle \text{irr}(\alpha, F) \rangle$ is a field and is isomorphic to the image $\phi_\alpha(F[x])$ in E (isomorphism theorems). The subfield $\phi_\alpha(F[x])$ is the smallest subfield of E containing F and α . We shall denote this field by $F(\alpha)$.

Case II. *Suppose α is transcendental over F .* Then by above theorem ϕ_α gives an isomorphism of $F[x]$ with a subdomain of E . Thus in this case, $\phi_\alpha(F[x])$ is not a field but an integral domain which we shall denote by $F[\alpha]$. E contains a field of quotients of $F[\alpha]$, clearly the smallest subfield of E containing F and α , which we denote by $F(\alpha)$ as in Case I. Note: $F(\alpha)$ is essentially just plugging in α into $f(x) \in F[x]$. From a structural point of view, an element that is transcendental over a field F behaves as though it were an indeterminate over F .

- An extension field E of a field F is a **simple extension** of F if $E = F(\alpha)$ for some $\alpha \in E$.
- **(Theorem)** Let E be a simple extension $F(\alpha)$ of a field F , and let α be algebraic over F . Let the degree of $\text{irr}(\alpha, F)$ be $n \geq 1$. Then every element β of $E = F(\alpha)$ can be uniquely expressed in the form

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

where the b_i are in F . (use $\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$)

- Example: as $x^2 + 1$ is irreducible over \mathbb{R} , $\langle x^2 + 1 \rangle$ is a maximal ideal in $\mathbb{R}[x]$ and $\mathbb{R}[x]/\langle x^2 + 1 \rangle$ is a field. It is an extension field of \mathbb{R} as we can identify $r \in \mathbb{R}$ with $r + \langle x^2 + 1 \rangle$. If $\alpha = x + \langle x^2 + 1 \rangle$, then $\mathbb{R}(\alpha) = \mathbb{R}[x]/\langle x^2 + 1 \rangle$ and by above theorem consists of elements of form $a + b\alpha$, for $a, b \in \mathbb{R}$ and $\alpha^2 + 1 = 0$. So, $\mathbb{R}(\alpha) \simeq \mathbb{C}$. We have constructed \mathbb{C} from \mathbb{R} .

8.2 Vector Spaces

DEFINITION AND ELEMENTARY PROPERTIES

- Let F be a field. A **vector space over F** (or **F -vector space**) consists of an abelian group V under addition together with an operation of scalar multiplication of each element of V by each element of F on the left, such that for all $a, b \in F$ and $\alpha, \beta \in V$ the following conditions are satisfied:

$$\mathcal{V}_1. a\alpha \in V.$$

$$\mathcal{V}_2. a(b\alpha) = (ab)\alpha.$$

$$\mathcal{V}_3. (a + b)\alpha = (a\alpha) + (b\alpha).$$

$$\mathcal{V}_4. a(\alpha + \beta) = (a\alpha) + (a\beta).$$

$$\mathcal{V}_5. 1\alpha = \alpha.$$

The elements of V are **vectors** and the elements of F are **scalars**. When only one field F is under discussion, we drop the reference to F and refer to a *vector space*. Examples: $(\mathbb{R}^n, +)$ over \mathbb{R} , $F[x]$ over F , E , an extension field of F over F , etc.

- **(Theorem)** If V is a vector space over F , then $0\alpha = 0$, $a0 = 0$, and $(-a)\alpha = a(-\alpha) = -(a\alpha)$ for all $a \in F$ and $\alpha \in V$. Note: “(0-scaler) α =0-vector”, “a(0-vector)=0-vector.”

LINEAR INDEPENDENCE AND BASES

- Let V be a vector space over F . The vectors in a subset $S = \{\alpha_i \mid i \in I\}$ of V **span** (or **generate** V) if for every $\beta \in V$, we have

$$\beta = a_1\alpha_{i_1} + a_2\alpha_{i_2} + \cdots + a_n\alpha_{i_n}$$

for some $a_j \in F$ and $\alpha_{i_j} \in S$, $j = 1, \dots, n$. A vector $\sum_{j=1}^n a_j\alpha_{i_j}$ is a **linear combination of the** α_{i_j} . Examples: the monomials x^m span $F[x]$ over F , $F(\alpha)$ for $\alpha \in E$ algebraic over F is a vector space over F and is spanned by $\{1, \alpha, \dots, \alpha^{n-1}\}$.

- A vector space V over a field F is **finite dimensional** if there is a finite subset of V whose vectors span V . Note: $F(\alpha)$ by above example is finite dimensional.
- The vectors in a subset $S = \{\alpha_i \mid i \in I\}$ of a vector space V over a field F are **linearly independent over** F if $\sum_{i=1}^n a_j\alpha_{i_j} = 0$ implies that $a_j = 0$ for $j = 1, \dots, n$. If the vectors are not linearly dependent over F , they are **linearly dependent over** F .
- Example: by theorem of last section, $\{1, \alpha, \dots, \alpha^{n-1}\}$ are linearly independent as each element of $F(\alpha)$ is uniquely expressed as a linear combination, in particular, the 0-vector $0 = 0 + 0\alpha + \cdots + 0\alpha^{n-1}$.
- If V is a vector space over a field F , the vectors in a subset $B = \{\beta_i \mid i \in I\}$ of V form a **basis for** V **over** F if they span V and are linearly independent.
- Note: in particular, $\{1, \alpha, \dots, \alpha^{n-1}\}$ form basis for $F(\alpha)$.

DIMENSION

- **(Lemma)** Let V be a vector space over a field F , and let $\alpha \in V$. If α is a linear combination of the vectors β_i for $i = 1, \dots, m$ and each β_i is a linear combination of vectors γ_j for $j = 1, \dots, n$, then α is a linear combination of the γ_j . (easy, show double sum)
- **(Theorem)** In a finite dimensional vector space, every finite set of vectors spanning the space contains a subset that is a basis. (build set by dropping dependent ones)
- **(Corollary)** A finite-dimensional vector space has a finite basis. (subset of a finite spanning set)
- **(Theorem)** Let $S = \{\alpha_1, \dots, \alpha_r\}$ be a finite set of linearly independent vectors of a finite-dimensional vector space V over a field F . Then S can be enlarged to a basis for V over F . Furthermore, if $B = \{\beta_1, \dots, \beta_n\}$ is any basis for V over F , then $r \leq n$. (add α_i to front and form basis from left.)
- **(Corollary)** Any two bases of a finite dimensional vector space V over F have the same number of elements. (squeeze using theorem)
- If V is a finite-dimensional vector space over a field F , the number of elements in a basis (independent of the choice of basis, as just shown) is the **dimension of** V **over** F .
- Example: if $\deg(\alpha, F) = n$ for an algebraic $\alpha \in E$, then the dimension of $F(\alpha)$ as a vector space over F is n .

AN APPLICATION TO FIELD THEORY

- **(Theorem)** Let E be an extension field of F , and let $\alpha \in E$ be algebraic over F . If $\deg(\alpha, F) = n$, then $F(\alpha)$ is an n -dimensional vector space over F with basis $\{1, \alpha, \dots, \alpha^{n-1}\}$. Furthermore, every element β of $F(\alpha)$ is algebraic over F , and $\deg(\beta, F) \leq \deg(\alpha, F)$. (form f for β)

8.3 Additional Algebraic Structures

GROUPS WITH OPERATORS

- A **group with operators** consists of a group G and a set \mathcal{O} , the **set of operators**, together with an operation of external multiplication of each element of G by each element of \mathcal{O} on the left such that for all $\alpha, \beta \in G$ and $a \in \mathcal{O}$, the following conditions are satisfied:

1. $(a\alpha) \in G$.
2. $a(\alpha\beta) = (a\alpha)(a\beta)$.

We shall somewhat incorrectly speak of the \mathcal{O} -group G .

- Example: every abelian group G is a \mathbb{Z} -group with $n\alpha = \alpha^n$ for $\alpha \in G$ and $n \in \mathbb{Z}$. Note: set of operators often has structure.
- Let G be any group and let \mathcal{O} be any set of homomorphisms of G into G (endomorphisms.) Then, as $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$ for $\phi \in \mathcal{O}$ and $\alpha, \beta \in G$, G is an \mathcal{O} -group.
- An **admissible subgroup** or **\mathcal{O} -subgroup** of an \mathcal{O} -group G , is a subgroup H of $\langle G, \cdot \rangle$ such that $a\alpha \in H$ for all $\alpha \in H$ and $a \in \mathcal{O}$.
- Example: let G be any group and \mathcal{I} be the set of all inner automorphisms of G . Then any admissible \mathcal{I} -group of G is a normal subgroup of G .
- (**Jordan-Hölder Theorem**) Any two composition series of an \mathcal{O} -group G are isomorphic. (no proof)

MODULES

- Let R be a ring. A (**left**) **R -module** consists of an abelian group M together with an operation of external multiplication of each element of M by each element of R on the left such that for all $\alpha, \beta \in M$ and $r, s \in R$, the following conditions are satisfied:

1. $(r\alpha) \in M$.
2. $r(\alpha + \beta) = r\alpha + r\beta$.
3. $(r + s)\alpha = r\alpha + s\alpha$.
4. $(rs)\alpha = r(s\alpha)$

An R -module is very much like a vector space except that the scalars need only form a ring. We shall somewhat incorrectly speak of the **R -module** M . If R is a ring with unity and $1\alpha = \alpha$ for all $\alpha \in M$, then M is a **unitary R -module**.

- An R -module M is **cyclic** if there exists $\alpha \in M$ such that $M = \{r\alpha \mid r \in R\}$.
- (**Theorem**) If R is a PID, then every finitely generated R -module is isomorphic to a direct sum of cyclic R -modules. (no proof)

ALGEBRAS

- An **algebra** consists of a vector space V over a field F , together with a binary operation of multiplication on the set V of vectors, such that for all $a \in F$ and $\alpha, \beta, \gamma \in V$, the following conditions are satisfied:

1. $(a\alpha)\beta = a(\alpha\beta) = \alpha(a\beta)$.
2. $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$.
3. $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$.

We shall somewhat incorrectly speak of an **algebra V over F** . Also, V is an **associative algebra over F** , if in addition to the preceding three conditions,

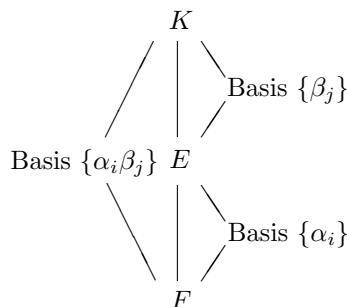
4. $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

- An algebra V over a field F is a **division algebra over F** if V has a unity for multiplication and contains a multiplicative inverse of each nonzero element. (Note that associativity of multiplication is not assumed.)
- **(Theorem)** The real numbers, the complex numbers, and the quaternions are the only (up to isomorphism) associative division algebras over the real numbers (Frobenius, 1878). The only additional division algebra over the real numbers is the Cayley algebra, which is a vector space of dimension 8 over \mathbb{R} (Bott and Milnor, 1957). (no proof)

8.4 Algebraic Extensions

FINITE EXTENSIONS

- An extension field E of a field F is an **algebraic extension of F** if every element in E is algebraic over F .
- If an extension field E of a field F is of finite dimension n as a vector space over F , then E is a **finite extension of degree n over F** . We shall let $[E : F]$ be the degree n of E over F .
- Observe that $[E : F] = 1$ iff $E = F$. (enlarge $\{1\}$ for basis of E)
- **(Theorem)** A finite extension field E of a field F is an algebraic extension of F .



- **(Theorem)** If E is a finite extension field of a field F , and K is a finite extension field of E , then K is a finite extension of F , and

$$[K : F] = [K : E][E : F].$$

(product of bases is a basis)

- **(Corollary 1)** If F_i is a field for $i = 1, \dots, r$ and F_{i+1} is a finite extension of F_i , then F_r is a finite extension of F_1 , and

$$[F_r : F_1] = [F_r : F_{r-1}][F_{r-1} : F_{r-2}] \cdots [F_2 : F_1].$$

- **Corollary 2** If E is an extension field of F , $\alpha \in E$ is algebraic over F , and $\beta \in F(\alpha)$, then $\deg(\beta, F)$ divides $\deg(\alpha, F)$. ($F \leq F(\beta) \leq F(\alpha)$)
- Example of use: there is no element of $\mathbb{Q}(\sqrt{2})$ that's a zero of $x^3 - 2$ as $\deg(\sqrt{2}, \mathbb{Q}) = 2$ but a zero of $x^3 - 2$ is of degree 3 over \mathbb{Q} and 3 doesn't divide 2.
- For $\alpha_i \in E$, $F(\alpha_1, \alpha_2, \dots, \alpha_n)$ is the smallest extension field of F containing all the α_i for $i = 1, \dots, n$. We obtain it by **adjoining to F the elements α_i** in E . It is the intersection of all the subfields containing all the elements (and is therefore a subfield.)

- **(Theorem)** Let E be an algebraic extension of a field F . Then there exist a finite number of elements $\alpha_1, \dots, \alpha_n$ in E such that $E = F(\alpha_1, \dots, \alpha_n)$ iff E is a finite-dimensional vector space over F , that is, iff E is a finite extension of F . (take $\alpha_i \notin F(\alpha_{i-1})$ and continue until you get E)

ALGEBRAICALLY CLOSED FIELDS AND ALGEBRAIC CLOSURES

- **(Theorem)** Let E be an extension field of F . Then

$$\overline{F}_E = \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$$

is a subfield of E , the **algebraic closure of F in E** .

- **(Corollary)** The set of all algebraic numbers forms a field. (it is \mathbb{C} , the algebraic closure of \mathbb{Q})
- A field F is **algebraically closed** if every nonconstant polynomial in $F[x]$ has a zero in F . Note: for $F = \mathbb{C}$, this is true and is the *Fundamental Theorem of Algebra*.
- **(Theorem)** A field F is algebraically closed iff every nonconstant polynomial in $F[x]$ factors in $F[x]$ into linear factors. (easy)
- **(Corollary)** An algebraically closed field F has no proper algebraic extensions, that is, no algebraic extensions E with $F < E$. Note: this means the algebraic enclosure is the maximal algebraic extension.
- **(Theorem)** Every field F has an **algebraic closure**, that is, an algebraic extension \overline{F} that is algebraically closed.
- **(Fundamental Theorem of Algebra)** The field \mathbb{C} of complex numbers is an algebraically closed field. (analytic proof)

PROOF OF THE EXISTENCE OF AN ALGEBRAIC CLOSURE

- A **partial ordering of a set** S is given by a relation \leq defined for certain ordered pairs of elements of S such that the following conditions are satisfied:
 1. $a \leq a$ for all $a \in S$ (**reflexive law**)
 2. If $a \leq b$ and $b \leq a$, then $a = b$ (**antisymmetric law**)
 3. If $a \leq b$ and $b \leq c$, then $a \leq c$ (**transitive law**)

In a partially ordered set, not every two elements need be **comparable**, that is, for $a, b \in S$, you need not have either $a \leq b$ or $b \leq a$. $a < b$ denotes $a \leq b$ but $a \neq b$.

- A subset T of a partially ordered set S is a **chain** if every two elements a and b in T are comparable. An element $u \in S$ is an **upper bound for a subset** A of a partially ordered set S if $a \leq u$ for all $a \in A$. An element m of a partially ordered set S is **maximal** if there is no $s \in S$ such that $m < s$.
- Examples: letting \leq be \subseteq , $\mathbb{Z} \subseteq \mathbb{Q}$ but \mathbb{Z} and \mathbb{Q}^+ are not comparable.
- **(Zorn's Lemma)** If S is a partially ordered set such that every chain in S has an upper bound in S , then S has at least one maximal element. Note: a form of **axiom of choice**.
- Proof idea is to form a set of algebraic extensions of F so large that it contains any conceivable algebraic extension. Then, we define a partial ordering and show Zorn's lemma's hypotheses are satisfied. Hence there is a maximal element, which can be shown to be algebraically closed.

8.5 Geometric Constructions

CONSTRUCTABLE ELEMENTS

- Given a single line segment *one unit* in length, a real number α is **constructible** if we can construct a line segment of length $|\alpha|$ in a finite number of steps from this given segment using a straightedge and a compass.
- **(Theorem)** If α and β are constructible numbers, then so are $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, and α/β , if $\beta \neq 0$.
- **(Corollary)** The set of all constructible real numbers forms a subfield F of the field of real numbers. Note: this set contains \mathbb{Q} as it is the smallest subfield of \mathbb{R} .
- **(Theorem)** The field F of constructible real numbers consists precisely of all real numbers that we can obtain from \mathbb{Q} by taking square roots of positive numbers a finite number of times and applying a finite number of field operations.
- **(Corollary)** If γ is constructible and $\gamma \notin \mathbb{Q}$, then there is a finite sequence of real numbers $\alpha_1, \dots, \alpha_n = \gamma$ such that $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ is an extension of $\mathbb{Q}(\alpha_1, \dots, \alpha_{n-1})$ of degree 2. In particular, $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2^r$ for some integer $r \geq 0$.

THE IMPOSSIBILITY OF CERTAIN CONSTRUCTIONS

- **(Theorem)** “Doubling the cube is impossible,” that is, given a side of a cube, it is not always possible to construct with a straightedge and a compass the side of a cube that has double the volume of the original cube. ($[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 2^r$)
- **(Theorem)** “Squaring the circle is impossible,” that is, given a circle, it’s not always possible to construct with a straightedge and a compass a square having area equal to the area of the given circle. ($\sqrt{(\pi)}$ is transcendental)
- **(Theorem)** “Trisecting the angle is impossible,” that is, there exists an angle that cannot be trisected with a straightedge and a compass. ($[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ where $\alpha = \cos(20)$)

8.6 Finite Fields

- In this section, we show that for every prime p and positive integer n , there is exactly one finite field (up to isomorphism) of order p^n . This field, denoted $\text{GF}(p^n)$ is referred to as the **Galois field of order p^n** .

THE STRUCTURE OF A FINITE FIELD

- **(Theorem)** Let E be a finite extension of degree n over a finite field F . If F has q elements, then E has q^n elements. ($\beta = \sum_{i=1}^n b_i \alpha_i$ for $\beta \in E$, $b_i \in F$, and α_i a basis for E)
- **(Corollary)** If E is a finite field of characteristic p , then E contains exactly p^n elements for some positive integer n , that is, *all finite fields have prime-power order* (E is a finite extension of field isomorphic to \mathbb{Z}_p)
- **(Theorem)** Let E be a field of p^n elements contained in an algebraic closure $\overline{\mathbb{Z}_p}$ of \mathbb{Z}_p . The elements of E are precisely the zeros in $\overline{\mathbb{Z}_p}$ of the polynomial $x^{p^n} - x$ in $\mathbb{Z}_p[x]$. (E^* forms a multiplicative group of order p^{n-1})
- An element α of a field is an **n th root of unity** if $\alpha^n = 1$. It is a **primitive n th root of unity** if $\alpha^n = 1$ and $\alpha^m \neq 1$ for $0 < m < n$.
- Note: this means all nonzero elements of a finite field of p^n elements are $(p^n - 1)$ th roots of unity.
- **(Theorem)** If G is a finite multiplicative subgroup of the multiplicative group $\langle F^*, \cdot \rangle$ of nonzero elements of a field F , then G is cyclic. ($G \simeq \mathbb{Z}_{d_1} \times \dots \times \mathbb{Z}_{d_r} \simeq \mathbb{Z}_m$, where $m = d_1 d_2 \dots d_r$)

- **(Corollary 1)** The multiplicative group of all nonzero elements of a finite field under field multiplication is cyclic.
- **(Corollary 2)** A finite extension E of a finite field F is a simple extension of F . ($E = F(\alpha)$, α generator of E^* shows $E \leq F$ and squeeze)

THE EXISTENCE OF $\text{GF}(p^n)$

- **(Lemma)** If F is a finite field of characteristic p with algebraic closure \overline{F} , then $x^{p^n} - x$ has p^n distinct zeros in \overline{F} . (show each solution α has multiplicity 1 by dividing out $x - \alpha$ and showing α not a solution to quotient)
- **(Theorem)** A finite field $\text{GF}(p^n)$ of p^n elements exists for every prime power p^n . ($\text{GF}(p^n)$ is the subfield of zeros of $x^{p^n} - x$)
- **(Corollary)** If F is any finite field, then for every positive integer n , there is an irreducible polynomial in $F[x]$ of degree n .

9 Automorphisms and Galois Theory

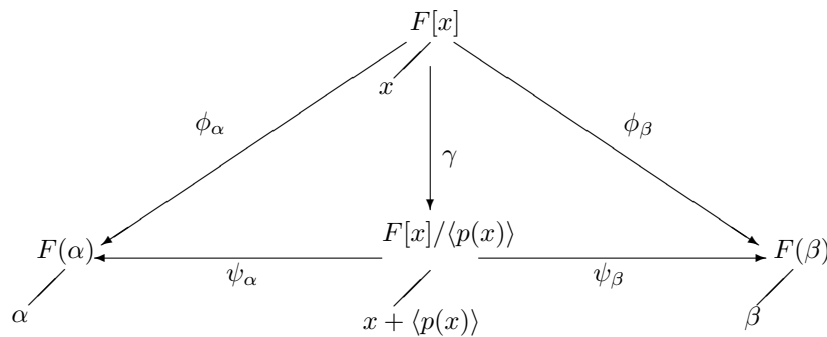
9.1 Automorphisms of Fields

THE BASIC ISOMORPHISMS OF ALGEBRAIC FIELD THEORY

- From now on, we assume that all algebraic extensions and all elements algebraic over a field F under consideration are contained in one fixed algebraic closure \overline{F} of F .
- Let E be an algebraic extension of a field F . Two elements $\alpha, \beta \in E$ are **conjugate over F** if $\text{irr}(\alpha, F) = \text{irr}(\beta, F)$, that is, α and β are zeros of the same irreducible polynomial over F .
- **(Theorem - The basic isomorphisms of algebraic field theory)** Let F be a field, and let α and β be algebraic over F with $\text{deg}(\alpha, F) = n$. The map $\psi_{\alpha, \beta} : F(\alpha) \rightarrow F(\beta)$ defined by

$$\psi_{\alpha, \beta}(c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + \dots + c_{n-1}\beta^{n-1}$$

for $c_i \in F$ is an isomorphism of $F(\alpha)$ onto $F(\beta)$ iff α and β are conjugates.



- **(Corollary 1)** Let α be algebraic over a field F . Every isomorphism ψ mapping $F(\alpha)$ onto a subfield of \overline{F} such that $\psi(a) = a$ for $a \in F$ maps α onto a conjugate β of α over F . Conversely, for each conjugate β of α over F , there exists one isomorphism $\psi_{\alpha, \beta}$ of $F(\alpha)$ onto a subfield of \overline{F} mapping α onto β and mapping each $a \in F$ onto itself. (use $\psi(\alpha)$ as conjugate)
- **(Corollary 2)** Let $f(x) \in \mathbb{R}[x]$. If $f(a + bi) = 0$ for $(a + bi) \in \mathbb{C}$, where $a, b \in \mathbb{R}$, then $f(a - bi) = 0$ also. Loosely, complex zeros of polynomials with real coefficients occur in conjugate pairs. (use $\psi_{i, -i}$)

AUTOMORPHISMS AND FIXED FIELDS

- An isomorphism of a field onto itself is an **automorphism of the field**.
- If σ is an isomorphism of a field E onto some field, then an element a of E is **left fixed by σ** , if $\sigma(a) = a$. A collection S of isomorphisms of E **leaves a subfield F of E fixed** if each $a \in F$ is left fixed by every $\sigma \in S$. If $\{\sigma\}$ leaves F fixed, then σ **leaves F fixed**.
- **(Theorem)** Let $\{\sigma_i \mid i \in I\}$ be a collection of automorphisms of a field E . Then the set $E_{\{\sigma_i\}}$ of all $a \in E$ left fixed by every σ_i for $i \in I$ forms a subfield of E .
- The field $E_{\{\sigma_i\}}$ of above theorem is the **fixed field of $\{\sigma_i \mid i \in I\}$** . For a single automorphism σ , we shall refer to $E_{\{\sigma\}}$ as the **fixed field of σ** .
- Example: $\psi_{\sqrt{2}, -\sqrt{2}}(a + b\sqrt{2}) = a - b\sqrt{2}$ of $\mathbb{Q}(\sqrt{2})$ has \mathbb{Q} as fixed field.
- **(Theorem)** The set of all automorphisms of a field E is a group under function composition. Note: forms subgroup of S_E , group of all permutations of E .
- **(Theorem)** Let E be a field, and let F be a subfield of E . Then the set $G(E/F)$ of all automorphisms of E leaving F fixed forms a subgroup of the group of all automorphisms of E . Furthermore, $F \leq E_{G(E/F)}$.
- The group $G(E/F)$ of the preceding theorem is the **group of automorphisms of E leaving F fixed**, or, more briefly, the **group of E over F** .

THE FROBENIUS AUTOMORPHISM

- We shall show that the group of all automorphisms of a finite field F is cyclic. The Frobenius automorphism or substitution is a generator of the this cyclic group.
- **(Theorem)** Let F be a finite field of characteristic p . Then, the map $\sigma_p(a) = a^p$ for $a \in F$ is an automorphism, the **Frobenius automorphism**, of F . Also, $F_{\{\sigma_p\}} \simeq \mathbb{Z}_p$.