Math 113: Notes

Matin Ghavamizadeh

Spring 2020

Contents

1 Group Theory **2**

1.1 Binary Operations and Structures 2

1.1.1 Properties of Binary Operations 2

1.1.2 Homomorphisms and Isomorphisms 3

1.2 Groups and Subgroups 3

1.3 Group Homomorphisms and Isomorphisms 5

1.4 Cosets and Lagrange's Theorem 6

1.5 Normal Subgroups and Quotient Groups 9

1.6 The Fundamental Homomorphism Theorem 10

1.7 Product Groups 11

2 Special Groups **12**

2.1 Cyclic Groups and $\mathbb{Z}_n$ 12

2.1.1 Classification of Cyclic Groups 13

2.1.2 Some Results in Elementary Number Theory 16

2.2 Permutation Groups 17

2.3 Dihedral Groups 17

3 Rings and Fields **18**

3.1 Definitions and Examples 18

3.2 Ring Homomorphisms, Ideals, and Quotient Rings 22

3.3 Wedderburn's Little Theorem 26

3.4 Field of Fractions of an Integral Domain 26

3.5 Polynomials 27

3.6 Ideals In Polynomial Rings 28

3.7 Field Extensions 28

3.8 Applications to Elementary Number Theory 30

3.9 Polynomial Factorization over $\mathbb{Z}$ and $\mathbb{Q}$ 30

3.9.1 An Alternate Proof of Euler's Theorem 31

3.9.2 Solving $ax = b$ in $\mathbb{Z}/n\mathbb{Z}$ 31

1 Group Theory

1.1 Binary Operations and Structures

Definition 1 (Binary Operation)**.** A binary operation $\circ$, on a set S is a mapping $\circ : S \times S \to S$. The element $\circ(a, b)$ is usually denoted $a \circ b$.

Definition 2 (Binary Structure)**.** A binary structure $(S, \circ)$ is a set equipped with a binary relation $\circ$ on S.

1.1.1 Properties of Binary Operations

Definition 3 (Closure)**.** Let $(S, \circ)$ be a binary structure. $T \subseteq S$ is said to be closed under $\circ$ if

$$\forall x, y \in T; x \circ y \in T.$$

Definition 4 (Commutativity)**.** Let $(S, \circ)$ be a binary structure. $x, y \in S$ are said to commute under $\circ$ if $x \circ y = y \circ x$. If all pairs of elements commute under $\circ$ it is said to be a commutative operation.

Definition 5 (Associativity)**.** Let $(S, \circ)$ be a binary structure. The operation $\circ$ is said to be associative if

$$\forall x, y, z \in S; x \circ (y \circ z) = (x \circ y) \circ z.$$

Definition 6 (Identity Element)**.** Let $(S, \circ)$ be a binary structure. The element $e \in S$ is said to be the identity element under $\circ$ if

$$\forall x \in S; e \circ x = x \circ e = e.$$

Remark (Uniqueness of Identity)**.** Identity elements are unique: suppose e and e' are both identity elements in $(S, \circ)$, then $e = e \circ e' = e'$ by definition. So the phrase, "the identity element of S", makes sense.

Definition 7 (Inverses)**.** Let $(S, \circ)$ be a binary structure. The element $x' \in S$ is said to be an inverse of element $x \in S$ under $\circ$ if

$$x \circ x' = x' \circ c = e,$$

where e is an identity element of $(S, \circ)$.

Remark (notation used for binary operations)**.** It is customary to denote binary structures as $(S, \cdot)$ and write ab instead of $a \cdot b$ for $a, b \in S$. What operation ab refers to depends on the structure a and b belong to. For commutative structures it is customary to use $+$ instead of $\cdot$ and write $a + b$ instead of ab.

1.1.2 Homomorphisms and Isomorphisms

Definition 8 (Homomorphism)**.** Let S and S' be binary structures. The mapping $\varphi : S \to S'$ is said to be a homomorphism if

$$\forall x, y \in S; \varphi(xy) = \varphi(x)\varphi(y).$$

Definition 9 (Isomorphism)**.** Let S and S be binary structures. The mapping $\varphi : S \to S'$ is said to be an isomorphism if it is a bijective homomorphism. The structures S and S' are said to be isomorphic.

Remark (Invariance of Identity under Isomorphisms)**.** The isomorphic image of the identity element is the identity element. Suppose e is the identity in S and $\varphi : S \to S'$ is an isomorphism then for any $y \in S'$, we can find $x \in S$ so that $\varphi(x) = y$ since φ is surjective. Now,

$$\varphi(e)y = \varphi(e)\varphi(x) = \varphi(ex) = \varphi(x) = y,$$

and similarly $y\varphi(e) = y$. So $\varphi(e)$ must be the identity in S'.

Remark (Invariance of Inverses under Isomorphisms)**.** Let S and S' be binary structures with identity elements e and e' and $\varphi : S \to S'$ be an isomorphism. If x' is an inverse of x in S then $\varphi(x')$ is an inverse of $\varphi(x)$:

$$\varphi(x')\varphi(x) = \varphi(x'x) = \varphi(e) = e'$$

and similarly $\varphi(x)\varphi(x') = e'$.

Remark. The inverse map of an isomorphism $\varphi : S \to S'$ is an isomorphism from S' to S. Note that clearly, φ^{-1} is bijective, so it is enough to show that φ^{-1} is a homomorphism:

$$\varphi^{-1}(y_1y_2) = \varphi^{-1}(\varphi(x_1)\varphi(x_2)) = \varphi^{-1}(\varphi(x_1x_2)) = x_1 \circ x_2 = \varphi^{-1}(y_1) \circ \varphi^{-1}(y_2).$$

1.2 Groups and Subgroups

Definition 10 (Group)**.** A group is a binary structure $(G, \cdot)$ where the following properties hold:

Associativity $\cdot$ is associative on G; i.e. $\forall x, y, z \in G; x(yz) = (xy)z$.

Existence of Identity G has an identity element under $\cdot$; i.e. $\exists e \in G; \forall x \in G; xe = ex = x$.

Existence of Inverse Each element in G has an inverse under $\cdot$; i.e. $\forall x \in G; \exists x^{-1} \in G; xx^{-1} = x^{-1}x = e$.

Definition 11 (Abelian Group)**.** G is called an abelian group if $(G, \cdot)$ is a group and $\cdot$ is commutative.

Remark (Cancellation Laws)**.** Note that in a group

$$xy = xz \implies x^{-1}(xy) = x^{-1}(xz) \implies (x^{-1}x)y = (x^{-1}x)z \implies y = z,$$

which is known as the left cancellation law. Similarly,

$$yx = zx \implies y = z,$$

which is known as the right cancellation law. Note that the cancellation laws rely on all properties of a group.

Remark (Uniqueness of Inverses)**.** The cancellation laws imply that inverses must be unique. Note that the uniqueness of the identity element is inherited from binary structures.

Remark (Sided Inverses)**.** The cancellation laws and uniqueness of inverses imply that if $xx^* = e$ then x^* must be the inverse of x. Similarly, if $x^*x = e$ then $x^* = x^{-1}$.

Remark (Inverse of Products)**.** Note that if $a, b \in G$ then

$$(ab)(b^{-1}a^{-1}) = aea^{-1} = e,$$

so by the above remarks $(ab)^{-1} = b^{-1}a^{-1}$.

Remark (Power Notation)**.** For any $g \in G$ we define $g^0 = e$, and let g^{-1} be the inverse of g. Also, we let $g^1 = g$ and $g^n = g^{n-1}g$ for $n > 1$. For $n < 0$ we define $g^n = \left(g^{-1}\right)^{-n}$. This way we have $g^n g^m = g^{n+m} = g^n g^m$, and $(g^n)^m = g^{nm}$ for any two integers n and m.

Definition 12 (Subgroup)**.** Let $(G, \cdot)$ be a group and let $S \subseteq G$. S is said to be subgroup of G, denoted by $S \leq G$, if $(S, \cdot)$ is a group.

Proposition 1 (Subgroup Criteria)**.** *A subset $S \subseteq G$ is a subgroup of $(G, \cdot)$ if and only if the following hold:*

1. *S is closed under $\cdot$.*
2. *$e \in S$ where e is the identity element of G.*
3. *S is closed under taking inverses, i.e. if $x \in S$ then $x^{-1} \in S$.*

Proof. First note that if the above properties hold $(S, \cdot)$ will be a group since the associativity of $\cdot$ is inherited from G, the first property ensures that $\cdot$ restricted to S is a binary relation on S, and the second and third properties make S into a group. Now consider any $S \leq G$. Since $(S, \cdot)$ is a group, $\cdot$ must be a binary operation on S, and hence S must be closed under $\cdot$. Since S must contain an identity element which by uniqueness of identity must be e. Similarly, every element in S must have an inverse in S which by uniqueness of inverses must be its inverse in G. □

Remark. Note that the set of the subgroup of the group G is partially ordered by the $\leq$ relation (a partial order is reflexive, anti-symmetric, and transitive). There is one maximal element which is G, and one minimal element $\{e\}$. This allows us to arrange the subgroups of any group in a Hasse diagram.

1.3 Group Homomorphisms and Isomorphisms

Remark. Group isomorphisms inherit the properties of isomorphisms on binary structures. In particular, the inverse map of an isomorphism is an isomorphism, isomorphisms map the identity element to the identity element, and the inverse of the image of an element is the image of its inverse. More interestingly, group homomorphism satisfies the last two properties.

Proposition 2 (Invariance of Identity under Group Homomorphisms)**.** *Assume G and G' are groups with respective identity elements e and e'. For any homomorphism $\varphi : G \to G'$, we must have $\varphi(e) = e'$. .*

Proof. We have

$$\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e) \implies \varphi(e)\varphi(e)^{-1} = \varphi(e)\varphi(e)\varphi(e)^{-1} \implies e' = \varphi(e).$$

Note that this proof uses every property of groups. □

Proposition 3 (Invariance of Inverses under Group Homomorphisms)**.** *Assume G and G' are groups with respective identity elements e and e'. For any homomorphism $\varphi : G \to G'$, and any $x \in G$ we must have $\varphi(x^{-1}) = \varphi(x)^{-1}$*

Proof. Clearly

$$\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e) = e',$$

By proposition 2. Noting the cancellation laws and the uniqueness of inverses we conclude $\varphi(x^{-1}) = \varphi(x)^{-1}$. □

Proposition 4 (Group Homomorphisms Preserve Subgroup Structure)**.** *Assume G and G' are groups and $\varphi : G \to G'$ is a homomorphism. We have the following:*

1. $H \leq G \implies \varphi(H) \leq G'$
2. $H \leq G' \implies \varphi^{-1}(H) \leq G$

Proof. We apply proposition 1 in the proof of both parts.

1. Take any two elements $y_1, y_2 \in \varphi(H)$ and note that for some $x_1, x_2 \in H$ we must have $y_1 = \varphi(x_1)$ and $y_2 = \varphi(x_2)$. We have

$$y_1 y_2 = \varphi(x_1)\varphi(x_2) = \varphi(x_1 x_2) \in \varphi(H),$$

so $\varphi(H)$ is closed under the group operation. Note that since $H \leq G$ we must have $e \in H$ and since φ is an isomorphism we must have $\varphi(e) = e'$ so $e' = \varphi(e) \in \varphi(H)$. Finally, for any $x \in H$, we must have $x^{-1} \in H$ so by proposition 3 $\varphi(x)^{-1} = \varphi(x^{-1}) \in \varphi(H)$. Hence, $\varphi(H)$ must be a subgroup of G' by proposition 1.

2. Take any two elements $x_1, x_2 \in \varphi^{-1}(H)$ and note that $\varphi(x_1), \varphi(x_2) \in H$. We have
$$\varphi(x_1 x_2) = \varphi(x_1)\varphi(x_2) \in H$$
since $H \leq G'$ so $\varphi^{-1}(H)$ is closed under the group operation. Note that since $H \leq G'$ we must have $e' \in H$ and since φ is an isomorphism we must have $\varphi(e) = e'$ so $e \in \varphi^{-1}(H)$. Also, for any $x \in \varphi^{-1}(H)$ we have $\varphi(x) \in H$ and since H is a subgroup and φ is a group homomorphism $\varphi(x)^{-1} = \varphi(x^{-1}) \in H$. Since $\varphi(x^{-1}) \in H$ we must have $x^{-1} \in \varphi^{-1}(H)$, so $\varphi^{-1}(H)$ is closed under taking inverses and by by proposition 1 must be a subgroup of G.

□

Definition 13 (Kernel and Image)**.** Using proposition 4 we can define two subgroups associated with each group homomorphism $\varphi : G \to G'$:

1. The **kernel** of φ, denoted by $\ker\varphi$ is the pre-image of the trivial subgroup $\{e'\} \leq G'$.

2. The **image** of φ, denoted by $\operatorname{Im}\varphi$ or $\varphi(G)$ is the image of G.

Proposition 5. *A group homomorphism $\varphi : G \to G'$ is injective if and only if it has a trivial kernel, i.e.* $\ker\varphi = \{e\}$.

Proof. Clearly, if φ is injective it must have a trivial kernel since it maps e to e'. Now supose the kernel is trivial and take any two $x_1, x_2 \in G$ so that $\varphi(x_1) = \varphi(x_2)$. We have
$$\varphi(x_1) = \varphi(x_2) \implies \varphi(x_1)\varphi(x_2)^{-1} = \varphi(x_2)\varphi(x_2)^{-1} \implies$$
since φ is a group homomorphism $\varphi(x_2)^{-1} = \varphi(x_2^{-1})$, and so
$$\varphi(x_1 x_2^{-1}) = e' \implies x_1 x_2^{-1} \in \ker\varphi,$$
but $\ker\varphi = \{e\}$ so $x_1 = x_2$. □

Definition 14 (Group Isomorphim)**.** As is the case with binary structures, a group isomorphism is a bijective group homomorphism. If $\varphi : G \to G'$ is an isomorphism we say G and G' are isomorphic and write $G \simeq G'$.

1.4 Cosets and Lagrange's Theorem

Remark. Given any group homomorphism $\varphi : G \to G'$, the structure of the per-image of any element in the image of φ has a peculiar form: given $y \in \varphi(G)$, and any $y_0 \in G$ such that $\varphi(y_0) = y$
$$\varphi^{-1}(y) = \{y_0 h | h \in \ker\varphi\} := y_0 \ker\varphi.$$

This motivates us to define the concept of a coset.

Definition 15 (Coset)**.** Let G be a group, $H \leq G$ and $a \in G$. The set

$$aH := \{ah|h \in H\}$$

is said to be a **left coset** of H, and the set

$$Ha := \{ha|h \in H\}$$

is said to be a **right coset** of H.

Remark. Our motivating remarks can be summarized as: the image of the cosets of the kernel of a group homomorphism are singletons.

Proposition 6. *Cosets of any subgroup $H \leq G$ partition G. Moreover, the equivalence relation "a and b belong to the same coset of H" is given by*

$$a \sim_L b \iff a^{-1}b \in H$$

if we are considering a left coset and

$$a \sim_R b \iff ab^{-1} \in H.$$

Proof. Take any $g \in G$ and note that $g = ge$ and $e \in H$ since H is a group so $g \in gH$. Hence, $\cup\{gH|g \in G\} \supseteq G$. Clearly, $\cup\{gH|g \in G\} \subseteq G$ as well so we must have $\cup\{gH|g \in G\} = G$. Same goes for right cosets. Now take two elements $g_1, g_2 \in G$ such that $g_1H \cap g_2H \neq \varnothing$. Suppose $x \in g_1H \cap g_2H$, so we can find $h_1, h_2 \in H$ so that $x = g_1h_1 = g_2h_2$. For any $h \in H$ we have

$$g_1h = eg_1h = xx^{-1}g_1h = g_2h_2h_1^{-1}g_1^{-1}g_1h = g_2h_2h_1^{-1}h \in g_2H$$

so $g_1H \subseteq g_2H$. Similarly, we can show $g_2H \subseteq g_1H$ and so $g_1H = g_2H$. Hence, no two different left cosets of H intersect, and therefore the left cosets of H partition G. Same goes for the right cosets.

Now suppose $g_1 \sim_L g_2$ so

$$g_1^{-1}g_2 \in H \implies g_1^{-1}g_2 = h \in H \implies g_2 = g_1h \implies g_2 \in g_1H.$$

Also, clearly $g_1 \in g_1H$ and so g_1 and g_2 belong to the same left coset. Conversely, if g_1 and g_2 belong to the same left coset gH of H we have $g_1 = gh_1$ and $g_2 = gh_2$ for $h_1, h_2 \in H$. Now

$$g_1^{-1}g_2 = h_1^{-1}g^{-1}gh_2 = h_1^{-1}h_2 \in H.$$

Hence, $g_1 \sim_L g_2$, and the second part of the theorem is proven for left cosets. The reasoning for right cosets is very similar. □

Proposition 7. *Every two (right or left) cosets of $H \leq G$ have the same cardinality. In particular, $|aH| = |eH| = |H|$.*

Proof. Given two cosets $aH, bH \subseteq G$ consider the map $\varphi : aH \to bH$ defined by $\varphi(x) = ba^{-1}x$. First, note that φ is injective:

$$\varphi(x_1) = \varphi(x_2) \implies ba^{-1}x_1 = ba^{-1}x_2 \implies x_1 = x_2$$

where the last implication is a result of the cancellation laws. Also, given any $bh \in H$ we know that $ah \in aH$ and

$$\varphi(ah) = ba^{-1}ah = bh$$

so φ is surjective. Hence φ is a bijection between aH and bH, so aH and bH must be of the same cardinality. The particular case follows immediately. □

The above two observation allow us to prove a useful result:

Definition 16 (Order of a Group)**.** Suppose $(G, \cdot)$ is a group. If G has n elements, G is said to be of order n, denoted by $|G| = n$. If G is infinite, the group is said to be of infinite order.

Theorem 1 (Lagrange's Theorem)**.** *If G is a group of finite order and $H \leq G$, then $|H|||G|$ (the order of H divides the order of G).*

Proof. Consider the set of all (left or right) cosets of H. By proposition **??** the cosets partition G, and by proposition 7 each coset has the same cardinality as H. Also, since G is finite H must be finite, and the number of cosets must be finite. Say we have k cosets, then

$$|G| = k|H| \implies |H|||G|.$$

□

Definition 17 (Index of a Subgroup)**.** Suppose G is a subgroup and $H \leq G$. The index of H in G denoted by $[G : H]$ is the number of cosets of H in G.

Remark. If G is finite, by our discussion of cosets and Lagrange's theorem $[G : H] = |G|/|H|$.

Proposition 8. *Suppose $K \leq H \leq G$ and both $[G : H]$ and $[H : K]$ are finite*

$$[G : K] = [G : H][H : K]$$

Proof. Let

$$A = \{gH : g \in G\} \qquad B = \{hK : h \in H\}.$$

By our assumption we know both A and B are finite. Consider gK for some $g \in G$. We know that since $K \leq H$, $gK \subseteq gH$. later □

1.5 Normal Subgroups and Quotient Groups

Definition 18 (Normal Subgroup)**.** Let G be a group. $H \leq G$ is a normal subgroup of G (denoted by $H \lhd G$) if

$$\forall g \in G; gH = Hg;$$

i.e. if H's left and right cosets are the same.

Remark. Note that subgroups of an abelian group and subgroups of index two are normal. Also, the kernel of any group homomorphism $\varphi : G \to G'$ is normal, because for any $k \in \ker \varphi$ we have $k^{-1} \in \ker \varphi$ and

$$\varphi(xk^{-1}) = \varphi(x) \implies e' = \varphi(xkx^{-1}) \implies xkx^{-1} = k' \in \ker \varphi \implies xk = k'x$$

so $x \ker \varphi \subseteq \ker \varphi x$. We can similarly see that $\ker \varphi x \subseteq x \ker \varphi$.

Proposition 9. *For a group G and a subgroup $H \leq G$, the following are equivalent*

1. $H \lhd G$.
2. $\forall g \in G; \forall h \in H; g^{-1}hg \in H$.
3. $\forall g \in G; g^{-1}Hg = H$.

Proof. ($1 \implies 2$) Given $g \in G$ and $h \in H$ we know that $g^{-1}h \in g^{-1}H$, but since $H \lhd G$, we have $g^{-1}H = Hg^{-1}$ so we can find $h' \in H$ such that

$$g^{-1}h = h'g^{-1} \implies g^{-1}hg = h' \implies g^{-1}hg \in H.$$

($2 \implies 3$) Our assumption immediately implies $g^{-1}Hg \subseteq H$. Now fix $g \in G$ and take any $h \in H$. By our assumption, since $g^{-1} \in G$ we must have $ghg^{-1} \in H$. Now consider

$$g^{-1}(ghg^{-1})g = ehe = h$$

so $h \in g^{-1}Hg$, and therefore $H \subseteq g^{-1}Hg$.

($3 \implies 1$) Immediately follows by taking $gh \in gH$ (or $hg \in Hg$)and noting that $gHg^{-1} \in H$.

□

Remark. Give $g \in G$ the automorphism $i_g : G \to G$ given by $i_g(x) = gxg^{-1}$ is known as a **conjugation** and gxg^{-1} is known as **the conjugation of** x **by** g. The above proposition can be stated as: A subgroup is normal if and only if it is fixed by every conjugation.

Remark. Any automorphism that is equal to a conjugation is called an **inner automorphism**.

$$\begin{tikzcd}
G \arrow[rr, "\varphi"] \arrow[dr, "\gamma"] & & \varphi(G) \\
& G/\ker\varphi \arrow[ur, "\mu"] &
\end{tikzcd}$$

Figure 1: The Fundamental Homomorphism Theorem

.

Remark. It is easy to see that any inner automorphism on an abelian group is the identity map

$$\psi(x) = gxg^{-1} = gg^{-1}x = x.$$

Proposition 10. *Suppose G is a group and $H \lhd G$. If $aH = a'H$ and $bH = b'H$, then $abH = a'b'H$.*

Proof. Take $abh \in abH$ since $bh \in bH = b'H$ we can find $h_1' \in H$ so that $bh = b'h_1'$ so $abh = ab'h_1'$. Since H is normal $b'H = Hb'$ and we can find $h_2' \in H$ so that $b'h_1' = h_2'b'$, and therefore $abh = ah_2'b'$. Using the same reasoning we can find $h_1'' \in H$ so that $ah_2' = h_1''a'$ so $abh = h_1''a'b'$, and then find $h_2'' \in H$ so that $h_1''a'b' = a'b'h_2''$. This allows us to conclude $abH \subseteq a'b'H$. Since cosets are equivalence classes we must have $abH = a'b'H$. □

Remark. The above proposition suggests that "coset multiplication" given by

$$(aH)(bH) = (ab)H$$

is well defined. Also, given any coset aH is is easy to see that $(aH)(eH) = aH$, and $(aH)(a^{-1}H) = (a^{-1}H)(aH) = eH$. Hence, we arrive at the following:

Definition 19 (Quotient Group)**.** Suppose G is a group and $H \lhd G$. The quotient group G/H (pronounced G modulo H) is the group on the cosets of H under coset multiplication.

1.6 The Fundamental Homomorphism Theorem

Theorem 2 (The Fundamental Homomorphism Theorem)**.** *The image of G under any homomorphism is isomorphic to a quotient of G, and any quotient of G is isomorphic to the image of G under a homomorphism.*

Proof. We first prove that any quotient of G is isomorphic to the image of G under a homomorphism. Take $N \lhd G$ and consider the "canonical homomorphism" $\gamma : G \to G/N$ defined by $\gamma(x) = xN$. Clearly, γ is surjective. Also

$$\gamma(xy) = (xy)N = (xN)(yN) = \gamma(x)\gamma(y).$$

So we can see that $G/N = \gamma(G)$.

Now we show that the image of G under any homomorphism is isomorphic to a quotient of G. Suppose $\varphi : G \to G'$ is a group homomorphism. We know that $\ker\varphi$ is a normal subgroup of G so we can consider the quotient $G/\ker\varphi$. Let $\gamma : G \to G/\ker\varphi$ be given by $\gamma(x) = x\ker\varphi$. Note that if $x\ker\varphi = y\ker\varphi$ then for $k_1, k_2 \in \ker\varphi$ we have

$$xk_1 = yk_2 \implies \varphi(xk_1) = \varphi(yk_2) \implies \varphi(x) = \varphi(y).$$

Hence, we can define the map $\mu : G/\ker\varphi \to \varphi(G)$ by $\mu(x\ker\varphi) = \varphi(x)$. First, note that for any $\varphi(x) \in \varphi(G)$, we can consider $x\ker\varphi \in G/\ker\varphi$ to see that $\mu(x\ker\varphi) = \varphi(x)$. Also, if $\mu(x\ker\varphi) = \mu(y\ker\varphi)$ we must have $\varphi(x) = \varphi(y)$ which implies $xy^{-1} \in \ker\varphi$ so $x \in y\ker\varphi$ and since cosets are equivalence classes $x\ker\varphi = y\ker\varphi$. Hence, μ is a bijection. Finally, note that

$$\mu((x\ker\varphi)(y\ker\varphi)) = \mu((xy\ker\varphi)) = \varphi(xy) = \varphi(x)\varphi(y) = \mu(x\ker\varphi)\mu(y\ker\varphi).$$

Hence, μ is an isomorphism, and therefore $\varphi(G)$ is isomorphic to $G/\ker\varphi$. Figure 1 summarizes this construction. □

1.7 Product Groups

Theorem 3 (Product Group). *If $(G_1, \circ_1)$ and $(G_2, \circ_2)$ are groups we can define the product group $(G_1 \times G_2, \circ)$ with the following operation:*

$$(x_1, x_2) \circ (y_1, y_2) = (x_1 \circ_1 y_1, x_2 \circ_2 y_2).$$

Proof. Associativity is a consequence of associativity of G_1 and G_2:

$$\begin{aligned}(x_1, x_2) \circ ((y_1, y_2) \circ (z_1, z_2)) &= (x_1, x_2) \circ (y_1 \circ_1 z_1, y_2 \circ_2 z_2)\\ &= (x_1 \circ_1 (y_1 \circ_1 z_1), x_2 \circ_2 (y_2 \circ_2 z_2))\\ &= ((x_1 \circ_1 y_1) \circ_1 z_1, (x_2 \circ_2 y_2) \circ_2 z_2)\\ &= ((x_1 \circ_1 y_1), (x_2 \circ_2 y_2)) \circ (z_1, z_2)\\ &= ((x_1, x_2) \circ (y_1, y_2)) \circ (z_1, z_2).\end{aligned}$$

The identity element is (e_1, e_2) where e_i is the identity in G_i:

$$\begin{aligned}(x_1, x_2) \circ (e_1, e_2) = (x_1 \circ_1 e_1, x_2 \circ_2 e_2) &= (x_1, x_2)\\ &= (e_1 \circ_1 x_1, e_2 \circ_2 x_2) = (e_1, e_2) \circ (x_1, x_2).\end{aligned}$$

The inverse of (x_1, x_2) is given by (x_1^{-1}, x_2^{-1}):

$$(x_1, x_2) \circ (x_1^{-1}, x_2^{-1}) = ((x_1 \circ_1 x_1^{-1}), (x_2 \circ_2 x_2^{-1})) = (e_1, e_2),$$

and

$$(x_1^{-1}, x_2^{-1}) \circ (x_1, x_2) = ((x_1^{-1} \circ_1 x_1), (x_2^{-1} \circ_2 x_2)) = (e_1, e_2).$$

□

Remark. Any group of order 2 is isomorphic to $\mathbb{Z}_2$, and any group of order 3 is isomorphic to $\mathbb{Z}_3$. This is not the case for groups of order 4, $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are not isomorphic.

2 Special Groups

2.1 Cyclic Groups and $\mathbb{Z}_n$

Proposition 11. *If $\{H_\alpha | \alpha \in I\}$ is a family of subgroups of G, then $H = \cap_{\alpha\in I} H_\alpha \leq G$.*

Proof. Take $x, y \in H$. For every $\alpha \in I$ we have $x, y \in H_\alpha$, and since each H_α is a subgroup we must have $xy \in H_\alpha$. Hence, $xy \in \cap_{\alpha\in I} H_\alpha = H$, and we conclude that H is closed under the group operation. Similarly, for any $x \in H$ we must have $x \in H_\alpha$ for all $\alpha \in I$, and since H_α is a group, $x^{-1} \in H_\alpha$. This allows us to conclude that H is closed under taking inverses. Finally, since each H_α is a subgroup, we must have

$$\forall \alpha \in I; e \in H_\alpha \implies e \in \cap_{\alpha\in I} H_\alpha.$$

Therefore, $H \leq G$. □

Definition 20 (Generator and Generated Subgroup)**.** Let G be a group and let $S \subseteq G$. The subgroup generated by S in G is defined as

$$\langle S \rangle = \bigcap \{H \leq G | H \supseteq S\}.$$

Each element of S is said to be a generator of $\langle S \rangle$. It is customary to write $\langle a_1, \ldots, a_n \rangle$ instead of $\langle \{a_1, \ldots, a_n\} \rangle$ when $S = \{a_1, \ldots, a_n\}$.

Proposition 12 (Identification of Finitely Generated Groups)**.** *Let G be a group and $S = \{a_1, \ldots, a_n\}$ be a subset of G. We have*

$$\langle S \rangle = \{x_1 x_2 \ldots x_k | k \in \mathbb{Z}^+, x_i \in \{a_1, \ldots, a_n, a_1^{-1}, \ldots, a_n^{-1}\}\} \tag{1}$$

Proof. Let H be the set on the RHS of (1). Take any $x, y \in H$ where $x = x_1 \ldots x_n$ and $y = y_1 \ldots y_m$. Note that clearly $xy = x_1 \ldots x_n y_1 \ldots y_m \in H$, and $x^{-1} = x_n^{-1} \ldots x_1^{-1} \in H$. Also, $e = a_1 a_1^{-1} \in H$ so $H \leq G$. Clearly $S \subseteq H$ so by definition of $\langle S \rangle$ we must have $\langle S \rangle \subseteq H$. Also, since we must have $S \subseteq \langle S \rangle$ and $\langle S \rangle$ must be closed under multiplication, we must have $H \subseteq \langle S \rangle$, and therefore $H = \langle S \rangle$. □

Definition 21 (Cyclic Group)**.** A group G is said to be cyclic if it has a single generator; i.e.

$$\exists g \in G; \langle g \rangle = G.$$

Proposition 13.

$$\langle g \rangle = \{g^n | n \in \mathbb{Z}\}.$$

Proof. Let $G = \{g^n | n \in \mathbb{Z}\}$. Clearly, $G \subseteq \langle g \rangle$. Note that $g^n g^m = g^{n+m} \in G$, $e = g^0 \in G$ and for each $g^n \in G$ we have $(g^n)^{-1} = g^{-n} \in G$. Hence, G is a group that contains g and we must have $\langle g \rangle \subseteq G$.[1] □

2.1.1 Classification of Cyclic Groups

Remark. Integers under addition form an abelian group.

Proposition 14. *Given each integer $n \in \mathbb{Z}$,*

$$n\mathbb{Z} = \{nk | k \in \mathbb{Z}\}$$

is a subgroup of $(\mathbb{Z}, +)$.

Proof. $nk_1 + nk_2 = n(k_1 + k_2)$, $-nk = (-n)k$, and $0 = n0$. □

Definition 22. Since $\mathbb{Z}$ is abelian, and every subgroup of an abelian group is normal, the cosets of the subgroup $n\mathbb{Z}$ are well-defined for every $n \in \mathbb{Z}$. The abelian group $\mathbb{Z}/n\mathbb{Z}$ for every positive n is known as the group of integers modulo n and is denoted by $\mathbb{Z}_n$. It is customary to denote $k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ by k alone, when the context is clear.

Theorem 4 (Division Theorem)**.** *Given $n \in \mathbb{Z}$ and $p \in \mathbb{Z}^+$ there exist unique $q, p \in \mathbb{Z}$ such that $n = pq + r$, and $0 \leq r < p$.*

Proof. Consider the set $A = \{m \in \mathbb{Z} | mp > n\}$. This set is non-empty, since if $n \leq 0$ we have $1 \in A$, and if $n > 0$ we have $n + 1 \in A$. Similarly, we can show that this set is bounded below. Hence, by the well-ordering principle it has a smallest element $q' \in \mathbb{Z}$. Note that q' being the smallest element of A implies $q' - 1 \notin A$, and so $(q' - 1)p \leq n$. To summarize, we have $(q' - 1)p \leq n < q'p$. Letting $q = q' - 1$ we see that

$$0 \leq \underbrace{n - qp}_{r} < p.$$

So that the claim is satisfied. Now assume q_2, r_2 also satisfy the claim. We must have

$$pq + r = pq_2 + r_2 \implies p(q - q_2) = r_2 - r \implies p | r_2 - r.$$

Since both r and r_2 are non-negative and less than p, their difference will satisfy $-p < r_2 - r < p$ so the only way $p | r_2 - r$ holds is that $r_2 - r = 0$. This implies that $q - q_2 = 0$. □

Definition 23 (Order of an Element)**.** Let G be a group. The order of $a \in G$ denoted by $o(a)$ is taken to be the smallest non-negative integer p such that $a^p = e$. If no such p exists a is said to be of infinite order.

[1] This derivation only makes sense if g is taken to be the element of a parent group. If we only have a single element g and the notion of a group operation, we can take this to be the definition of the group generated by g.

Proposition 15. *Let G be a group and $a \in G$. If a^p then $o(a)|p$.*

Proof. First note that since e is its own inverse, by uniqueness of inverses we must have $a^{-p} = e$, hence the set $\{p \in \mathbb{Z}^+ | a^p = e\}$ will be non-empty. Therefore, by the well ordering theorem a is of finite order. Apply the division theorem to p and $o(a)$ to get $p = qo(a) + r$ where $0 \leq r < o(a)$. Note that

$$e = a^p = a^{qo(a)+r} = (a^{o(a)})^q a^r = a^r$$

since $o(a)$ is the smallest positive integral power that annihilates a we must have $r = 0$. Hence $p = qo(a)$, namely $o(a)|p$. □

Proposition 16. *Let $G = \langle g \rangle$ be of finite order. Then $o(g) = |G|$.*

Proof. First note that G must have at least $o(g)$ elements $g, g^2, \ldots, g^{o(a)}$, since if $g^i = g^j$ for $1 \leq i < j \leq o(a)$ we must have $g^{j-i} = e$ so the order of g must be less than $j - i$, contradiction. Also, for any $p > o(a)$ we can apply the division theorem to get $p = qo(a) + r$ for $0 \leq r < o(a)$, and we can see that $g^p = g^r$. Hence, we must have $G = \{g, g^2, \ldots, g^{o(a)}\}$ and therefore $|G| = o(g)$. □

Theorem 5 (Classification of Cyclic Groups)**.** *Every cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Every cyclic group of infinite order is isomorphic to $\mathbb{Z}$.*

Proof. Let $G = \langle g \rangle$. We consider two cases:

1. If $G = \langle g \rangle$ is of order n, we can apply proposition 16 to see that $o(g) = n$ and therefore if $k + n\mathbb{Z} = k' + n\mathbb{Z}$ we must have

   $$g^k = g^{k'+pn} = g^{k'}(g^n)^p = g^{k'}.$$

   Hence, we can define $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$ by $\varphi(k + n\mathbb{Z}) = g^k$. By proposition 13, φ is surjective. Now assume

   $$\varphi(k + n\mathbb{Z}) = \varphi(k' + n\mathbb{Z}) \implies g^k = g^{k'} \implies g^{k-k'} = e.$$

   By proposition 15 we must have $o(g)|k-k'$ and by proposition 16, $o(g) = n$. Hence, $n|k - k'$; i.e. $k = np + k'$ or equivalently $k \in k' + n\mathbb{Z}$. Hence, we must have $k + n\mathbb{Z} = k' + n\mathbb{Z}$, and, therefore, φ is injective. Finally, note that

   $$\begin{aligned}\varphi\left((k + n\mathbb{Z}) + (k' + n\mathbb{Z})\right) = \varphi((k + k') + n\mathbb{Z}) &= g^{k+k'} \\ &= g^k g^{k'} \\ &= \varphi(k + n\mathbb{Z}) + \varphi(k' + n\mathbb{Z}).\end{aligned}$$

   Hence, $G \simeq \mathbb{Z}/n\mathbb{Z}$.

2. If G is of infinite order we define $\varphi : \mathbb{Z} \to G$ by $\varphi(k) = g^k$. By proposition 13, φ is surjective. Also,

   $$\varphi(k) = \varphi(k') \implies g^{k-k'} = 0$$

if $k - k' \neq 0$ the order of g and hence the order of G will be finite. Hence, we must have $k - k' = 0$. Finally, note that

$$\varphi(k + k') = g^{k+k'} = g^k g^{k'} = \varphi(k)\varphi(k').$$

Therefore, $G \simeq \mathbb{Z}$.

□

Corollary. Cyclic groups are countable.

Corollary. Cyclic groups are abelian.

Proposition 17. *Subgroups of cyclic groups are cyclic.*

Proof. Let $G = \langle g \rangle$ and $H \leq G$. $e \in H$ so $|H| \geq 1$. If $|H| = 1$ we must have $H = \{e\} = \langle e \rangle$. Otherwise, the set $\{k \in \mathbb{Z}^+ | g^k \in H\}$ non-empty, and by the well-ordering principle it must have a minimum element, p. We claim that $H = \langle g^p \rangle$. Note that by closure of H we must have $H \supseteq \langle g^p \rangle$. Now for any $g^n \in H$ we can apply the division theorem to n and p to get $q = np + r$, and therefore $g^r = e$. Since p is the smallest positive integral power that annihilates g and $0 \leq r < p$ we must have $r = 0$. So $\langle g^p \rangle \subseteq H$. □

Proposition 18. *Quotients of a cyclic group are cyclic.*

Proof. Let $G = \langle g \rangle$ and $H \leq G$. Since G is abelian H is normal. Consider $gH \in G/H$. Note that $g^r H = (gH)^r$ so $G/H \subseteq \langle gH \rangle$. Also, $\langle gH \rangle \subseteq G/H$. Hence, $G/H = \langle gH \rangle$. □

Definition 24 (Center)**.** The center of a group G is given by

$$Z(G) = \{z \in G | \forall x \in G; zx = xz\}.$$

Proposition 19. *The center of a group is a normal subgroup.*

Proof. Note that if $z_1, z_2 \in G$ we have

$$xz_1z_2 = z_1xz_2 = z_1z_2x,$$

$e \in Z(G)$, and

$$xz = zx \implies z^{-1}z = xz^{-1}.$$

Also, clearly the left and right cosets are equal, since the elements in $Z(G)$ commute with every element of G. □

Proposition 20. *If $G/Z(G)$ cyclic then g abelian.*

Proof. Let $G/Z(G) = \langle gZ(G) \rangle$ for some $g \in G$. Take $x, y \in G$, we have

$$(xZ(G)) = g^p Z(G) \implies x = g^p z_1$$

where $p \in \mathbb{Z}^+$ and $z_1 \in Z(G)$, and similarly

$$(yZ(G)) = g^q Z(G) \implies x = g^q z_2.$$

Now

$$\begin{aligned} xy = g^p z_1 g^q z_2 = g^p g^q z_1 z_2 = g^q g^p z_1 z_2 = g^q z_1 g^p z_2 \\ = g^q z_1 z_2 g^p = g^q z_2 z_1 g^p = g^q z_2 g^p z_1 = yx. \end{aligned}$$

□

2.1.2 Some Results in Elementary Number Theory

Remark. The fact that groups of integers and cyclic groups are isomorphic allows us to use group theory to derive some of the standard results in elementary number theory.

Theorem 6 (Bezout's Identity)**.** *Given two positive integers a and b their greatest common divisor can be expressed as a linear combination; that is $x, y \in \mathbb{Z}$ exist so that* $\gcd(a, b) = ax + by$.

Proof. Consider $\langle a, b\rangle$ in $\mathbb{Z}$. Note that clearly $\{ar + bs | r, s \in \mathbb{Z}\} \subseteq \langle a, b\rangle$. Also, $\{ar+bs|r, s \in \mathbb{Z}\}$ is a group containing a and b, hence $\langle a, b\rangle \subseteq \{ar+bs|r, s \in \mathbb{Z}\}$.

Since $\mathbb{Z}$ is cyclic, and every subgroup of a cyclic group is cyclic, $\langle a, b\rangle$ must be cyclic. In particular, the smallest positive integer $d \in Z^+$ must exist so that $\langle a, b\rangle = \langle d\rangle$, and by our above remarks $d = ax + by$

Clearly, d is a common divisor of a and b. If d' is another common divisor it must be a generator of $\langle a, b\rangle$. Since d is the smallest positive such generator we must have $d' \leq d$. Hence, $\gcd(a, b) = d = ax + by$. □

Corollary (Euclid's Lemma)**.** If $\gcd(a, b) = 1$ and $a|bc$ then $a|c$.

Proof. By Bezout's identity $x, y \in \mathbb{Z}$ exist such that $ax + by = 1$. Now $a|bc$ so for some $p \in \mathbb{Z}$ we have $ap = bc$. So

$$ax+by = 1 \implies acx+bcy = c \implies acx+apy = c \implies a(cx+py) = c \implies a|c.$$

□

Proposition 21. *Every group G of prime order is cyclic, and every element of G other than the identity is a generator.*

Proof. Let $H \leq G$. By Lagrange's theorem $|H|||G|$, and since G is of prime order we must have $|H| = 1$ or $|H| = |G|$. So for any $g \neq e$ we must have $|\langle g\rangle| = |G|$, i.e. g must generate G. □

Theorem 7 (Fermat's Little Theorem)**.** *If p is prime then for any $a \in \mathbb{Z}/p\mathbb{Z}$ we must have $a^p = a$.*

Proof. First note that $0 \in \mathbb{Z}/p\mathbb{Z}$ raised to any power is 0. Now consider 21 for any $a \neq 0$, $a + p\mathbb{Z}$ must be a generator of $\mathbb{Z}/p\mathbb{Z}$. We know that the order of a generator is the order of the group, so $(a + p\mathbb{Z})^p = p\mathbb{Z}$ □

2.2 Permutation Groups

Definition 25 (Permutation)**.**

Theorem 8 (Cayley's Theorem)**.**

2.3 Dihedral Groups

Loosely speaking, The n-th dihedral group encodes the symmetries of a regular n-gon ($n \geq 3$) through reflections and rotations. Consider the set of points in a plane comprising a regular n-gon. If we rotate this set of points by an integer multiple of $2\pi/n$ around its center of gravity the transformed set will be indistinguishable form the original one. Same is true if we reflect the set about any of its diagonals. Finish these introductory remarks.

Consider the following maps:

Rotation by $2\pi/n$ $r : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $r(x) = x + 1$

Reflection about Vertex 0 $s : \mathbb{Z}_n \to \mathbb{Z}_n$ given by $s(x) = -x$

Since both r and s are permutations on $\mathbb{Z}_n$, we can consider the subgroup of S_n they generate, and denote it by D_n. This subgroup is called the n-th dihedral group. The following properties hold:

1. $r^n = e$ because $r^n(x) = x + n = x \pmod{n}$.
2. $s^2 = e$ because $s^2(x) = -(-x) = x \pmod{n}$.
3. $sr = r^{-1}s$ because $s(r(x)) = -(x+1) = s(x) - 1 = r^{-1}(s(x)) \pmod{n}$

Note that the last property implies that $rs = sr^{-1}$. Now, by definition of D_n, we must have $r^i \in D_n$ for $0 \leq i < n$. Also note that

$$r^i = r^j \implies r^i(0) = r^j(0) \implies i = j \pmod{n}$$

so the r^is are unique for the specified is. We must also have $sr^i \in D_n$ for $1 \leq i \leq n$ and since $sr^i = sr^j$ implies $r^i = r^j$ by the uniqueness of r^is we must have that sr^is are unique for the specified is. Finally note that

$$sr^i = r^j \implies sr^i(0) = r^j(0) \implies -i = j \pmod{n}$$

while at the same time

$$sr^i = r^j \implies sr^i(1) = r^j(1) \implies -i - 1 = 1 + j \pmod{n}$$

so we must have $-1 = 1 \pmod{n}$ or equivalently $2 = 0 \pmod{n}$, which contradicts our assumption that $n \geq 3$. Hence, $r^0, \ldots, r^{n-1}, s, \ldots, sr^{n-1}$ are $2n$ unique elements of D_n; i.e. $\{r^0, \ldots, r^{n-1}, s, \ldots, sr^{n-1}\} \subseteq D_n$.

We will now show that the inclusion also holds in the other direction. To show this we rely on the following two lemmas:

Lemma 1. *For all $k \in \mathbb{Z}^+$, $sr^k = r^{-k}s$.*

Proof. We prove the lemma by induction. The base case of $k = 1$ is proved above, so assume that the lemma holds for some $k \geq 1$. We have $sr^{k+1} = srr^k = r^{-1}sr^k$ and by the induction hypothesis $sr^k = r^{-k}s$ so we can conclude $sr^{k+1} = r^{-1}r^{-k}s = r^{-k-1}s$. □

Corollary. The above lemma also holds for all $k \in \mathbb{Z}$ since if $k < 0$ we have

$$sr^{-k} = r^k s \implies r^{-k} = sr^k s \implies r^{-k}s = sr^k$$

and if $k = 0$ we have the trivial statement $s = s$.

Lemma 2. *Every element of D_n is of the form $r^i s^j$ for some $i, j \in \mathbb{Z}$.*

Proof. Note that by definition of D_n and proposition 12 we have

$$D_n = \{x_1 x_2 \ldots x_k | k \in \mathbb{Z}^+, x_i \in \{r, s, r^{-1}\}\}.$$

We prove the lemma by induction on k, the number of x_is in the above representation of D_n.

base case ($k = 1$) There are only three such elements in D_n: r, s, and r^{-1} all of which have the claimed form.

inductive step Take any $x_1 \ldots x_{k+1} \in D_n$. We must have $x_2 \ldots x_{k+1} \in D_n$ and by the induction hypothesis we must have $x_2 \ldots x_{k+1} = r^i s^j$. Now, if x_1 is r or r^{-1} we are done. Otherwise we have $x_1 \ldots x_{k+1} = sr^i s^j$ which by the corollary to the first lemma can be written as $r^{-i}s^{j+1}$.

□

Now, take any element x of D_n. By the second lemma we must have $x = r^i s^j$. Noting that $s^2 = e$, we consider two cases. Either j is even, in which case $s^j = e$ and $x = r^i$, or j is odd, in which case $s^j = s$ and so $x = r^i s$ which by the corollary to the first lemma can be written as sr^{-i}. In either case we can use the fact that $r^n = e$ and use division theorem to express x as r^l or sr^l for some $0 \leq l < n$. Hence, x must be one of $r^0, \ldots, r^{n-1}, s, \ldots, sr^{n-1}$; i.e. $\{r^0, \ldots, r^{n-1}, s, \ldots, sr^{n-1}\} \supseteq D_n$. We can now conclude that

$$D_n = \{r^0, \ldots, r^{n-1}, s, \ldots, sr^{n-1}\}.$$

3 Rings and Fields

3.1 Definitions and Examples

We start with the usual definitions: the ring structure itself, structure preserving mapping between rings (ring homomorphisms), and substructures (subrings).

Definition 26 (Ring)**.** A ring $(R, +, \cdot)$ is a set R equipped with two binary operations $\cdot : R \times R \to R$ and $+ : R \times R \to R$. Such that

1. $(R, +)$ is an abelian group.
2. $\cdot$ is associative.
3. $\cdot$ distributes over $+$ from both left and right; i.e. for all $x, y, z \in R$

$$x(y+z) = xy + xz \qquad (y+z)x = yx + zx.$$

Remark. A ring is said to be commutative if $\cdot$ is commutative.

Definition 27 (Ring With Unity)**.** A ring R is said to have a unity element if for some element $1 \in R$ and any $x \in R$

$$1 \cdot x = x \cdot 1 = x.$$

Remark. There is no consensus in the mathematical community on whether a ring should contain a unity. Some take the existence of unity as a defining ring axiom and call a ring without unity a pseudo-ring or 'rng', while others allow rings to lack a multiplicative identity element and then call a ring that have unity a 'ring with unity' or 'ring with identity'.

Definition 28 (Ring Homomorphsim and Isomorphism)**.** Let R and R' be rings. A ring homomorphism is a mapping $\phi : R \to R'$ that satisfies the following for any $x, y \in R$

$$\phi(x+y) = \phi(x) + \phi(y) \qquad \phi(xy) = \phi(x)\phi(y).$$

If the homomorphism ϕ is bijective it is said to be an isomorphism and R and R' are said to be isomorphic, and we write $R \simeq R'$.

Definition 29 (Subrings)**.** A non-empty subset S of a ring $(R, +, \cdot)$ is said to be a subring of R if $(S, +, \cdot)$ is itself a ring.

Remark. As was the case with groups, multiplication and addition inherits their properties in S. So in order for S to be ring it is enough that it is closed under the ring operations and additive inverses.

Remark (Some examples)**.**

1. Integers modulo n for any $n \geq 2$ form a commutative ring with unity.
2. If R is a ring, then the set of all matrices on R under matrix multiplication and addition is a ring.
3. If S is a set and R is a ring the set of all functions from S to R with the usual function addition and multiplication is a ring.

4. The familiar sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}/p\mathbb{Z}$ when p is prime are all commutative rings with unity. They also have the extra property of existence of multiplicative inverses which makes them into such sets to be ideals.

5. Polynomials with coefficients in a ring (defined later) form a ring.

Before giving more definitions, we prove the following basic identities concerning additive inverses and identity that hold in all rings.

Proposition 22. *Let R be a ring with additive identity 0. The following hold*

1. *For any $x \in R$ we have $x0 = 0x = 0$.*

2. *For any $x, y \in R$ we have $x(-y) = (-x)y = -(xy)$ and $(-x)(-y) = xy$.*

Proof. 1. By left distributivity $x0 = x(0+0) = x0 + x0$ and by cancellation in the additive group $(R, +)$ we have $0 = x0$. Similarly $0x = 0$.

2. Since R is an abelian group under addition, additive inverses are unique. Now
$$xy + x(-y) = x(y + (-y)) = x0 = 0,$$
and
$$xy + (-x)y = (x + (-x))y = 0y = 0,$$
so $x(-y) = (-x)y = -(xy)$. Using this we can write
$$-(xy) + (-x)(-y) = (-x)y + (-x)(-y) = (-x)(y + (-y)) = (-x)0 = 0.$$

3. For any $x, y \in R$ we have $x(-y) = (-x)y = -(xy)$ and $(-x)(-y) = xy$.

□

Definition 30 (Zero Divisors)**.** A non-zero element x of a ring R is said to be a left (right) zero-divisor in R if non-zero $y \in R$ exists such that $xy = 0$ ($yx = 0$).

Definition 31 (Domain)**.** A ring that has no zero divisors is said to be a domain.

Definition 32 (Integral Domain)**.** A commutative domain with identity is said to be an integral domain.

Remark. Integers are canonical example and the namesake of integral domains.

Proposition 23. *A ring R has no left (right) zero divisors if and only if multiplicative cancellation on the left (right) holds; i.e. for any non-zero x, and $y, z \in R$, the equation $xy = xz$ ($yx = zx$) implies $y = z$.*

Proof. First suppose R has no right zero divisors and for some non-zero $x, y, z \in R$ we have $xy = xz$. Using what we know about additive inverses in R we have
$$xy = xz \implies xy - (xz) = xy + x(-z) = 0 \implies x(y + (-z)) = 0.$$

Since x is non-zero and R has no zero divisors we can conclude that $y+(-z)=0$ or equivalently $x=z$.

Now suppose left cancellation holds and for some non-zero x and $z \in R$ we have $xz = 0$. We know that $0 = x0$ and so we must have $xz = x0$. By left cancellation we conclude $z = 0$ so R does not have any zero divisors.

The case of right divisors and cancellation is similar. □

Remark. By the above proposition, integral domains are commutative rings with identity over which cancellation holds.

Definition 33 (Units)**.** An element x of a ring R with unity is said to be a unit if it has a multiplicative inverse.

Remark. By proposition 22 the additive identity 0 can never be a unit.

Definition 34 (Division Ring)**.** A ring with unity in which every non-zero element is a unit is called a division ring or a skew-field.

Remark. Quaternions are the canonical example of a skew field.

Definition 35 (Field)**.** A commutative division ring is a field; i.e. a commutative ring with identity $(F,+,\cdot)$ is said to be a field if every non-zero element has a multiplicative inverse.

Remark. The familiar $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}/p\mathbb{Z}$ are all fields.

Remark. Observe that if $0 \not 1$ on a field, then $F \setminus \{0\}$ is an abelian group under multiplication. This in turn implies that the multiplicative identity and inverses are unique.

Definition 36 (Characteristic of a Ring)**.** Given a ring R, if we can find a positive integer n so that if any $x \in R$ added n times with itself gives 0 -i.e. $n \cdot x = 0$-, then we call the smallest such n the characteristic of R. If no such n exists, R is said to be of characteristic zero.

Proposition 24. *If R has a multiplicative identity 1, then -if extant- the smallest positive integer n for which $n \cdot 1 = 0$ is the characteristic of R, and $n \cdot 1 \neq 0$ for all $n \in \mathbb{Z}^+$ if and only if R is of characteristic zero. That is, for unital rings the definition of the characteristic can be done in terms of 1.*

Proof. By definition if R is of characteristic $n > 0$ we must have $n \cdot 1 = 0$. Also, if $m \cdot 1 = 0$ for some $m < n$ we can multiply by x on both sides to see that m must be the characteristic of R, and so n must be the smallest positive integer that has this property. This also shows that the smallest n such that $n \cdot 1 = 0$ must be the characteristic of R. Also, if for all $n > 0$ we have $n \cdot 1 \neq 0$ then clearly the characteristic of R must be zero. □

I end this section with a little nugget:

Proposition 25 (Freshman's Dream)**.** *If a commutative ring with identity R has prime characteristic p, then for any $x, y \in R$ we have*

$$(x+y)^p = x^p + y^p.$$

Proof. First note that because of commutativity, the binomial theorem holds. Sencod, note the identity

$$\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$$

which is easily verified by expressing binomial coefficients in terms of factorials. Now, note that for $1 \leq k < p$, we have $\gcd(k, p) = 1$, since p is prime, and since $\binom{p}{k}$ must be an integer we must have $k | p\binom{p-1}{k-1}$. By Euclid's lemma we conclude that $k | \binom{p-1}{k-1}$ So $\binom{p}{k}$ is a multiple of p for $1 \leq k < p$. Using this we have

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = \binom{p}{0} x^0 y^{p-0} + \binom{p}{p} x^p y^{p-p} = x^p + y^p.$$

□

3.2 Ring Homomorphisms, Ideals, and Quotient Rings

Proposition 26. *Ring homomorphisms preserve identities, inverses, and subring structures; i.e. if $\phi : R \to R'$ is a ring homomorphism then,*

1. *If 0 is the additive identity of R and $0'$ is the additive identity of R' then $\phi(0) = 0'$.*

2. *For all $x \in R$ we have $\phi(-x) = -\phi(x)$.*

3. *If S and S' are subrings of R and R' respectively, then $\phi(S)$ and $\phi^{-1}(S')$ will be subrings of R' and R respectively.*

Proof.

1. $$\phi(0) = \phi(0+0) = \phi(0) + \phi(0) \implies \phi(0) = 0'.$$

2. We have
$$\phi(-x) + \phi(x) = \phi((-x) + x) = \phi(0) = 0'$$
by part 1. So by the uniqueness of additive inverses in the abelian group $(R', +)$ we conclude $\phi(-x) = -\phi(x)$.

3. It is enough to show that $\phi(S)$ and $\phi^{-1}(S')$ are closed under ring operations and additive inverses. Note that ϕ is also an abelian group homomorphism and S and S' are additive subgroups of R and R', respectively. So $\phi(S)$ and $\phi^{-1}(S)$ will be abelian subgroups, and therefore closed under addition and taking additive inverses. Now, $\phi(x)\phi(y) = \phi(xy)$ and since S is closed under multiplication we conclude $\phi(S)$ is closed under multiplication, and for $a, b \in \phi^{-1}(S')$ we have $\phi(ab) = \phi(a)\phi(b)$ and since

S' is closed under multiplication, $\phi^{-1}(S')$ is closed under multiplication. Therefore $\phi^{-1}(S')$ and $\phi(S)$ are rings.

□

The definition of the kernel is similar:

Definition 37. Let $\phi : R \to R'$ be a ring homomorphism. The pre-image of the trivial subring $\{0'\} \subseteq R'$ is said to be the kernel of ϕ.

Remark. By the structure preserving property of homomorphisms, the kernel is always a subring.

Again, the kernel has the property that if two elements have the same image under a homomorphism, then their difference is an element of the kernel. More formally,

Proposition 27. *If $\phi : R \to R'$ is a ring homomorphism, then*

$$\phi^{-1}(\phi(a)) = a + \ker \phi = \ker \phi + a.$$

Proof. Since addition is commutative clearly $a + \ker \phi = \ker \phi + a$. Also, clearly $h \in \ker \phi$ implies $\phi(a+h) = \phi(h+a) = \phi(a)$. Now, suppose $\phi(b) = \phi(a)$. Then, by the fact that homomorphisms preserve additive inverses we get $\phi(b-a) = 0$ so $b - a \in \ker \phi$ or equivalently $b \in a + \ker \phi$. □

Corollary. A ring homomorphism is injective if and only if its kernel is trivial.

Remark. Similar to how we could define quotient groups from the cosets of the kernels of group homomorphisms, we can define quotient rings from the cosets of the kernels of ring homomorphisms. In group theory, the notion of a normal subgroup allowed us to generalize the construction of quotient groups from cosets of the kernel, to the cosets of any normal subgroup. The analogous to the notion of a normal subgroup in group theory, we can define an ideal of a ring. The definition of the ideal is motivated by the following observation.

Proposition 28. *Suppose R is a ring and H is a additive subgroup of R. Multiplication of cosets as*

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

is well-defined if and only if for any $x \in R$ we have $xH \subseteq H$ and $Hx \subseteq H$; i.e. H is closed under multiplication by any element of R.

Proof. First suppose that the coset product is well-defined. This means that, in particular for any $x \in R$ we must have $(x+H)(0+H) = x0+H$, or equivalently $(x + H)H = H$. This implies that for any $h \in H$ since 0 is a member of any additive subgroup we must have $(x + 0)h = xh \in H$, and therefore $xH \subseteq H$. Similarly we can show that $Hx \subseteq H$.

Now suppose for any $x \in R$ both $xH \subset H$ and $Hx \subset H$ hold. Take any $h_1, h_2 \in H$ and note that

$$(a + h_1)(b + h_2) = ab + ah_2 + h_1 b + h_1 h_2.$$

By our assumption, $ah_2, h_1 b, h_1 h_2 \in H$, and since H is an additive group their sum must be in H. We conclude that $(a + h_1)(b + h_2) \in ab + H$ and therefore the coset product is independent of the chosen representatives. □

Definition 38 (ideal)**.** Let R be a ring and I be an abelian subgroup of R such that for any $x \in R$ we have $xI \subseteq I$ and $Ix \subseteq I$. We call I an ideal of the ring R.

Definition 39. Let I be an ideal in the ring R. The quotient (factor) ring R/I is the set of all additive cosets of I equipped with addition and multiplication defined by

$$(a + I)(b + I) = ab + I \qquad (a + I) + (b + I) = (a + b) + I.$$

Remark. Note that R under addition is an abelian group and so any additive subgroup of R is a normal subgroup with respect to which coset addition is well-defined. Also, by the motivation of the definition of an ideal, coset multiplication is well-defined for ideals so the operations on R/I are well-defined. The rest of the properties of ring operations on R/I follow from the corresponding properties in R.

Theorem 9 (The Fundamental Homomorphism Theorem for Rings)**.** *Suppose $\phi : R \to R'$ is a ring homomorphism. Then $\ker \phi$ is an ideal and $R/\ker \phi \simeq \phi(R)$ under the isomorphism $\mu : R/\ker \phi \to \phi(R)$ given by $\mu(x + \ker \phi) = \phi(x)$.*

Conversely, if I is an ideal of R then I is the kernel of the homomorphism $\gamma : R \to R/I$ given by $\gamma(x) = x + I$, and trivially $\gamma(R) = R/I \simeq R/I$.

Proof. First, suppose $\phi : R \to R'$ is a ring homomorphism, and note that for any $h \in \ker \phi$ and $x \in R$ we have

$$\phi(hx) = \phi(h)\phi(x) = 0\phi(x) = 0 \qquad \phi(xh) = \phi(h)\phi(x) = \phi(x)0 = 0.$$

Also, since ϕ is an additive group homomorphism, we know that its kernel will be an additive subgroup of R, and so $\ker \phi$ is an ideal. Since $\ker \phi$ is an ideal, the ring $R/\ker \phi$ is well-defined. Now consider the mapping μ, as defined in the theorem statement. First, note that the mapping is well-defined, since if $x + \ker \phi = x' + \ker \phi$ there must exist $h \in \ker \phi$ so that $x' = x + h$ and since ϕ is a homomorphism we can write

$$\mu(x + \ker \phi) = \phi(x) = \phi(x) + 0 = \phi(x) + \phi(h) = \phi(x') = \mu(x' + \ker \phi).$$

Hence, μ is a well-defined mapping. Similarly, using the homomorphism properties of ϕ we can write

$$\begin{aligned} \mu((x+\ker\phi)+(y+\ker\phi)) &= \mu((x+y)+\ker\phi) \\ &= \phi(x+y) \\ &= \phi(x)+\phi(y) \\ &= \mu(x+\ker\phi)+\mu(y+\ker\phi) \end{aligned}$$

and

$$\begin{aligned} \mu((x+\ker\phi)(y+\ker\phi)) &= \mu((xy)+\ker\phi) \\ &= \phi(xy) \\ &= \phi(x)\phi(y) \\ &= \mu(x+\ker\phi)\mu(y+\ker\phi). \end{aligned}$$

So μ is a homomorphism. Also, note that $\mu(x+\ker\phi)=0$ implies $\phi(x)=0$ which is equivalent to x being in $\ker\phi$. So the kernel of μ is the coset $0+\ker\phi$ which is the additive identity over $R/\ker\phi$. Since μ has a trivial kernel, it must be injective. Also, μ is clearly surjective. So μ is a bijective homomorphism, and therefore an isomorphism.

Now suppose I is an ideal and consider the mapping γ defined in the theorem statement. We can easily see that γ is a homomorphism:

$$\gamma(x+y)=(x+y)+I=(x+I)+(y+I) \qquad \gamma(xy)=(xy)+I=(x+I)(y+I).$$

Also, note $\gamma(x)=0+I$ implies $x+I=0+I$ or equivalently $x\in I$. Also, clearly $\gamma(I)=0+I$ so $\ker\gamma=I$. □

Remark. Analogous to the case of groups, the fundamental homomorphism theorem shows us that ideals and kernels of ring homomorphism are the same.

Definition 40 (Principal Ideal)**.** A principle ideal of a commutative ring R is an ideal of the form $\{ra|r\in R\}$. The set $\{ra|r\in R\}$ is said to be the principal ideal generated by a and is denoted by $\langle a\rangle$.

Definition 41 (Principal Ideal Domain)**.** A principal ideal domain (PID) is an integral domain in which every ideal is principal.

Proposition 29. *$\mathbb{Z}$ is a principal ideal domain.*

Proof. Similar to subgroup of cyclic group cyclic. □

Lastly, we establish necessary and sufficient conditions for when a quotient ring is a field or integral domain. Before doing so we recall some standard terminology.

Definition 42. Let R be a ring. The ideal I of R is said to be trivial if $I=\{0\}$, and improper if $I=R$. If $I\neq R$ it is said to be a proper ideal, and if $I\neq\{0\}$ it is said to be a non-trivial ideal.

The following lemma is useful in achieving our goal of classifing quotient rings that are fields or integral domains.

Proposition 30. *If an ideal contains a unit, then it is improper.*

Proposition 31. *Suppose I is an ideal of the ring R, and $u \in I$ is a unit. Since u is a unit it posesses a multiplicative inverse u^{-1} in R, and sice I is closed under multiplication by elements in R we must have $uu^{-1} = 1$ be in I. Now since $1 \in I$ and $xI \subseteq I$ for all $x \in R$ we must have $R \subseteq I$. So $I = R$, and therefore I is improper.*

Proposition 32. *Let R be a ring with unity, and $M \subseteq R$ be an ideal of R. The quotient ring R/M is a field if and only if no other proper ideal contains M.*

Proof. First, suppose R/M is a field. This means that for any $u \notin I$ we can find u^{-1} so that $(u + I)(u^{-1} + I) = 1 + I$.... finish. □

Definition 43 (Maximal Ideal)**.**

Definition 44 (Prime Ideal)**.** An ideal $I \subseteq R$ is prime if $ab \in I$ implies $a \in I$ or $b \in I$.

Proposition 33. *R/N is an integral domain iff N prime.*

Corollary. Every maximal ideal is prime.

Remark. The trivial ideal is prime, and can be maximal (in which case R is a field).

3.3 Wedderburn's Little Theorem

Proposition 34 (Wedderburn's Little Theorem)**.** *Every finite division ring is a field.*

3.4 Field of Fractions of an Integral Domain

The construction is the abstract version of going from $\mathbb{Z}$ to $\mathbb{Q}$. Given an integral domain D define the relation $\sim$ on $D \times D$ by

$$(a, b) \sim (c, d) \iff ad = bc,$$

and let frac(D) be the set of equivalence classes of $D \times (D \setminus \{0\})$ with multiplication and addition defined as follows

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)] \qquad [(a, b)] \cdot [(c, d)] = [(ac, bd)].$$

It is easy (yet tedious) to see that the above operations are well-defined and make frac(D) into a field.

Definition 45 (Embedding)**.** A ring homomorphism $\phi : R \to R'$ is said to be an embedding of R in R' if $\phi(R) \simeq R'$.

Proposition 35. *The field of quotients of an integral domain is its minimal super-field. That is, if F is field and D is an integral domain embedded in F, then F has a subfield isomorphic to the field of quotients of D.*

3.5 Polynomials

Definition 46 (Ring of Formal Power Series)**.** Let R be a commutative ring with identity. The ring of formal power series over R in one indeterminate (denoted by $R[[x]]$) consists of the set of all sequences $P = (p_0, p_1, \ldots)$ in R, with addition and multiplication defined by

$$(P+Q)_i = p_i + q_i \qquad (PQ)_i = \sum_{j=0}^{i} p_j q_{i-j}.$$

We define the special elements $0 = (0, 0, \ldots)$, $x^0 := 1 := (1, 0, \ldots)$, and $x = (0, 1, 0, \ldots)$.

Remark. Since addition of formal power series is defined term-by-term and R is an abelian group under addition, $R[[x]]$ is an abelian group under addition. It is easy to see that 1, as defined above, is an identity element:

$$(P \cdot 1)_i = \sum_{j=0}^{i} p_j \delta_{0,i-j} = p_i = \sum_{j=0}^{i} \delta_{0,j} p_{i-j} = (1 \cdot P)_i.$$

It is not hard to see (add later) that multiplication is associative and commutative, and so $R[[x]]$ is a commutative ring with identity. This allows us to define integer powers of polynomials. In particular, we can see that $x^i_j = \delta_{ij}$. Equating the element a of R with the formal power series $(a, 0, \ldots)$, we can represent the formal power series $P = (p_0, p_1, \ldots)$ by

$$P = \sum_{i=0}^{\infty} p_i \cdot x^i.$$

Definition 47. Given a commutative ring R, the ring of polynomials in x over R (denoted by $R[x]$) consists of all elements of $R[[x]]$ that have finitely many non-zero terms.

Remark. By definition $R[x] \subseteq R[[x]]$ and clearly $R[x]$ is closed under formal power series addition and multiplication. So, indeed, $R[x]$ is a commutative ring.

Proposition 36. *If D is a commutative domain, then $D[x]$ is a domain.*

Proof. □

Definition 48 (Degree of a Polynomial)**.** The degree of $P \in R[x]$ is given by

$$\deg P = \begin{cases} -\infty & P = 0 \\ \max\{n \in \mathbb{N} \cup \{0\}; p_n \neq 0\} & \text{o.w..} \end{cases}$$

3.6 Ideals In Polynomial Rings

Proposition 37. *For any field F, the polynomial ring $F[x]$ is a principal ideal domain.*

Proof. similar to the case of $\mathbb{Z}$. □

Proposition 38. *For a non-constant polynomial $f \in F[x]$, the principal ideal $\langle f(x)\rangle$ is maximal in $F[x]$ if and only if f is irreducible over F.*

Proof. If f is reducible to pq certainly $\langle f\rangle \subseteq \langle p\rangle$ and so $\langle f\rangle$ is not maximal.

Suppose f irreducible and assume I is an ideal such that $\langle f\rangle \subseteq I$. Since $F[x]$ is a PID we must have $I = \langle g\rangle$ for some g. This implies $f = gq$ for some q since $g \in I$, but we must have $\deg q = 0$ or $\deg g = 0$ since otherwise f will be reducible. If $\deg g = 0$ the ideal I is improper, and if $\deg g = 0$ then $\langle g\rangle = \langle f\rangle$. So $\langle f\rangle$ is maximal. □

Corollary. We can conclude that the quotient ring $F[x]/\langle f\rangle$ for a non-constant polynomial f is a field if and only if f is irreducible in $F[x]$.

Proposition 39 (Euclid's Lemma for Polynomials)**.** *Let F be a field. If $p \in F[x]$ is irreducible and $p|fg$ then $p|f$ or $f|g$.*

Proof. Since p divides fg we must have $fg \in \langle p\rangle$. Since p is irreducible, $\langle p\rangle$ is maximal, and therefore prime. Hence, we must either have $f \in \langle p\rangle$ or $g \in \langle p\rangle$. □

Proposition 40. *Let F be a field. Any $p \in F[x]$ can be factored as a product of irreducible polynomials in $F[x]$, and the factorization is unique up to order and constant factors.*

3.7 Field Extensions

Definition 49. A field F is said to be an extension of the field E if F contains a subfield isomorphic to E.

Theorem 10 (Kronecker's Theorem)**.** *Given any field F and polynomial $f \in F[x]$, there exists an extension of F such that f has a root in $E[x]$.*

Proof.

1. If f has a root in F there's nothing to be done.
2. If f has no root in F, we can assume f is irreducible since f can be written as a product of irreducible factors, and if we can find an extension of F over which one of these factors has a root, f will have a root over that extension field. So assume f is irreducible.
3. We just showed that $E = F[x]/\langle f\rangle$ is a field. We claim E extends F and f has a root in E.

4. First consider the mapping $\phi : F \to E$ given by $\phi(a) = a + \langle f \rangle$. It is easy to see that E is a ring homomorphism, and that $\ker E = \{0\}$ so E is an isomorphism between F and $\phi(F)$. So E is an extension of F.

5. Now let $f = a_0 + a_1 x + \ldots + a_n x^n$ and note that for $\alpha = x + \langle f \rangle$ we have

$$\tilde{f}(\alpha) = \sum_{i=0}^{n} (a_i + \langle f \rangle)(x + \langle f \rangle)^i = \sum_{i=0}^{n} a_i x^i + \langle f \rangle = f(x) + \langle f \rangle = 0 + \langle f \rangle.$$

   So α is a root of f in E.

□

Definition 50 (Algebraic and Transcendental Elements)**.** Let E be an extension field of the field F. An element $\alpha \in E$ is said to be algebraic over F if it is a root of a polynomial in $F[x]$, and it is said to be transcendental over F otherwise.

Proposition 41. *If E is an extension field of the field F, and element $\alpha \in E$ is transcendental over F, if and only if the evaluation homomorphism $\varphi_\alpha : F[x] \to E$ given by $\varphi_\alpha(f) = \tilde{f}(\alpha)$ is injective. Note that in this case $F[x]$ is isomorphic to a subring of E.*

Proof. The homomorphism φ_α is injective, if and only if it has a trivial kernel. In which case there are no polynomials in $F[x]$ that have α as a root; i.e. α is a transcendental element over F. □

Remark. We can see that if $\alpha \in E$ is an algebraic element over F then the kernel of the homomorphism φ_α is non-trivial, and since $F[x]$ is a principal ideal domain ideal domain we must have $\ker \varphi_\alpha = \langle g \rangle$ for some polynomial $g \in F[x]$. Note that g must be irreducible since if $g = pq$ then where none of p or q are constant, then either $\tilde{p}(\alpha) = 0$ or $\tilde{q}(\alpha) = 0$ and in both cases the kernel cannot be limited to $\langle g \rangle$. This also implies that if α is a root of $f \in F[x]$ we must have $g|f$, and so among all polynomials that have α as a root g is has the smallest degree. This implies that g is unique up to a multiplicative factor. All this motivates the following definition.

Definition 51. If E is an extension field of the field F, and the element $\alpha \in E$ is algebraic over F then the monic polynomial $g \in F[x]$ that has α as a root and has the smallest degree among such polynomials is said to be the minimal polynomial of α over F.

Definition 52. The degree of an algebraic element over a field is the degree of its minimal polynomial.

Definition 53 (Simple Extension)**.**

Proposition 42. *A simple extension $F(\alpha)$ of F where α is algebraic and $\deg(\alpha, F) = n$ is a vector space over F for which $\{1, \alpha, \ldots, \alpha^n\}$ is a basis.*

3.8 Applications to Elementary Number Theory

3.9 Polynomial Factorization over $\mathbb{Z}$ and $\mathbb{Q}$

Proposition 43 (Gauss's Lemma)**.** *If $f \in \mathbb{Z}[x]$, then $r, s \in \mathbb{Q}[x]$ such that $f = rs$ exist, if and only if $p, q \in \mathbb{Z}[x]$ exist such that $f = pq$ and $\deg p = \deg r$ and $\deg q = \deg q$.*

Corollary. If a monic polynomial in $\mathbb{Z}[x]$ with non-zero constant term has a rational root, then it must have an integer root that divides its constant term.

Theorem 11 (Eisenstein Criterion)**.** *Let $f = f_0 + f_1 x + \ldots + f_n x^n$ be a polynomial in $\mathbb{Z}[x]$, and suppose p is a prime number. The polynomial f is irreducible over $\mathbb{Z}$ if the following hold:*

1. *$p \not| f_n$*
2. *for all $0 \leq i < n$, we have $p | f_i$*
3. *$p^2 \not| f_0$*

Proof. Assume

$$f(x) = (p_r x^r + \ldots + p_0)(q_s x^s + \ldots + q_0)$$

with $r, s < n$.

1. Use Euclid's lemma to show that we can WLOG assume $p | p_0$ but $p | q_0$.
2. Assume for some $p | p_j$ for all $0 \leq j \leq i < r$ and show that $p | p_{i+1}$ since we must have $p | a_{i+1}$.
3. Hence, all the p_is are multiples of p and so all the f_i must be. This contradicts $p \not| f_n$.

□

Corollary. By Gauss's Lemma, if the Eisenstein criterion holds for a polynomial $f \in \mathbb{Z}[x]$ for a prime p, then f is irreducible over $\mathbb{Q}$.

Proposition 44. *If p is a prime, then the p-th cyclotomic polynomial*

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

is irreducible over $\mathbb{Q}$.

Proof. If $\Phi_p(x)$ reducible then $\Phi_p(x+1)$ reducible and

$$\Phi_p(x+1) = \sum_{i=1}^{p} \binom{p}{i} x^{i-1}$$

which satisfies an Eisenstein criterion at p. □

3.9.1 An Alternate Proof of Euler's Theorem

Proposition 45. *The set of elements in a ring with no zero divisors form a group under multiplication.*

3.9.2 Solving $ax = b$ in $\mathbb{Z}/n\mathbb{Z}$

Proposition 46 (Zero Divisors in $\mathbb{Z}_n$)**.**