Abstract Algebra

November 25, 2013

Author: James Brofos
james.a.brofos.15@dartmouth.edu
http://www.cs.dartmouth.edu/~james/
Dartmouth College

Abstract

Presented here is a detailed discussion of select topics in algebra as obtained from Dartmouth College's Math 71 offering. We hope that these notes will be useful to students of algebra and will serve as a resource for those wishing to refresh their memory. Notice that these notes are intended as an introduction to algebra, and only some prior understanding of linear algebra will be necessary for reading this document.

1 Group Theory

Definition Fix $n \in \mathbb{Z}$. Say that two integers a, b are congruent modulo n if $a = b + kn$ for some $k \in \mathbb{Z}$. Write that $a \equiv b(\mod n)$. Equivalently, $a - b = kn$ or $n|(a - b)$.

Example For example $1 = 6 + (-1)(5) \implies 1 \equiv 6(\mod 5)$.

Let $[a] = \{a + kn|k \in \mathbb{Z}\}$. We call this the congruence class of a. Let $\mathbb{Z}/n\mathbb{Z} = \{[a]|a \in \mathbb{Z}\}$.

Example As an example, let $n = 5$, then $[0] = \{\ldots, -5, 0, 5, 10, \ldots\} = [5]$, $[1] = \{\ldots, -4, 1, 6, \ldots\} = [6]$. $\mathbb{Z}/5\mathbb{Z} = \{[0], [1], [2], [3], [4]\}$.

Proposition 1.1 $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n - 1]\}$.

Proof *Recall the Division Algorithm that given $a, b \in \mathbb{Z}\exists$ unique integers q, r with $a = bq + r$ and $0 \leq r < |b|$. Then given a, n there exists unique q, r with $a = nq + r$ and $0 \leq r \leq n - 1$. We have $[a] = \{a + kn|k \in \mathbb{Z}\} = \{nq + r + kn|k \in \mathbb{Z}\} = \{r + n(k + q)|k \in \mathbb{Z}\} = [r]$.*

Suppose $0 \leq a \leq b \leq n - 1$ and that $[a] = [b]$. Then $a \equiv b(\mod n)$ and $a = b + kn$ with $k \in \mathbb{Z}$ and $n|(a - b)$. But $0 \leq |a - b| \leq n - 1 \implies a - b = 0 \implies a = b$.

Thus, $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n - 1]\}$.

Structure: $[a] + [b] = [a + b]$ and $[a][b] = [ab]$

Lemma 1.2 *Addition and multiplication of congruence classes is a well-defined operation.*

Proof *Let $[a] = [b], [c] = [d]$. Thus, $a = b + k_1 n$ and $c = d + k_2 n$, $k_1, k_2 \in \mathbb{Z}$. We have that $a + c = b + d + k_1 n + k_2 n = b + d + k_3 n$ for some $k_3 \in \mathbb{Z}$. Show multiplication is well-defined as exercise.*

Definition Equivalence relations are relationships between two objects. For example $a, b \in \mathbb{Z}$ may have $a = b, a \leq b$. A binary relation on a nonempty set S is a subset of $R \subseteq S \times S = \{(s_1, s_2)|s_1, s_2 \in S\}$. We say that $a \sim b$ if $(a, b) \in R$. A relation on a set S is:

1. Reflexive if $a \sim a \; \forall \; a \in S$
2. Symmetric if $a \sim b \implies b \sim a \; \forall \; a, b \in S$

3. Transitive if $a \sim b$ and $b \sim c \implies a \sim c \; \forall \; a, b, c \in S$

A relation $\sim$ on a nonempty set S is an equivalence relation if it is reflexive, symmetric, and transitive.

Partition: A partition of a nonempty set S is a set of nonempty subsets $\{A_i\}$ such that:

1. $S = \cup_{i \in I} A_i$
2. $A_i \cap A_j = \{\varnothing\}$ when $i \neq j$.

Example As an example, consider possible partitions of $\mathbb{Z}$. We have $P_1 = \{\ldots, \{-2\}, \{-1\}, \{0\}, \{1\}, \{2\} \ldots\}$ or $P_2 = \{\{\text{odd numbers}\}, \{\text{even numbers}\}\}$.

Proposition 1.3 *Let S be a nonempty set. Then an equivalence relation on S gives rise to a partition of S. Further, a partition gives rise to a equivalence relation.*

Proof *Suppose $\{A_i\}$ is a partition of S. Let $a, b \in S$. Let $a \sim b$ if $a, b \in A_j$ for some j. The relation is reflexive practically by definition and we need only confirm that indeed $a \in A_i$ for some i. Suppose $a \sim b$, so $a, b \in A_i$. So $b, a \in A_i$ so $b \sim a$. Suppose that $a \sim b$ and $b \sim c$ and $a, b \in A_i$ and $b, c \in A_j$. We want to show that $a \sim c$ and that $A_i = A_j$. We know $b \in A_i \cap A_j = \{\varnothing\}$ unless $i = j$. So $A_i = A_j$ and $a \sim c$.*

Conversely, suppose $\sim$ is an equivalence relation on S. Then simply $P = \{[a] | a \in S\}$.

Definition A binary operation on a nonempty set G if a function $\star : G \times G \to G$. We write $\star(a, b)$ as $a \star b$. A binary operation is associative if $(g_1 \star g_2) \star g_3 = g_1 \star (g_2 \star g_3) \; \forall g_1, g_2, g_3 \in G$. The operation is commutative if $g_1 \star g_2 = g_2 \star g_1 \; \forall \; g_1, g_2 \in G$.

Definition A group is a set G with a binary operation $\star : G \times G \to G$ such that:

1. $\star$ is associative
2. $\exists e \in G$ such that $e \star a = a \star e = a \; \forall \; a \in G$. e is called the identity.
3. $\forall \; a \in G, \exists a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = e$. a^{-1} is called an inverse.

If $\star$ is also commutative, say that $(G, \star)$ is abelian. We say a group is finite or infinite if the set G is finite or infinite. Consider $(\mathbb{Z}, +)$:

1. $+$ is associative
2. $0 + a = a + 0 = a$ so zero is the identity
3. Let $a \in \mathbb{Z}$. Then $a + (-a) = 0 = (-a) + a$ so $-a$ is the inverse of a.

Therefore, $(\mathbb{Z}, +)$ is a group. Since addition is commutative, $(\mathbb{Z}, +)$ is abelian.

Are the following groups:

- $(\mathbb{N}, +)$. No, because there is no inverse element
- $(\mathbb{Z}, -)$. No, because $0 - a \neq a - 0$.
- $(\mathbb{Z} - \{0\}, \times)$. No, because 2 has no inverse.
- $(\mathbb{Q} - \{0\}, \times)$. Yes.
- $(Gl_n(F))$. No under addition, but yes under multiplication.
- $(M_n(F))$. Yes under addition, but no under multiplication.

If $(A, \star)$ and $(B, \circ)$ are groups, consider $A \times B = \{(a, b) | a \in A, b \in B\}$. Consider the operation $(a_1, b_1) \diamond (a_2, b_2) = (a_1 \star a_2, b_1 \circ b_2)$. Then $(A \times B, \diamond)$ is a group called the direct product of A and B. Consider $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} = \{([a], b) | a \in \{0, 1\}, b \in \mathbb{Z}\}$. Then $([0], 6) \diamond ([1], -11) = ([1], -5)$.

Proposition 1.4 *Let G be a group under $\star$. Then:*

1. *The identity is unique.*
2. *The inverse of a is unique*
3. $(a^{-1})^{-1} = a$
4. $(a \star b)^{-1} = b^{-1} \star a^{-1}$

Proof *We provide the following proof:*

1. *Suppose e_1 and e_2 are both identities. Then $e_1 \star a = a \star e_1 = a \ \forall \ a \in G$. $e_2 \star a = a \star e_2 = a \ \forall \ a \in G$. $e_1 \star e_2 = e_1 = e_2$. Therefore, identity is unique.*
2. *Suppose a has two inverses b, c. Then $a \star b = b \star a = e$ and $a \star c = c \star a = e$. $b = b \star e = b \star (a \star c) = (b \star a) \star c = e \star c = c$. Therefore, inverse is unique.*
3. $(a \star b) \star (b^{-1} \star a^{-1}) = e = (b^{-1} \star a^{-1}) \star (a \star b) \leftarrow$ *Show this and the fourth property as an exercise.*

Proposition 1.5 *For $(G, \star)$ a group, $a, b \in G$, then $ax = b$ and $ya = b$ has a unique solution.*

Definition The order of a group is the number of elements in G and denote this number $|G|$. The order of $a \in G$ is the smallest positive integer n such that $a^n = e$. If no such n exists, then we say that a has infinite order.

Example Consider $(\mathbb{Z}, +)$. Then $|5| = \infty$ and $|-12| = \infty$ and $|0| = 1$. Indeed, $|a| = \infty \ \forall \ a \neq 0$. Consider $(\mathbb{Z}/4\mathbb{Z}, +)$, then $|[0]| = 1, |[1]| = 4, |[2]| = 2, |[3]| = 4, |\mathbb{Z}/4\mathbb{Z}| = 4$.

Proposition 1.6 *If $|g| = n \ \forall \ g \in G$ and $g^m = e$ for some $m \in \mathbb{Z}$, then $n|m$.*

Proof *We have $n \leq m$. Division Algorithm gives $m = nq + r, 0 \leq r \leq n-1$. We desire that $r = 0$. Write that $e = g^m = g^{nq+r} = g^r$ and $r < n$ so $r = 0$.*

Definition Let D_{2n} be the set of all symmetries of a regular n-gon. Rigid motions of $\mathbb{R}^3$ preserving the n-gon. For example reflections and rotations.

For example, $D_6 = \{1, r, r^2, s, sr, sr^2\}$ and $|D_6| = 6$.

Lemma 1.7 $|D_{2n}| = 2n$

Proof *A symmetry preserves adjacency. Let f be a symmetry of the n-gon. There are n possibilities for $f(1)$, two possibilities for $f(2)$ and only one possibility for $f(3)$. Thus, there are $2n$ possible symmetries.*

Let r be a clockwise rotation through the center by $\frac{2\pi}{n}$ radians. Let s be reflection through the line between the vertex one and the center. Then:

1. $r, r^2, \ldots, r^{n-1}$ and $r^n = 1$ are all distinct.
2. $|s| = 2$.
3. $s \neq r^i$ for any i since $s(1) = 1$ and $s(2) = n$, but $r^i(1) = i+1$, $r^i(2) = i+2$. If $r^i(1) = 1$, then $i = 0$, but $r^0(2) = 2 \neq n$.
4. $sr^i \neq sr^j$ since $sr^i = sr^j \implies ssr^i = ssr^j \implies r^i = r^j \implies i = j$.
5. $sr^i \neq r^j$

We say that r, s generate the dihedral group. Products of r, s and their inverses give the whole group.

Lemma 1.8 *$rs = sr^{-1}$. In particular, D_{2n} is not abelian. Suppose that $sr^{-1} = rs = sr \implies r^{-1} = r$. Clearly, this is not true so the group is not abelian.*

Proof *We proceed by induction. We have that $r^i s = sr^{-i}$ so $r^i s = rr^{i-1}s = r(sr^{-i+1}) = sr^{-1}r^{-(i-1)} = sr^{-i}$*

Definition A presentation of a group G consists of a generating set S and a set of relations R and from these we may completely determine the structure of G. We write $G = \langle \{\text{generators}\} | \{\text{relations}\} \rangle$. Consider $D_6 = \langle r, s | r^3 = 1 = s^2, rs = sr^{-1} \rangle$ and $D_{2n} = \langle r, s | r^n = 1 = s^2, rs = sr^{-1} \rangle$. Consider $\mathbb{Z}/3\mathbb{Z} = \langle [1] | [1]^3 = [0] = e \rangle$

Let S_n be the set of bijections from $\{1, 2, \ldots, n\}$ to itself. Elements of S_n are called permutations. For example $\sigma = (1\ 3\ 2)(4\ 5)$ and $\tau = (1\ 3)(2\ 4)$. The length of a cycle is the number of integers appearing in the cycle. Two cycles are disjoint if they have no integers in common. Note that disjoint cycles commute: $\gamma = (1\ 3) \circ (2\ 3) = (1\ 3\ 2)$.

Cycle decomposition writes $\sigma \in S_n$ as a product of disjoint cycles. $\sigma \circ \tau$ is read right to left. Do τ first, then perform σ. $\sigma \circ \tau(1) = \sigma(3) = 2$. We have $\sigma \circ \tau = (1\ 2\ 5\ 4)$ and $\tau \circ \sigma = (1\ 3)(2\ 4) \circ (1\ 3\ 2)(4\ 5) = (2\ 3\ 4\ 5)$. S_n is a group under composition called the symmetric group:

1. Function composition is associative.
2. $(1)(2) \ldots (n) = e$ is the identity.
3. Every bijection has an inverse.

Lemma 1.9 $|S_n| = n!$. *For example* $S_3 = \{(1)(2\ 3), (1)(2)(3), (1\ 2)(3), (1\ 2\ 3), (1\ 3)(2), (1\ 3\ 2)\}$.

Let $\sigma \in S_n$ such that $\sigma = \sigma_1\sigma_2 \ldots \sigma_k$. Then $|\sigma| = \text{LCM}\{|\sigma_1|, |\sigma_2|, \ldots, |\sigma_k|\}$.

Definition A field F is a set along with two binary operations $+, \star$ such that $(F, +)$ is an abelian group and $(F - \{0\}, \star)$ is abelian too. We also require that $a \star (b + c) = a \star b + a \star c$ and $(a + b) \star c = a \star c + b \star c\ \forall\ a, b, c \in F$.

Example We have $(\mathbb{R}, +, \star), (\mathbb{C}, +, \star), (\mathbb{Q}, +, \star)$. However $(\mathbb{Z}, +, \star)$ is not a field, however. When p is a prime, consider $\mathbb{Z}/p\mathbb{Z}$:

1. $(\mathbb{Z}/p\mathbb{Z}, +)$ is an abelian group.
2. $(\mathbb{Z}/p\mathbb{Z})^\times = \{[a] | (a, p) = 1\} = \mathbb{Z}/p\mathbb{Z} - \{0\}$.

We write $\mathbb{F}_p$ for $\mathbb{Z}/p\mathbb{Z}$.

Hamilton's Quarternions: $\mathbb{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ such that $i^2 = j^2 = k^2 = -1, ij = k, -ji = k$. Then $\mathbb{Q}_8 = \langle i, j, k | i^2 = j^2 = k^2 = -1, ij = k, -ji = k\rangle$.

Let V, W be vector spaces and let $f : V \to W$ be a linear transformation. That is, $f(v + w) = f(v) + f(w)$ and $f(cv) = cf(v)$. If f is bijective, then it is an isomorphism.

Definition Let $(G, \star)$ and $(H, \circ)$ be groups. Then a function $\phi : G \to H$ is a homomorphism if $\phi(g_1 \star g_2) = \phi(g_1) \circ \phi(g_2)\ \forall\ g_1, g_2 \in G$. Often write that $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$. We have that ϕ is an isomorphism if it is a bijective homomorphism.

If exists an isomorphism between G, H we say G. For example $\phi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ such that $\phi(a) = [a]$. We have that $\phi(a + b) = [a + b] = [a] + [b] = \phi(a) + \phi(b)$. Thus, homomorphic and $\phi(1) = [1] = [7] = \phi(7)$, so not injective. If $[a] \in \mathbb{Z}/6\mathbb{Z}$ then $\phi(a) = [a]$ so surjective.

Consider $\exp : (\mathbb{R}, +) \to (\mathbb{R}, \star)$ such that $\exp(a) = e^a$. Then $\exp(a + b) = e^{a+b} = e^a e^b = \exp(a)\exp(b)$. Then it will suffice to find an inverse homomorphism. Say $\log : (\mathbb{R}, \star) \to (\mathbb{R}, +)$. Therefore, $\log[a \star b] = \log a + \log b$, so homomorphic. We have then $\exp[\log b] = e^{\log b} = b$ and $\log[\exp a] = \log e^a = a$, so the two are inverses and therefore exp is an isomorphism.

If $\phi : G \to H$ is a homomorphism, then $\phi(e_G) = e_H$ and $\phi(x^n) = \phi(x)^n$. If ϕ is isomorphism, then $|G| = |H|$. G is abelian $\iff$ H is abelian. Further, $\forall\ x \in G, |x| = |\phi(x)|$.

We will see that all groups of order six are either $\mathbb{Z}/6\mathbb{Z}$ or S_3. $\mathbb{Z}/6\mathbb{Z}$ is not isomorphic to S_3 because S_3 is not abelian, whereas $\mathbb{Z}/6\mathbb{Z}$ is abelian. Further, $\mathbb{Z}/6\mathbb{Z}$ has an element of order six, but S_3 has elements of order one, two, or three.

Definition A subgroup H of a group G is a subset of G that is itself a group under the operation inherited from G. We write that $H \leq G$.

Example We simply have $\mathbb{Z} \leq \mathbb{R}$ under addition. For any group G, $\{e\} \leq G$ is the trivial subgroup. Further, $G \leq G$.

Proposition 1.10 ***The Subgroup Criterion***. *If G is a group and H is a subgroup of G and $H \neq \{\varnothing\}$. Then the following are equivalent:*

1. *$H \leq G$*
2. *H is closed under multiplication and inverses*
3. *$\forall\ x, y \in H, xy^{-1} \in H$*

Proof $H \leq G \implies H$ **closed under multiplication and inverses** : *True by definition.*
H **closed under multiplication and inverses** $\implies \forall\ x, y \in H, xy^{-1} \in H$: *We have that $y^{-1} \in H$ since closed under inverses. Then $xy^{-1} \in H$ since closed under multiplication.*
$\forall\ x, y \in H, xy^{-1} \in H \implies H \leq G$: *We examine the conditions necessary for a group:*

1. *Identity: Since H is not empty, $\exists x \in H$ and $xx^{-1} \in H$ and $xx^{-1} = e \in H$.*
2. *Inverse: Let $x \in H$. Since $e \in H$, $ex^{-1} \in H \implies x^{-1} \in H$.*
3. *Associativity: Free because inherited from G.*
4. *Binary: Let $x, y \in H$. $y \in H \implies y^{-1} \in H$ so $x(y^{-1})^{-1} \in H \implies xy \in H$.*

Consider $D_6 = \{1, r, r^2, s, sr, sr^2\}$ and $H = \{1, r, r^2\}$. H is closed under multiplication and inverses since $1^{-1} = 1, r^{-1} = r^2, (r^2)^{-1} = r \implies H \leq D_6$. We may also have $\mathbb{Z}/6\mathbb{Z}$ with $H = \{[0], [2], [4]\}$. H is closed under addition and inverses: $[2] + [4] = [4] + [2] = [0]$. Hence, $H \leq \mathbb{Z}/6\mathbb{Z}$.

Definition Let G be a group and $x \in G$. Then the cyclic subgroup generated by G is $\langle x \rangle = \{x^n | n \in \mathbb{Z}\}$. Say that G is cyclic if $G = \langle x \rangle$. As above, the first subgroup is generated by r, so $H = \langle r \rangle$. The second subgroup is generated by $[2]$, so $H = \langle [2] \rangle$. Notice that $\mathbb{Z}/6\mathbb{Z} = \langle [1] \rangle$ and $\mathbb{Z} = \langle 1 \rangle$.

Proposition 1.11 *All cyclic groups are abelian.*

Proof *Let G be a cyclic subgroup. Then $G = \langle x \rangle$ for $x \in G$. Let $g, h \in G$. Then $g = x^a, h = x^b$ for $a, b \in \mathbb{Z}$. Then $gh = x^a x^b = x^{a+b} = x^{b+a} = x^b x^a = hg$.*

Proposition 1.12 *If $G = \langle x \rangle$ then $|G| = |x|$. In particular, $|G| = n < \infty \iff x^n = e$. Then $\{1, x, x^2, \ldots, x^{n-1}\}$ are the distinct elements of G. If $|G| = \infty$, then $x^n \neq e\ \forall\ n \in \mathbb{Z} - \{0\}$ and $x^a \neq x^b\ \forall\ a, b \in \mathbb{Z}$.*

Proof *Let $|G| = n$ and suppose $|x| = m$. We know that $\{1, x, \ldots, x^{m-1}\}$ are all distinct. Then $\{1, x, \ldots, x^{m-1}\} \subseteq G$. Let $x^t \in G$. The Division Algorithm gives that $t = mq + r$ for $0 \leq r < |m|$. Then $x^t = x^{mq+r} = x^r \implies x^t = x^r \implies x^t \in \{1, x, \ldots, x^{m-1}\} \implies G \subseteq \{1, x, \ldots, x^{m-1}\}$. The other direction is clear since the elements are given.*

Suppose $|G| = \infty$ and $x^n = e$. Then $x^{-n} = (x^n)^{-1} = e$. Then by previous part $|G|$ is finite so contradiction. If $x^a = x^b \implies x^{b-a} = e$, but we just showed this was impossible. Therefore $\{1, x, x^2, \ldots\}$ are all distinct $\implies |G| = \infty$.

Theorem 1.13 ***Lagrange's Theorem***. *If G is a group and $H \leq G$, then $|H|$ divides $|G|$.*

Corollary 1.14 *Any group of prime order p is cyclic.*

Proof *Let $|G| = p$ and $x \in G$ such that $x \neq e$. Let $H = \langle x \rangle$. Note that $H \neq \{e\}$ so $|H| \neq 1$. By Lagrange, $|H|$ divides p. Therefore, $|H| = p$. Thus, $H \leq G$ and $|H| = |G|$ and both have finite order. Therefore, $H = G$.*

Theorem 1.15 *Any two cyclic groups of the same order are isomorphic.*

Proof *Suppose $|G| = |H| = n < \infty$ and $G = \langle x \rangle = \{x^k | k \in \mathbb{Z}\}$ and $H = \langle y \rangle = \{y^k | k \in \mathbb{Z}\}$. Let $\phi : G \to H$ such that $\phi(x^k) = y^k$. We must check that ϕ is well-defined, is a homomorphism, is surjective, and is injective. If $x^k = x^l$, show that $\phi(x^k) = \phi(x^l)$. Notice that $|x| = |y| = n \implies n | k - l \implies k = nq + l$. Then $\phi(x^k) = y^k = y^{nq+l} = y^l = \phi(x^l)$. Let $x^a, x^b \in G$. Then $\phi(x^a x^b) = \phi(x^{a+b}) = y^{a+b} = y^a y^b = \phi(x^a)\phi(x^b)$.*

We show next surjectivity: Let $y^m \in H$ and $\phi(x^m) = y^m$. For injectivity we do: If $\phi(x^a) = \phi(x^b)$, then we must show that $x^a = x^b$. This implies that $y^a = y^b \implies y^{a-b} = 1$. So $n|a-b \implies a = nq + b$. Then $x^a = x^{nq}x^b = x^b$. Therefore ϕ is an isomorphism.

Suppose that G is cyclic and $|G| = \infty$. We have that $G = \langle x \rangle$ and $|x| = \infty$. Let $\phi : \mathbb{Z} \to G$ such that $\phi(a) = x^a$. We must check that ϕ is a homomorphism, that it is injective, that it is surjective. $\phi(a+b) = x^{a+b} = x^a x^b = \phi(a)\phi(b)$. For surjectivity: Let $x^a \in G$. Then $a \in \mathbb{Z}$ and $\phi(a) = x^a$. For injectivity: If $\phi(a) = \phi(b) \implies x^a = x^b$, so $a = b$ because all powers are distinct when $|x| = \infty$. Therefore ϕ is an isomorphism.

We define Z_n to be the unique cyclic group of order n. In particular, $Z_n = \langle x \rangle = \{1, x, x^2, \dots, x^{n-1}\}$ where $|x| = n$. We have that $Z_n \cong \mathbb{Z}/n\mathbb{Z}$.

Proposition 1.16 *For G a group and for $x \in G$ and $a \in \mathbb{Z} - \{0\}$. Then if $|x| = \infty$ then $|x^a| = \infty$. If $|x| = n < \infty$ then $|x^a| = \frac{n}{(n,a)}$ and in particular, if $a|n$ then $|x^a| = \frac{n}{a}$.*

Proof *If $|x| = \infty$. Suppose $|x^a| = n$. Then $x^{an} = 1$, but then x has finite order, which is a contradiction. Suppose $|x| = n$. We want to show that $|x^a| = \frac{n}{(n,a)}$. Let $d = (a, n)$, so $a = da'$ and $n = dn'$ such that $(a', n') = 1$. We want to show that $|x^a| = \frac{n}{d} = n'$. We need that $(x^a)^{n'} = 1$ and also n' is smallest positive possibility. $(x^a)^{n'} = x^{an'} = x^{da'n'} = x^{dn'a'} = (x^n)^{a'} = 1$. Let $|x^a| = k$. Then $k|n'$ and $x^{ak} = 1$. Then $n|ak$. Since $dn'|da'k \implies n'|a'k$ we have that $n'|k$ since $(n', a') = 1$. So $n' = \pm k$, but both are positive so we obtain $n' = k$.*

Example Consider as an example $Z_6 = \{1, x, x^2, x^3, x^4, x^5\} \cong \mathbb{Z}/6\mathbb{Z} = \{[0], [1], [2], [3], [4], [5]\}$ and $|x| = 6$ and $|x^2| = 3$.

Generators of a Group: Suppose $G = \langle x \rangle \iff |x^a| = n \iff n = \frac{n}{(n,a)} \iff (n, a) = 1$.

Proposition 1.17 *If G is a cyclic group then:*

1. *If $|G| = n < \infty$ then x^a generates $G \iff (a, n) = 1$*
2. *If $|G| = \infty$ then $G = \langle x^a \rangle \iff a = \pm 1$*

Example Consider as an example $Z_6 \cong \mathbb{Z}/6\mathbb{Z}$. Then $\langle x \rangle = Z_6 = \langle x^5 \rangle$ and $\langle [1] \rangle = \mathbb{Z}/6\mathbb{Z} = \langle [5] \rangle$.

Theorem 1.18 *Let G be a cyclic group $G = \langle x \rangle$.*

1. *All groups of a cyclic group are cyclic. If $H \leq G$ then $H = \{e\}$ or $H = \langle x^d \rangle$ where d is the smallest positive power appearing in H.*
2. *If $|G| = \infty$, then $\langle x^a \rangle \neq \langle x^b \rangle \ \forall \ a \neq b, a, b \in \mathbb{Z}^+$. Further $\langle x^a \rangle = \langle x^{-a} \rangle \ \forall \ a \in \mathbb{Z}$.*
3. *If $|G| = n < \infty$ then for each positive divisor a of n $\exists$ a unique subgroup of order a: $\langle x^{\frac{n}{a}} \rangle$. Further $\langle x^b \rangle = \langle x^{(b,n)} \rangle$.*

Proof *The proof is as follows:*

1. *If $H \leq G$. Note that if $H = \{e\}$ then we are done immediately. The let $H = \{e\}$. Then there exists $a \in \mathbb{Z} - \{0\}$ with $x^a \in H$. Then $x^{-a} \in H$ by closure of subgroups. So there is some positive power of $x \in H$. Define $P = \{b | b \in \mathbb{Z}^+, x^b \in H\}$. We can see that P is nonempty and P is a set of positive integers. Thus. P has a least element d by the well-ordering principle. Consider x^d then $x^d \in H$. Then $\langle x^d \rangle \leq H$. We wish to show that $H \leq \langle x^d \rangle$. Then let $x^a \in H$. Want that $x^a = x^{dk}$. By the Division Algorithm $a = dq + r$ where $0 \leq r < d$. Write that $x^r = x^{a-dq} = x^a (x^d)^{-q}$. We know that $x^a, (x^d)^{-q} \in H$. Therefore, $x^r \in H$. But d was smallest power, so $r = 0$. If $r = 0$, then $d|a$. Thus $x^a = x^{dq} \in \langle x^d \rangle \implies H \leq \langle x^d \rangle$.*
2. *Let $|G| = \infty$. Clearly $\langle x^a \rangle = \langle x^{-a} \rangle \ \forall \ a \in \mathbb{Z}$ since $x^a \in \langle x^{-a} \rangle$ and $x^{-a} \in \langle x^a \rangle$. Now let $a, b \in \mathbb{Z}^+$ and suppose $\langle x^a \rangle = \langle x^b \rangle$. Want to show that $a = b$. Then $x^a \in \langle x^b \rangle$ and $x^b \in \langle x^a \rangle$. Thus, $x^a = x^{br}$ and $x^b = x^{as}$. So $a = br$ and $b = as$. Therefore $a|b$ and $b|a$. So $a = \pm b$, but both are positive so $a = b$.*

3. *Suppose G has finite order and let a be a positive divisor of n. We want to show that $\langle x^{\frac{n}{a}} \rangle$ is the unique subgroup of order a. Let $d = \frac{n}{a}$ so $ad = n$ so $d|n$. We have that $|x^d| = \frac{n}{(n,d)} = \frac{n}{d} = a \implies |\langle x^d \rangle| = a$. Let $K \leq G$ such that $|K| = a$. Then $K = \langle x^b \rangle$ for some integer b. Then $|x^b| = \frac{n}{(b,n)} = a = \frac{n}{d}$. So $d = (n,b)$. Then $d|b \implies dq = b$. Thus, $x^b = x^{dq}$. Thus, $x^b \in \langle x^d \rangle$. Thus $K \leq \langle x^d \rangle$. The two groups have the same number of elements. That is $|K| = |\langle x^d \rangle| = a \leq \infty$. Therefore, $K \leq \langle x^d \rangle \implies K = \langle x^d \rangle$.*

Definition If A is a subset of G, let:

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

Be the subgroup generated by A. This is the smallest subgroup of G that contains A. $\langle A \rangle$ is a subgroup because $e \in H \;\forall\; H$ in intersection. Let $x, y \in A$. Then $xy^{-1} \in A$ because $xy^{-1} \in H \;\forall\; H$ in intersection because the H are subgroups.

Notice that $\mathbb{Z}$ is an infinite cyclic subgroup generated by one. Thus $\mathbb{Z} = \langle 1 \rangle$. For $n \in \mathbb{Z}$, let $n\mathbb{Z} = \{nz | z \in \mathbb{Z}\}$. We have subgroups of $\mathbb{Z} : \langle 0 \rangle$ and $\langle 1 \rangle = \mathbb{Z} = 1\mathbb{Z}$ and $\langle 2 \rangle = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = 2\mathbb{Z}$ and $\langle n \rangle = n\mathbb{Z}$. Let $g \in \mathbb{Z}$ and define $g + n\mathbb{Z} = \{g + h | h \in n\mathbb{Z}\}$. Let $\mathbb{Z}/n\mathbb{Z} = \{g + n\mathbb{Z} | g \in \mathbb{Z}\}$.

Example We know $2+3\mathbb{Z} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$, which is the congruence class of $2 (\mod 3)$. Then, $\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\} = \{[0], [1], [2]\}$. We also see that $\mathbb{Z}$ is equal to the disjoint unions of $[0], [1], [2]$.

Definition Let G be a group and let $H \leq G$. Write that $g \star H = gH = \{g \star h | h \in H\}$ a left coset of H in G.

All of the following theorems apply also to right cosets, which are analogous. Recall that a partition of G is a set of subsets $\{A_i\}$ such that $G = \cup_{i \in I} A_i$ and $A_i \cap A_j = \{\varnothing\}$ when $i \neq j$.

Proposition 1.19 *Let G be a group and $H \leq G$. Then left cosets of H in G partition G.*

Proof *We can see that $G = \cup_{g \in G} gH$. Suppose that $g_1 H \cap g_2 H$ is nontrivial. Let $g \in g_1 H \cap g_2 H$. Then $g = g_1 h_1$ for some $h_1 \in H$ and $g = g_2 h_2$ for some $h_2 \in H$. Let $g_1 h \in g_1 H$. We have that $g_1 = g_2 h_2 h_1^{-1}$ and $g_2 = g_1 h_1 h_2^{-1}$. Thus, $g_1 h = g_2 h_2 h_1^{-1} h \implies g_1 h \in g_2 H$. Therefore, $g_1 H \subseteq g_2 H$. Let $g_2 h' \in g_2 H$. Then $g_2 h' = g_1 h_1 h_2^{-1} h' \in g_1 H \implies g_2 H \subseteq g_1 H \implies g_1 H = g_2 H$.*

Note that no coset except $1H$ is a subgroup of G. Therefore, $1 \in H$ since cosets partition G, no other coset may contain 1.

Corollary 1.20 *Let $H \leq G$. Then $g_1 H = g_2 H \iff g_2^{-1} g_1 \in H \iff g_1 g_2^{-1} \in H$.*

Proof *Suppose $g_1 H = g_2 H$. We know that $g_1 1 \in g_1 H$. Since $g_1 H = g_2 H$, $g_1 \in g_2 H$. Therefore $g_1 = g_2 h$ for some $h \in H$. Thus, $g_2^{-1} g_1 = h \implies g_2^{-1} g_1 \in H$. Suppose $g_2^{-1} g_1 \in H \implies g_2^{-1} g_1 = h \in H$. So $g_1 = g_2 h \implies g_1 \in g_2 H \implies g_1 \in g_1 H \cap g_2 H \implies g_1 H = g_2 H$.*

Let $G/H = \{gH | g \in G\}$. This is called the set of left cosets. For example, let $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. We obtain that $G/H = \mathbb{Z}/n\mathbb{Z} = \{g + n\mathbb{Z} | g \in \mathbb{Z}\} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$.

Suppose that $aH = cH$ and let bH be any other coset. Suppose that $bH = dH$. Then we will need that $aH \cdot bH = cH \cdot dH \implies (ab)H = (cd)H$, which further implies that $(cd)^{-1}(ab) \in H$. We know that $c^{-1}a = h_1 \in H$ and $d^{-1}b = h_2 \in H$. Then $(cd)^{-1}(ab) = d^{-1}h_1 b = d^{-1}bb^{-1}h_1 b = h_2 b^{-1} h_1 b$. This implies that we need $b^{-1} h_1 b \in H \;\forall\; b \in G, h_1 \in H$.

Definition A subgroup H is normal if $gHg^{-1} = H \;\forall\; g \in G$. That is, if $g_1 H g_2 H = g_1 g_2 H$. We call G/H the quotient group for a normal H.

Definition Let $N_G(H) = \{g \in G | gHg^{-1} = H\}$. This is the normalizer of H in G. If $H \trianglelefteq G \iff N_G(H) = G$.

Proposition 1.21 *Let $H \leq G$. Then the following are equivalent:*

1. $H \trianglelefteq G$
2. $gH = Hg \ \forall \ g \in G$
3. $gHg^{-1} \subseteq H \ \forall \ g \in G$

Proof *First note that if $S \subseteq G$ and $T \subseteq G$ with $T = S$, then $gS = gT$.*

1. $\implies$ 2.: $H \trianglelefteq G$ *so* $gHg^{-1} = H \ \forall \ g \in G \implies gHg^{-1}g = Hg \implies gH = Hg$

2. $\implies$ 3.: $gH = Hg \ \forall \ g \in G \implies gHg^{-1} = Hgg^{-1} = H \ \forall \ g \in G \implies gHg^{-1} \subseteq H \ \forall \ g \in G$

3. $\implies$ 1.: $gHg^{-1} \subseteq H \ \forall \ g \in G \implies gH \subseteq Hg \implies H \subseteq g^{-1}Hg \implies H \subseteq g'Hg'^{-1} \ \forall \ g \in G \implies gHg^{-1} = H \implies H \trianglelefteq G$.

To prove that $H \trianglelefteq G$, we need only show that $gHg^{-1} \subseteq H \ \forall \ g \in G$.

Example Let G be a group and let $H = \{e\}$. Let $g \in G$ and $h = e$. Then $ghg^{-1} = geg^{-1} = e \in H$. Therefore $\{e\} \trianglelefteq G$. Further, $g\{e\} = g \implies G/\{e\} = \{g\{e\} | g \in G\} = G$.

Let G be a group and let $H = G$. Let $g \in G$ and $h \in H$. Then $ghg^{-1} \in G = H$ so $ghg^{-1} \in H \implies H \trianglelefteq G$ and $G \trianglelefteq G$. In particular $G/G = \{e\}$. For example, let $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. Let $g \in \mathbb{Z}$ and $h \in n\mathbb{Z}$. Consider $g + h + g^{-1} = g + h + (-g) = g + (-g) + h = h \in H = n\mathbb{Z}$. Therefore $n\mathbb{Z} \trianglelefteq \mathbb{Z}$.

Let G be abelian and $H \leq G$. Let $g \in G, h \in H$ and $ghg^{-1} = gg^{-1}h = h \in H$. Therefore $H \trianglelefteq G$. We see that all subgroups of abelian groups are normal.

Lemma 1.22 *Any two cosets of H in G have the same cardinality.*

Proof *Let gH be an arbitrary coset of H in G. We want to show that $|gH| = |H|$. Let $f : H \to gH$ such that $f(h) = gh$. We will want to show that f is a bijection.*

Surjective: *If $gh \in gH$, then $h \in H$ and $f(h) = gh$.*
Injective: *If* $f(h_1) = f(h_2) \implies gh_1 = gh_2 \implies gg^{-1}h_1 = h_2 \implies h_1 = h_2$

Therefore, f is a bijection.

Definition For $H \leq G$, the index of H in G, denoted $[G : H]$ is the number of distinct left cosets of H in G. In other words $[G : H] = |G/H|$.

Example Allow $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. Then $[\mathbb{Z} : n\mathbb{Z}] = |\mathbb{Z}/n\mathbb{Z}| = n$.

Theorem 1.23 ***Lagrange's Theorem***. *Let G be a finite group. Then let $H \leq G$. Then we obtain that $|G| = |H|[G : H]$. In particular, $|H| \big| |G|$ and $|G/H| = \frac{|G|}{|H|}$.*

Proof *Let $\{g_1H, g_2H, \dots, g_rH\}$ be the distinct left cosets of H in G. Then $[G : H] = r$ and $G = \cup_{i=1}^{r} g_iH$. Further $|G| = \sum_{i=1}^{r} |H| = r|H| = [G : H]|H|$.*

A consequence of Lagrange is that if G is a group of prime order p then $G \cong \mathbb{Z}/p\mathbb{Z}$.

Corollary 1.24 *If G is a finite group, then $\forall \ g \in G$, $|g| \big| |G|$ because $|g| = |\langle g \rangle|$.*

Example Suppose that $G = S_3$ and let $H = \{1, (1\ 2\ 3), (1\ 3\ 2)\}$. We wish to know if $N_G(H) = G$. We know that $N_G(H) = \{g \in G | gHg^{-1} = H\}$. We know in particular that $|G| = 3! = 6$ and therefore, $|N_G(H) \in \{1, 2, 3, 6\}$ by Lagrange. Since $|H| = 3$, we have that $3 \big| |N_G(H)| \implies |N_G(H)| \in \{3, 6\}$. Therefore, $N_G(H)$ is either G or H. Consider $(1\ 2)(1\ 2\ 3)(1\ 2)^{-1} = (1\ 3\ 2) \in H$, $(1\ 2)(1\ 3\ 2)(1\ 2)^{-1} = (1\ 2\ 3) \in H$, and $(1\ 2)1(1\ 2)^{-1} = 1 \in H$. Therefore, $(1\ 2) \in N_G(H)$ but $(1\ 2) \notin H$. Therefore, $N_G(H) = G \implies H \trianglelefteq G$.

Theorem 1.25 ***Index-2 Theorem***. *If G is a finite group and $H \leq G$ with $[G : H] = 2$, then $H \trianglelefteq G$.*

We may now consider "products" of groups. Let $H, K \leq G$. Then define $HK = \{hk | h \in H, k \in K\}$. We wish to know when HK is a subgroup. First of all, we require that HK be nonempty and, further, that $h_1k_1 \cdot h_2k_2 = h_3k_3$. This is true for abelian groups clearly.

Proposition 1.26 *Let $H, K \leq G$. Then HK is a group $\iff$ $KH = HK$. Note that this only means that $h_1k_1 = k_2h_2$.*

Proposition 1.27 *Let $H, K \leq G$, then $|HK| = \frac{|H||K|}{|H \cap K|}$*

Proof *$HK = \cup_{h \in H} hK \implies |HK| = |K| \times \{$The number of distinct hK$\}$. We have $h_1K = h_2K \iff h_2^{-1}h_1K = K \iff h_2^{-1}h_1 \in K \cap H \iff h_1(K \cap H) = h_2(K \cap H)$. Therefore $\{\#$ of distinct $hK\} = \{\#$ of distinct $h(H \cap K)\} = |H/(H \cap K)| \implies |HK| = |H/(H \cap K)| = \frac{|H||K|}{|H \cap K|}$.*

Example We have $G = S_3$ and $H = \{e, (1\ 2)\}$ and $K = \{e, (2\ 3)\}$. Then $|HK| = \frac{2 \cdot 2}{1} = 4$. Therefore HK cannot be a subgroup by Lagrange since $|G| = 6$.

Theorem 1.28 ***The Isomorphism Theorems***. *Take $\phi : G \to H$ as being a homomorphism. We have that $ker\phi = \{g \in G | \phi(g) = e_H\} \trianglelefteq G$. Further $ker\phi = \{e_G\} \iff \phi$ is injective. We also have that $\phi(G) \leq H$.*

First Isomorphism Theorem: *Let $\phi : G \to H$ is a homomorphism. Then $\phi(G) \cong G/ker\phi$. In particular, if ϕ is surjective, then $H \cong G/ker\phi$.*

Second Isomorphism Theorem: *If $H, K \leq G$ and $H \leq N_G(K)$ then $HK \leq G$ and $K \trianglelefteq HK$ and $HK/K \cong H/(H \cap K)$. Note that if $n|m$ then $m\mathbb{Z} \subseteq n\mathbb{Z}$. Furthermore, $m\mathbb{Z} \trianglelefteq n\mathbb{Z}$ and $n\mathbb{Z}/m\mathbb{Z} = \frac{m}{n}$. Take as example $G = \mathbb{Z}, H = a\mathbb{Z}, K = b\mathbb{Z}$ for $a, b \in \mathbb{Z}^+$.*

Third Isomorphism Theorem: *If $H, K \trianglelefteq G$ and $H \leq K$ then $K/H \trianglelefteq G/H$ and $(G/H)/(H/K) \cong G/K$. We give as an example $G = \mathbb{Z}, H = m\mathbb{Z}, K = n\mathbb{Z}$ such that $n|m$ with $n, m \in \mathbb{Z}^+$. Then $H \leq K$ and $H, K \trianglelefteq G \implies (\mathbb{Z}/m\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$.*

Example As an example of the First Isomorphism Theorem, let $\phi : G \to H$ be an isomorphism such that $\phi(G) = H, \ker\phi = \{e\}$. Therefore, $H \cong G/\{e\} = G$. Consider next $\mathbb{F}_q$ the finite field with q elements. Then define $\phi : Gl_n(\mathbb{F}_q) \to \mathbb{F}_q$ such that $\phi(A) = \det A$. Then $\text{im}\phi = \mathbb{F} - \{0\}$. We also have that $\ker\phi = \{A \in Gl_n(\mathbb{F}_q) | \det A = 1\} = Sl_n(\mathbb{F}_q) \implies |Gl_n(\mathbb{F}_q)/Sl_n(\mathbb{F}_q) = |\mathbb{F}_q - \{0\}| = q - 1$.

A group is simple if it has no nontrivial normal subgroups. That is, the only normal subgroups are $\{e\}$ and the whole group itself.

Hölder Program: We seek to (1) classify all finite simple groups, and (2) find all ways of building new groups from simple ones.

Theorem 1.29 *If G is abelian and simple, then $G \cong \mathbb{Z}/p\mathbb{Z}$ for a prime p.*

Proof *If G is the identity, then we are done quickly. Suppose instead then that $x \in G$ such that $x \neq e$. Consider then $H = \langle x \rangle \trianglelefteq G$. But $H \neq \{e\} \implies H = G = \langle x \rangle$. Suppose $|x| = \infty$. Then $\langle x^2 \rangle \trianglelefteq G$ and $\{e\}$ is not a proper subset of $\langle x^2 \rangle$ which is not a proper subset of G. This is a contradiction. Thus, $|x| = n < \infty$. But $p|n$ with $n \neq p$. Thus $\langle x^{\frac{n}{p}} \rangle \trianglelefteq G$, which is again a contradiction. Therefore, $|x| = n = p$.*

Theorem 1.30 *If G is simple and of odd order, then $G \cong \mathbb{Z}/p\mathbb{Z} \implies$ all nonabelian simple groups have even order.*

Definition A composition series for a group G is a chain of subgroups $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ such that G_i/G_{i-1} is simple for each $1 \leq i \leq n$. Consider $G = \mathbb{Z}_6$. Then $\{e\} \trianglelefteq \langle x^2 \rangle \trianglelefteq \mathbb{Z}_6$ and $\{e\} \trianglelefteq G\ \forall\ G$ since $\mathbb{Z}_6$ is abelian and also because of the Index-2 Theorem. $\langle x^2 \rangle/\{e\} \cong \mathbb{Z}_3$ and $\mathbb{Z}_6/\langle x^2 \rangle \cong \mathbb{Z}_2$.

Theorem 1.31 ***The Jordan-Hölder Theorem.*** *Every group has a composition series. Further the number of composition factors and their isomorphism types are uniquely determined.*

Example For example, consider another composition series for $\mathbb{Z}_6$: $\{e\} \trianglelefteq \langle x^3 \rangle \trianglelefteq \mathbb{Z}_6$ and $\langle x^3 \rangle / \{e\} \cong \mathbb{Z}_2$ and $\mathbb{Z}_6 / \langle x^3 \rangle \cong \mathbb{Z}_3$. Or, alternatively, for D_8: $\{1\} \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle r \rangle \trianglelefteq D_8$.

Theorem 1.32 ***The Extension Theorem.*** *Given two groups K and Q, find all possible groups G such that $K \trianglelefteq G$ and $G/K \cong Q$.*

Theorem 1.33 *The parity of the number of transpositions in a decomposition of a permutation into a product of transpositions is always the same.*

Definition If the number of transpositions in a decomposition is even, the σ is an even permutation. Otherwise, σ is odd.

Example For example, take (1 2 3 4 5) is an even permutation and (1 2) is an odd permutation. 1 is an even permutation.

Definition The alternating group is the set A_n of even permutations of S_n.

Theorem 1.34 *$A_n \trianglelefteq S_n$ and $[A_n : S_n] = 2$.*

Proof Define $\phi : S_n \to \mathbb{Z}/2\mathbb{Z}$ by $\phi(\sigma) = [0]$ if σ is even, and $\phi(\sigma) = [1]$ if σ is odd.

Homomorphism: $\phi(\text{even} \cdot \text{even}) = [0] = [0] + [0] = \phi(\text{even}) + \phi(\text{even})$. $\phi(\text{even} \cdot \text{odd}) = \phi(\text{odd}) = [1] = [0] + [1] = \phi(\text{even}) + \phi(\text{odd})$. $\phi(\text{odd} \cdot \text{odd}) = \phi(\text{even}) = [0] = [1] + [1] = \phi(\text{odd}) + \phi(\text{odd})$.

Implications: $\ker\phi \trianglelefteq S_n$ and $\ker\phi = \{\sigma \in S_n | \phi(\sigma) = [0]\} = \{\text{even permutations}\}$. Therefore $A_n \trianglelefteq S_n$. By the First Isomorphism Theorem, $S_n/A_n \cong \phi(S_n) = \mathbb{Z}/2\mathbb{Z}$. Therefore, $[S_n : A_n] = 2$.

Definition Let G be a group and A a set. A group action of G on A is a map $G \times A \to A$ such that:

1. $e.a = a \;\forall\; a \in A$
2. $g_1.(g_2.a) = (g_1 g_2).a$

Example Let G be a group and suppose $A = G$. Let G act on A by conjugation. Then $g.a = gag^{-1}$. Then we have that $e.a = eae^{-1} = a \;\forall\; a \in A$ and $g_1.(g_2.a) = g_1 g_2 a g_2^{-1} g_1^{-1} = (g_1 g_2).a$. Consider G a group and let $H \leq G, A = G/H = \{xH | x \in G\}$. Suppose that $g.(xH) = gxH$. Then $e.xH = exH = xH \;\forall\; xH \in A$. Further, $(g_1 g_2).xH = g_1 g_2 xH = g_1.(g_2 xH) = g_1.(g_2.xH)$.

A group action gives rise to a homomorphism $\phi : G \to S_A$. Let S_A be the set of bijections from A to A. We obtain that $S_A \cong S_{|A|}$. Given a group action, let $g \in G$ and define $\phi_g : A \to A$ such that $\phi_g(a) = g.a$.

Proposition 1.35 *Define $\phi : G \to S_A$ such that $\phi(g) = \phi_g$. Then $\phi_g \in S_A$ and ϕ is a homomorphism.*

Proof *Consider $\phi_{g^{-1}}$. Then $\phi_{g^{-1}} \phi_g(a) = g^{-1}.(g.a) = (g^{-1}g).a = e.a = a \;\forall\; a \in A$. Additionally, $\phi_g \phi_{g^{-1}} = a \implies \phi_{g^{-1}}$ is an inverse to ϕ_g. Also consider $\phi_{g_1} \phi_{g_2}(a) = \phi_{g_1}(g_2.a) = g_1.(g_2.a) = (g_1 g_2).a = \phi_{g_1 g_2}(a)$.*

Definition The homomorphism arising from a group action is called the permutation representation of that action. A homomorphism $\psi : G \to S_A$ gives rise to a group action $G \times A \to A$ and we define an action $g.a = \psi_g(a)$. Let G act on itself via left multiplication. Then $g.a = ga \;\forall\; g \in G, a \in A$. Then let $\phi : G \to S_G$ be the associated permutation representation. Therefore, $\phi(g) = \phi_g$ and $\phi_g : A \to A$ such that $\phi_g(a) = ga$. Then $\ker\phi = \{g \in G | \phi(g) = 1_{S_G}\} = \{g \in G | \phi_g(a) = a \;\forall\; a \in A\} = e_G$. Therefore, by the First Isomorphism Theorem, $G/\{e\} \cong \phi(G)$ and $G \cong \phi(G) \leq S_G$.

Theorem 1.36 ***The Cayley's Theorem***. *Every group is isomorphic to a subgroup of the symmetric group. In particular, if* $|G| = n$ *then* $G \cong H \leq S_n$.

Proposition 1.37 *If* $|G| = n, H \leq G, [G : H] = p$ *for* p *the smallest prime dividing* n, *then* $H \trianglelefteq G$.

Definition Let $a \in A$. Then the orbit of a is $\mathcal{O}_a = \{g.a | g \in G\} \subseteq A$. The stabilizer of a is $G_a = \{g.a | g.a = a\} \subseteq G$.

Example Let G be a group which acts on itself via conjugation. Then $\mathcal{O}_a = \{gag^{-1} | g \in G\}$ is called the conjugacy class of a. We have that $G_a = \{g \in G | gag^{-1} = a\} = C_G(a)$ is the centralizer of a in G. If $|\mathcal{O}_a| = 1 \iff gag^{-1} = eae^{-1} = a \iff ga = ag \; \forall \; g \in G \iff a \in Z(G)$. Further, $C_G(a) = G \iff a \in Z(G)$. In an abelian group, each element is its own conjugacy class. The centralizer of each element is the whole group.

Lemma 1.38 $G_a \leq G$ *and* $\mathcal{O}_a$ *such that* $a \in A$ *partition* A.

Theorem 1.39 ***The Orbit-Stabilizer Theorem***. *We have that* $|\mathcal{O}_a| = [G : G_a]$ *so there exists a one-to-one correspondence between cosets in* G/G_a *and elements in the orbit of* a.

Proof *Let* $g : G/G_a \to \mathcal{O}_a$ *such that* $f(gG_a) = g.a$.

Well Defined: $gG_a = hG_a \iff h^{-1}g \in G_a \iff (h^{-1}g).a = a \iff g.a = h.a \iff f(gG_a) = g(hG_a)$. *This also gives injectivity.*
Surjectivity: *This is satisfied.*

Let G act on itself via conjugation. Then G is equal to the disjoint union of the orbits of every element of G. Therefore, $|G| = \sum_{i=1}^{k} |\mathcal{O}_{g_i}| = \sum_{i=1}^{k} [G : G_{g_i}] = \sum_{i=1}^{k} [G : C_G(g_i)]$. Therefore $|\mathcal{O}_{g_i}| = 1 \iff g_i \in Z(G)$. This leads to the Class Equation. If G is finite, let $\{g_1, \ldots, g_r\}$ be the representatives for the distinct conjugacy classes that are not in $Z(G)$. Therefore:

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

Proposition 1.40 *If* $|G| = p^m$ *for a prime* p, *then* $|Z(G)| \neq 1$.

Proof *We know that* $C_G(g_i) \leq G$. *Therefore,* $|C_G(g_i)| \big| |G|$ *since* $|G| = |C_G(g_i)|[G : C_G(g_i)]$. *But* $[G : C_G(g_i)] > 1 \implies p \big| [G : C_G(g_i)]$ *but* $p \big| |G| \implies p \big| |Z(G)|$.

Corollary 1.41 *If* $|G| = p^2$, *then* G *is abelian.*

Proof *We have that* $|Z(G)| \big| p^2$. *Thus,* $|Z(G)| \in \{p, p^2\}$. *If* $|Z(G)| = p^2$, *then* G *is abelian. If* $|Z(G)| = p$, *then* $|G/Z(G)| = p \implies G/Z(G) \cong \mathbb{Z}_p \implies G$ *is abelian.*

Theorem 1.42 ***Cauchy's Theorem***. *If* $|G| = n$ *and* $p | n$ *for a prime* p, *then* $\exists \; x \in G$ *such that* $|x| = p$.

Definition Let p be a prime. A group is called a p-group if it has order p^l for some $l \geq 1$. A subgroup H of a group G such that $|H| = p^l$ is called a p-subgroup. If $|G| = p^k m$ and p does not divide m, then a subgroup H of order p^k is a Sylow p-subgroup.

Theorem 1.43 ***Sylow's Theorem***. *Let* G *be a group of order* $p^k m$ *such that* p *does not divide* m. *Then:*

1. G *has a Sylow* p*-subgroup. In fact,* G *has a subgroup of order* $p^l \; \forall \; 1 \leq l \leq k$.
2. *If* H, K *are Sylow* p*-subgroups of* G, *then they are conjugate such that there exists* g *such that* $gHg^{-1} = K$.
3. *Let* n_p *be the number of Sylow* p*-subgroups. Then* $n_p \equiv 1 (\mod p)$ *and* $n_p | m = |G|/p^k$.

Proof *We prove only the first item. Note that if $H \trianglelefteq G$ then subgroups G/H are of the form A/H for $A \leq G$. We proceed by induction on $|G|$.*

Base Case: *If $|G| = 1$ then there is nothing to prove since no primes are involved.*
Assumption: *Assume that all groups with order less that $|G|$ have a Sylow p-subgroup.*
Induction: *Suppose that $p\big||Z(G)|$, then Cauchy gives that there exists $H \leq Z(G)$ such that $|H| = p$. Then $H \leq Z(G) \trianglelefteq G$ and in fact $H \trianglelefteq G$. Thus, G/H is a group and $|G/H| = \frac{p^k m}{p} = p^{k-1}m$. Then by the induction hypothesis, G/H has a subgroup of order p^{k-1}. Call this P/H and $P \leq G$. Therefore, we have that $|P| = \frac{|P|}{|H|}|H| = p^k$.*
But suppose that p does not divide $|Z(G)|$. Then $|G| = |Z(G)| + \sum_{i=1}^{r}[G : C_G(g_i)]$. Thus, p does not divide $[G : C_G(g_i)]$ for some element g_i. Then $|C_G(g_i)| = p^k l$. Furthermore, $|C_G(g_i)| < |G| \implies C_G(g_i)$ has a Sylow p-subgroup by induction. Thus $C_G(g_i)$ has a subgroup of order p^k. Thus, G has a subgroup of order p^k.

Corollary 1.44 *If G has a Sylow p-subgroup, P, then $P \trianglelefteq G \iff n_p = 1$.*

Proof *If $n_p = 1$, let $g \in G$. Consider $gPg^{-1} \leq G$. Further, $|gPg^{-1}| = |P|$. Therefore $gPg^{-1} = P$ since $n_p = 1$. Therefore $P \trianglelefteq G$. If $P \trianglelefteq G$ then $gPg^{-1} = P \ \forall\ g \in G$. Suppose Q is another Sylow p-subgroup. Then by Sylow, $Q = gPg^{-1} = P$ for some $g \in G$. Therefore $n_p = 1$.*

Example Consider any group of order 56. We will show this group is not simple. We have that $56 = 2^3 \cdot 7$ and $n_2 \equiv 1(\mod 2)$ and $n_2|7 \implies n_2 \in \{1, 7\}$. We also have that $n_7 \equiv 1(\mod 7)$ and $n_7|8 \implies n_7 \in \{1, 8\}$. If $n_7 = 1$, then we have a normal subgroup of the corollary. If $n_7 = 8$ we have eight subgroups of order seven, none of which have nontrivial intersection. Therefore, $8 \cdot 6 = 48$ distinct elements of order seven. Thus, there are only eight possible elements left, which must be the Sylow 2-subgroup. Thus, there is only one Sylow 2-subgroup.

Example A group of order 108 must have a subgroup of order nine or twenty-seven. We have that $|G| = 108 = 2^2 \cdot 3^3$. Let H be a Sylow 3-subgroup and $|H| = 27$. Let G act on G/H via left multiplication. Then $g.xH = gxH$. This gives rise to a homomorphism $\phi : G \to S_{G/H} \cong S_4$. Then $\ker\phi \leq H \implies |\ker\phi| \in \{1, 3, 9, 27\}$. By the First Isomorphism Theorem, $G/\ker\phi \cong \phi(G) \leq S_{G/H}$. Thus, $|G/\ker\phi|\big||S_{G/H}| = 4!$. Thus, $\frac{|G|}{|\ker\phi|} = \frac{108}{|\ker\phi|}\big|24 \implies |\ker\phi| \in \{9, 27\}$.

If H, K are subgroups of G such that:

1. $H \trianglelefteq G, K \trianglelefteq G$
2. $H \cap K = \{e\}$
3. $HK = G$

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

Example Let $|G| = 77 = 7 \cdot 11$ and G is abelian. Then by Sylow $n_7 \equiv 1(\mod 7)$ and $n_7|11 \implies n_7 = 1$. Similarly, $n_{11} = 1$. Let H be the Sylow 7-subgroup and K be the Sylow 11-subgroup. We have that $H \trianglelefteq G, K \trianglelefteq G$ and $H \cap K = \{e\}$ and $|HK| = 77 \implies HK = G$. Therefore $G \cong H \times K \cong \mathbb{Z}_7 \times \mathbb{Z}_{11} \cong \mathbb{Z}_{77}$.

Theorem 1.45 ***The Fundamental Theorem of Finite Abelian Groups***. *Let $|G| = n = p_1^{a_1} \dots p_k^{a_k}$ with G abelian. G has Sylow p_i-subgroups for all i. Thus, G abelian implies that the p_i-subgroups are all normal, so the p_i-subgroups are all unique. Let G_{p_i} be the Sylow p_i-subgroup. We have that $|G_{p_i}| = p_i^{a_i}$ and $G_{p_i} \trianglelefteq G \ \forall\ i$. $G_{p_i} \cap G_{p_j} = \{e\} \ \forall\ i, j$ and then $G = G_{p_1}G_{p_2} \dots G_{p_k}$. If G is abelian, then $G \cong G_{p_1} \times \dots \times G_{p_k}$. Furthermore, for each G_p with $|G_p| = p^a$, we have that:*

1. *$G_p \cong \mathbb{Z}_{p^{b_1}} \times \dots \times \mathbb{Z}_{p^{b_s}}$ where $1 \leq b_1 \leq \dots \leq b_s$ and $\sum_{i=1}^{s} b_i = a$.*
2. *If $G_p \cong \mathbb{Z}_{p^{c_1}} \times \dots \times \mathbb{Z}_{p^{c_s}}$ then $s = t$ and $b_i = c_i \ \forall\ i$.*

Example As an example, find all abelian groups of order p^4 up to isomorphism. If $|G| = p^4$ then $G \cong G_{p^4} \cong \mathbb{Z}_{p^{b_1}} \times \dots \times \mathbb{Z}_{p^{b_s}}$ where the b_i partition four. We wish to find the partitions of four:

1. (4)
2. $(1+1+1+1)$
3. $(1+1+2)$
4. $(1+3)$
5. $(2+2)$

Example Alternatively, find all abelian groups of order $72 = 2^3 \cdot 3^2$. Then $G \cong G_2 \times G_3$. The partitions of three are: $(1+1+1), (1+2), (3)$. And the partitions of two are: $(1+1), (2)$. Then the possibilities for G_2 are:

1. $\mathbb{Z}_2 \times \mathbb{Z}_4$
2. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
3. $\mathbb{Z}_8$

And the possibilities for G_3:

1. $\mathbb{Z}_3 \times \mathbb{Z}_3$
2. $\mathbb{Z}_9$

Therefore, there are six total possibilities for G.

Theorem 1.46 ***The Fundamental Theorem of Invariant Factors****. If G is abelian and finite, then $G \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$ where $n_1|n_2|\ldots|n_r$ and $|G| = n_1 n_2 \ldots n_r$ and the $n_i \geq 2$. Further these representations are unique.*

2 Ring Theory

Definition A ring is a set R with two binary operations $+, \times$ such that:

1. $(R, +)$ is an abelian group.
2. $\times$ is associative.
3. There exists a distributive property: $a \times (b+c) = a \times b + a \times c$ and $(a+b) \times c = a \times c + b \times c$.

We say that R is a commutative ring if $\times$ is commutative. R has identity if $\exists\ 1 \in R$ such that $1 \times a = a \times 1 = a$. We write zero for the additive identity and write 1 for the multiplicative identity if it exists. We have that $-a$ is the additive inverse and a^{-1} is the multiplicative inverse if it exists.

Example We have the rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. We write that R is a c-ring if it is commutative. Then for example we have that $M_n(\mathbb{Z})$ is a non-commutative ring with identity. We also have c-rings $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}[x]$. Further, $2\mathbb{Z}$ is a c-ring without identity. $\mathbb{H} = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ij = -ji = k\}$ is a non-commutative ring with identity.

Proposition 2.1 *Let R be a ring with one. Then there exist the following properties:*

1. $0 \times a = a \times 0 = 0$.
2. $(-a)(b) = (a)(-b) = -(ab)$.
3. $(-a)(-b) = ab$.
4. *1 is unique and* $-a = (-1)(a)$.

Proof *We provide a proof of the first item. Demonstrate the remaining properties as an exercise.*

1. $0 \times a = (0+0) \times a = 0 \times a + 0 \times a \implies 0 = 0 \times a$

Definition Let R be a ring with identity. An element $u \in R$ is a unit if $\exists\ v \in R$ with $uv = vu = 1$. If R is a ring with identity where every non-zero element is a unit, R is a division ring.

Recall that a field F was $(F, +)$ that was an abelian group and further that $(F - \{0\}, \times)$ also abelian. A field is a commutative division ring.

Example In $\mathbb{Z}$ the only units are ± 1. In $\mathbb{Z}/n\mathbb{Z}$ the units are $[a]$ such that $(n, a) = 1$. This group is a division ring only when n is prime. We also have that $\mathbb{H}$ is a division ring.

Let us denote with $R^\times$ the set of units of R. Then $(R^\times, \times)$ is a group.

Example We obtain the results that $\mathbb{Z}^\times = \{\pm 1\}$ and $\mathbb{R}^\times = \mathbb{R} - \{0\}$.

Definition Let R be a ring. An element $a \in R - \{0\}$ is a zero divisor if $\exists\, b \in R - \{0\}$ such that $ab = 0$ or $ba = 0$. A commutative ring with no zero divisors is called an integral domain.

Suppose we have that $ab = ad$. Then we want to conclude that $a = 0$ or $b = d$. We obtain, $ab - ad = 0 = a(b - d)$. In an integral domain, this forces $a = 0$ or $b = d$.

Example We have that $\mathbb{Z}/n\mathbb{Z}$ is an integral domain when n is prime. $\mathbb{Z}$ is an integral domain. $M_n(\mathbb{Z})$ is an integral domain when $n = 1$. Fields are all integral domains by necessity. Lastly, we have that $\mathbb{Z}[x]$ is an integral domain.

Notice that a unit may never be a zero divisor.

Proposition 2.2 *A finite integral domain R is a field.*

Proof *We wish to show that all non-zero elements are units. Let $a \in R$ such that $a \neq 0$. We define $f : R \to R$ such that $f(r) = ar$. Then if we have that $f(r) = f(s)$ and $ar = as \implies a = s$ because we are in an integral domain. Since $|R|$ is finite and $R = R$, we have that f is surjective. There exists $r \in R$ such that $f(r) = 1 \implies ar = ra = 1$ since R is commutative.*

Definition A subring of R is a subgroup of R that is closed under multiplication. To show that S is a subring of R, show that $S \neq \{\varnothing\}$ and show $x - y \in S$ and $x \times y \in S$.

Definition The following is the definition of a polynomial ring. Let R be a commutative ring with identity then define $R[x] = \left\{\sum_{i=0}^n a_i x^i | a_i \in R, n \geq 0\right\}$. We assume that $x^k a = a x^k$ and $x^0 = 1$ so that we may consider $(ax + b)(cx) = acx^2 + bcx$. One may view R as a subring of $R[x]$.

Proposition 2.3 *Let R be an integral domain and let $f(x), g(x) \in R[x] - \{0\}$. Then:*

1. $\deg fg = \deg f + \deg g$.
2. *$R[x]$ is an integral domain.*
3. *The units of R are the units of $R[x]$. That is $R^\times = R[x]^\times$*

Proof *We prove the results as follows:*

1. *Let $f(x) = a_n x^n + \ldots a_1 x + a_0$ such that $a_n \neq 0$ and $g(x) = b_m x^m + \ldots + b_1 x + b_0$ such that $b_m \neq 0$. Then the coefficient of x^{n+m} is $a_n b_m \neq 0$. This gives 1.*
2. *This is immediate from the proof of 1.*
3. *This is a containment argument. We have $R^\times \subseteq R[x]^\times$ clearly because R is a subring of $R[x]$. Then let $f \in R[x]^\times$. There exists g such that $fg = 1 \implies \deg fg = \deg f + \deg g = 1 \implies f = a_0 \implies f \in R^\times$.*

Example We seek to answer the question, "What are the roots of a monic polynomial, $f(x) = x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$"? Then we may wish to know how many rational roots the polynomial possesses in $\mathbb{Q}$? How many roots does $f(x)$ have that are of the form $x + y\sqrt{d}$?

Definition $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}$ is the quadratic field. Then $\{\text{roots of } f(x)\} \cap \mathbb{Q}(\sqrt{d}) = \mathbb{Z}(\sqrt{d})$ as long as $d \equiv \{2, 3\} (\mod 4)$. We have that $\mathbb{Z}(\sqrt{d}) = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$ is the ring of integers.

The following is Pell's Equation: $x^2 + dy^2 = \pm 1 = (x + \sqrt{d}y)(x - \sqrt{d}y)$.

Definition $N : \mathbb{Z}(\sqrt{d}) \to \mathbb{Z}$ such that $N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$. Notice that $N(x + y) = N(x)N(y)$ for $x, y \in \mathbb{Z}(\sqrt{d})$. We have that N is a homomorphism.

Let $u \in \mathbb{Z}(\sqrt{d})^\times \implies \exists\ v \in \mathbb{Z}(\sqrt{d})^\times$ such that $uv = 1$. Then $N(u)N(v) = N(uv) = N(1) = 1 \implies N(u) = \pm 1 \in \mathbb{Z}^\times$. If $u \in \mathbb{Z}(\sqrt{d})$ and $N(u) = 1$, $u = a + b\sqrt{d} \implies u^{-1} = \frac{a-b\sqrt{d}}{a^2-b^2d} = \frac{a-b\sqrt{d}}{N(u)}$.

Therefore, $u \in \mathbb{Z}(\sqrt{d})^\times$. Then $u = a + b\sqrt{d} \in \mathbb{Z}(\sqrt{d})^\times \iff N(u) = a^2 - b^2d = \pm 1 \in \mathbb{Z}(\sqrt{d})$. The solutions to Pell's Equations are x, y such that $x + \sqrt{d}y \in \mathbb{Z}(\sqrt{d})^\times$. We have that $\mathbb{Z}(\sqrt{d})^\times = \{\{\pm 1\}$ when $d < -1, \{\pm 1, \pm i\}$ when $d = -1, \{\pm 1\} \times \mathbb{Z}$ when $d > 1\}$. In particular, suppose $d = 2$, then let $x = 1 + \sqrt{2} \implies N(x) = -1$. Then $\langle x \rangle \subseteq \mathbb{Z}(\sqrt{d})^\times$ since $x \in \mathbb{Z}(\sqrt{d})^\times$. But x is a real number and $x \neq \pm 1$ so all powers of x are distinct.

Definition A map $\phi : R \to S$ is a ring homomorphism if:

1. $\phi(x + y) = \phi(x) + \phi(y)$.
2. $\phi(xy) = \phi(x)\phi(y)$.

Then ϕ is an isomorphism if it is bijective and $\ker\phi = \{r \in R | \phi(r) = 0_s\}$.

Example This is actually a counter-example. We have that $2\mathbb{Z} \cong 3\mathbb{Z}$ as groups, but $2\mathbb{Z} \not\cong 3\mathbb{Z}$ as rings. Indeed, suppose $\phi : 2\mathbb{Z} \to 3\mathbb{Z}$ is an isomorphism such that $\phi(2) = 3k \neq 0$. Then $\phi(4) = \phi(2) + \phi(2) = 6k$ but $\phi(4) = \phi(2)\phi(2) = 9k^2$. This implies that k is not an integer value.

Let I be a subring of R. We wish to know when is R/I a ring? We have that $R/I = \{a + I | a \in R\}$. Then we will require that $(a + I) + (b + I) = (a + b) + I$. This operation is well-defined when $I \trianglelefteq R$, but this is always true since R is an abelian group. Then again we wish to understand when $(a + I) \times (b + I) = ab + I$. Suppose $a + I = c + I$ and $b + I = d + I$. We desire that $ab + I = cd + I$. We know that $a = c + i$ for $i \in I$ and $b = d + j$ for $j \in I$. Then $ab + I = (c + i)(d + i) + I = cd + id + jc + ij + I = cd + id + jc + I$. Then this question is reduced to understanding when $id + cj \in I\ \forall i, j \in I, c, d \in R$.

Definition We say that $I \subseteq R$ is an ideal of R if I is an additive subgroup of R and $xr \in I$ and $rx \in I\ \forall\ r \in R, x \in I$. That is, $RI \subseteq I$ and $IR \subseteq I$.

Example Let $R = \mathbb{Z}$ and $I = n\mathbb{Z}$. Another example is $R = \mathbb{Z}[x]$ and $I = \{f | f(0) = 0\}$.

Proposition 2.4 *If I is an ideal of R then R/I is a ring called the quotient ring.*

Lemma 2.5 *Let $\phi : R \to S$ be a ring homomorphism. Then:*

1. *$\phi(R)$ is a subring of S and $\phi(r_1)\phi(r_2) = \phi(r_1r_2)$.*
2. *$\ker\phi$ is an ideal of R. Let $x \in \ker\phi \implies \phi(x) = 0$. Then for $r \in R$, $\phi(xr) = \phi(x)\phi(r) = 0 = \phi(rx)$.*

Theorem 2.6 ***The First Isomorphism Theorem for Rings***. *If $\phi : R \to S$ is a ring homomorphism, then $R/\ker\phi \cong \phi(R)$.*

Example Show that $\mathbb{Z}[x]/\{f | f(0) = 0\} \cong \mathbb{Z}$. Let $\phi : \mathbb{Z}[x] \to \mathbb{Z}$ such that $\phi(f) = f(0)$. Show that ϕ is a homomorphism and that $\ker\phi = \{f | f(0) = 0\}$ and that $\phi(\mathbb{Z}[x]) = \mathbb{Z}$. We see that $\ker = \{f | f(0) = 0\} = \{xg(x) | g(x) \in \mathbb{Z}[x]\} = (x)$.

For the remaining examples, let R be a ring with one.

Definition Let A be a subset of R. The ideal generated by A is the smallest ideal containing A. $(A) = \cap_{A \subseteq I \subseteq R} I$, where I is an ideal.

Let $RAR = \{\sum r_i a_i s_i | r_i, s_i \in R, a_i \in A\}$. Note that $RAR \subseteq (A)$. But RAR is an ideal of R and $1 \in R \implies 1 \cdot a \cdot 1 \in RAR \implies A \subseteq RAR$.

Definition Let $a \in R$ then (a) is the principal ideal generated by a. Note that $(a) = \{ras | r \in R, s \in R\}$. If R is commutative, then $(a) = \{ra | r \in R\}$.

Example Let $R = \mathbb{Z}$ and $I = n\mathbb{Z} = (n)$.

Proposition 2.7 *Every ideal of $\mathbb{Z}$ is principal.*

Proof *Let I be an ideal of $\mathbb{Z}$ $\implies$ I is a subgroup $\implies$ $I = n\mathbb{Z} = (n)$.*

Proposition 2.8 *Let R be a ring with identity and let $I \subseteq R$ be an ideal. Then:*

1. *$I = R \iff I$ contains a unit.*
2. *If R is commutative, R is a field $\iff$ the only ideals of R are (0) and R.*

Proof *We prove the two results as follows:*

1. *If $I = R \implies 1 \in I$. Let $a \in I \cap R^\times \implies a \in I, a^{-1} \in R \implies a^{-1}a \in I \implies 1 \in I \implies I = R$.*
2. *Suppose R is a field so every nonzero ideal contains one $\implies I = R$. Let $u \in R, u \neq 0$. Then consider $(u) = R \implies 1 \in (u) \implies uv = 1$ for some $v \in R$.*

We wish to know now whether or not every ideal in $\mathbb{Z}[x]$ is principal and similarly for $\mathbb{Q}[x]$. Suppose $R = \mathbb{Z}[x]$ and $I = (5, x) = \{5p(x) + xq(x) | p(x), q(x) \in \mathbb{Z}[x]\} \neq \mathbb{Z}[x]$. Suppose further that I is principal $\implies I = (g(x)) = \{g(x)f(x) | f(x) \in \mathbb{Z}[x]\}$. We know that $5 \in I \implies 5 = f(x)g(x)$ for some $f(x) \in \mathbb{Z}[x] \implies g(x) = a_0, f(x) = b_0$ since $\deg[fg] = 0 \implies a_0 b_0 = 5$. So we have that $a_0 = \pm 1$ or $b_0 = \pm 5$.

If ± 1: This implies $\mathbb{Z}[x]^\times = \mathbb{Z}^\times = \{\pm 1\} \implies a_0 \in \mathbb{Z}[x]^\times \implies I = \mathbb{Z}[x]$, a contradiction.
If ± 5: Then $I = (\pm 5) \implies x = \pm 5 \cdot h(x)$ for $h(x) \in \mathbb{Z}[x]$ where $h(x) = \sum_i c_i x^i$ but $c_1 = 1 \implies c_1 = \pm\frac{1}{5}$ a contradiction.

Therefore, $(5, x)$ is not principal in $\mathbb{Z}[x]$. Suppose instead that $R = \mathbb{Q}[x]$ and $I = (5, x)$. We again have that $5 \in I$ and $\mathbb{Q}[x]^\times = \mathbb{Q}^\times = \mathbb{Q} - \{0\}$ so that I contains a unit $\implies I = R$.

Consider $\mathbb{Q}[x]/(x), \mathbb{Q}[x]/(x^2 - 1), \mathbb{Q}[x]/(x^2 + 1)$. All of these are rings. We have that $\mathbb{Q}[x]/(x) \cong \mathbb{Q}$ where $(x) = \{xg(x) | g(x) \in \mathbb{Q}[x]\} = \{f(x) | f(0) = 0\}$. Suppose $\phi : \mathbb{Q}[x] \to \mathbb{Q}$ and $\ker = (x)$. Clearly ϕ is surjective $\implies \phi(\mathbb{Q}[x]) = \mathbb{Q}$. More generally, $\mathbb{Q}[x]/(x - a) \cong \mathbb{Q}$.

Consider $\mathbb{Q}[x]/(x^2 - 1)$ is not an integral domain. Let $I = (x^2 - 1)$. The additive inverse of $\mathbb{Q}[x]/I$ is I, Consider $(x + 1) + I \neq 0 + I$ and $(x - 1) + I \neq 0 + I$ but $[(x + 1) + I][(x - 1) + I] = (x^2 - 1) + I = I \implies \mathbb{Q}[x]/I$ is not an integral domain.

Consider next $\mathbb{Q}[x]/(x^2 + 1)$ and let $J = (x^2 + 1)$ and take $[p(x) + J][q(x) + J] = 0 + J = J \implies p(x) \in J$ or $q(x) \in J$.

Definition Let R be a commutative ring and let $I \subseteq R$ be an ideal.

1. I is a prime ideal if $I \neq R$ and $\forall\, a, b \in R$ if $ab \in I$ then $a \in I$ or $b \in I$.
2. I is a maximal ideal if $I \neq R$ and for any ideal J with $I \subseteq J \subseteq R$, then either $I = J$ or $J = R$.

Example Let $R = \mathbb{Z}$. Take $I = p\mathbb{Z} = (p)$ for p a prime. Suppose $ab \in p\mathbb{Z}$ then $ab = np$ for $n \in \mathbb{Z}$ so $p|ab \implies p|a$ or $p|b \implies$ either a or b in $p\mathbb{Z}$.

Suppose $p\mathbb{Z} \subseteq J\mathbb{Z}$ for some ideal J. We have that $J = k\mathbb{Z}$. Then $p = kn, n \in \mathbb{Z} \implies k|p \implies k = \pm 1$ or $k = \pm p$. Therefore, $J = \mathbb{Z}$ or $J = p\mathbb{Z}$ respectively.

Theorem 2.9 *We have that (0) is a prime ideal in any integral domain.*

Let $R = \mathbb{Z}[x]$ and let $P = (x)$. Suppose $f(x)g(x) \in (x) = \{\text{polynomials with zero constant term}\}$. Either $f(x)$ or $g(x)$ has zero constant term (because $\mathbb{Z}[x]$ is an integral domain) $\implies f(x)$ or $g(x) \in P \implies P$ is a prime ideal of $\mathbb{Z}[x]$. We then wish to know if P is maximal. But $(x) \subset (5, x) \subset \mathbb{Z}[x] \implies P$ is not maximal.

Proposition 2.10 *Let R be a commutative ring with identity. Then:*

1. *$M \subseteq R$ is a maximal ideal $\iff$ R/M is a field.*
2. *$P \subseteq R$ is a prime ideal $\iff$ R/P is an integral domain.*
3. *All maximal ideals are prime ideals.*

Let R be an integral domain. Then a norm on R is a function $N : R \to \mathbb{Z}^+ \cup \{0\}$ such that $N(0) = 0$. N is a positive norm if $N(a) > 0 \; \forall \; a \neq 0$. An integral domain R is a Euclidean Domain if $\exists$ a norm such that $\forall \; a, b, b \neq 0 \; \exists q, r \in R$ such that $a = bq + r$ with $r = 0$ or $N(r) < N(b)$.

Example Let $R = \mathbb{Z}, N : \mathbb{Z} \to \mathbb{Z}^+ \cup \{0\}$ such that $N(n) = |n|$. Then $\forall \; a, b \in \mathbb{Z} \; \exists \; q, r$ such that $a = bq + r$ and either $r = 0$ or $|r| < |b|$.

Example Suppose R is a field and $a = bq + 0$ such that $q = b^{-1}a$. Suppose $N : R \to \mathbb{Z}^+ \cup \{0\}$ such that $N(a) = 0 \; \forall \; a$.

Example Consider $F[x]$ for F a field. Then consider $N : F[x] \to \mathbb{Z}^+ \cup \{0\}$ such that $N(f) = \deg [f]$.

Theorem 2.11 *$F[x]$ is a Euclidean Domain for F a field. In fact, if $f(x), g(x) \in F[x], g(x) \neq 0$ then $\exists \; q(x), r(x)$ with $f(x) = g(x)q(x) + r(x)$ with $r(x) = 0$ or $\deg [r] < \deg [q]$.*

Proof *If $f(x) = 0$, then let $q(x) = r(x) = 0$. Now suppose that $f(x) \neq 0$ and let $f(x) = a_n x^n + \ldots + a_1 x + a_0$ with $n \geq 0$ and $g(x) = b_m x^m + \ldots + b_1 x + b_0$ with $m \geq 0$.*

$n < m$**:** *Then $f(x) = g(x) \cdot 0 + f(x)$ so $r(x) = f(x)$ and $\deg [r] < \deg [g]$.*
$n \geq m$**:** *Proceed by induction on $\deg [f] = n$.*

Base $n = m$**:** *$f(x) = g(x) \cdot a_n b_m^{-1} + f(x) - g(x) \cdot a_n b_m^{-1}$ and $\deg [r] < \deg [g]$. And assume true for all polynomials of degree less than n.*

Induction: *Consider $h(x) = f(x) - g(x)x^{n-m}a_n b_m^{-1}$ has degree less than $\deg [f]$. We have $h(x) = g(x)q'(x) + r'(x)$ and $r'(x) = 0$ or $\deg [r'] < \deg [g] \implies f(x) = h(x) + g(x)x^{n-m}a_n b_m^{-1} = g(x)q'(x) + r'(x) + g(x)x^{n-m}a_n b_m^{-1} = g(x)\left(q'(x) + x^{n-m}a_n b_m^{-1}\right) + r'(x)$ and $r'(x) = 0$ or $\deg [r'] < \deg [g]$.*

Uniqueness: *If $f(x) = g(x)q_1(x) + r_1(x) = g(x)q_2(x) + r_2(x)$. Then $g(x)\left(q_1(x) - q_2(x)\right) = r_2(x) - r_1(x) \implies \deg [g] + \deg [q_1 - q_2] = \deg [r_2 - r_1]$ because $F[x]$ is an integral domain. Therefore $q_1 - q_2 = 0, r_1 - r_2 = 0 \implies q_1 = q_2, r_1 = r_2$.*

Proposition 2.12 *If F is a field and $f(x) \in F[x]$ and $a \in F$ then $f(a) = 0 \iff f(x) = (x - a)g(x)$ for some $g(x) \in F[x]$.*

Proof *Suppose $f(a) = 0$. Then $f(x) = (x - a)q(x) + r(x)$ with either $r(x) = 0$ or $\deg [r] < \deg [x - a]$ so that $r(x) = c$, where c is a constant. We know that $f(a) = 0$ so $(a - a)g(a) + c = 0 \implies c = 0$. Suppose next that $f(x) = (x - a)g(x) \implies f(a) = (a - a)g(a) = 0$.*

Example Consider $\mathbb{H} = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ij = -ji = k\}$. Then $(x^2 + 1) = (x + i)(x - i) = (x + j)(x - j) = (x + k)(x - k) = f(x)$. Then $f(j) = (j^2 + 1) = 0$ but $(j + i)(j - i) \neq 0$.

Definition If a is a root of f then the multiplicity of a in f is the smallest positive integer m such that $(x - a)^m | f$.

Proposition 2.13 *If $f(x) \in F[x]$ with degree n then $f(x)$ has at most n roots, counting multiplicity.*

Proof *If $f(x) = a_0$ and $a_0 \neq 0$ then f has no roots, so the number of roots is less than or equal to the degree of f which is zero. Suppose that $n \geq 1$ and proceed by induction on n. If f has no roots in F then we are done. Otherwise f has a root $a \in F$.*

Induction Hypothesis: Suppose this is true for all polynomials of degree less than n. Then $f(x) = (x - a)g(x)$ for $g(x) \in F[x]$ and $\deg [g] = n - 1$ so $g(x)$ has at most $n - 1$ roots $\implies f(x)$ has at most n roots because we assume that $f(x)$ has unique factorization.

Example Consider again $\mathbb{H}$ and let $f(x) = x^2 + 1$ can be factored infinitely many ways so proof breaks down in Quarternions.

Definition A principal ideal domain is an integral domain is which every ideal is principal. For example $\mathbb{Z}$ is a principal ideal domain. As a counter-example, $\mathbb{Z}[x]$ has $(x, 5)$ which is not principal.

Proposition 2.14 *A Euclidean Domain is a principal ideal domain.*

Proof *Let R be a Euclidean Domain and let $I \subseteq R$ be an ideal. We want that $I = (a)$. Let $\nu = \{N(a) | a \in I, a \neq 0\} \subseteq \mathbb{Z}^+ \cup \{0\}$. Well-ordering implies ν has a least element d. Let $a \in I$ with $N(a) = d$. We want to show that that $(a) = I$. We have immediately that $(a) \subseteq I$ since $a \in I$. Let $b \in I$ be arbitrary. Then $\exists\ q, r \in R$ with $b = aq + r$ with either $r = 0$ or $N(r) < N(a)$. But $r = b - aq \in I \implies N(r) \neq N(a) \implies r = 0 \implies N(a)$.*

Definition Let R be a commutative ring with one. Let $a, b \in R, b \neq 0$. We say that a is a multiple of b or b divides a if $\exists\ c \in R$ such that $a = bc$.

Example $(x-1)|(x^2-1)$ in $\mathbb{Z}[x]$ since $(x^2-1) = (x-1)(x+1)$, which is also true in $\mathbb{Q}[x]$. But $(2x-2)$ does not divide (x^2-1) in $\mathbb{Z}[x]$, but it does in $\mathbb{Q}[x]$ since $(x^2-1) = (2x-2)(x+1)(\frac{1}{2})$.

Definition Let R be a commutative ring with identity and $a, b \in R, b \neq 0$. A greatest common divisor of a, b is an element $d \in R$ such that $d|a$ and $d|b$ and if $d'|a$ and $d'|b$ then $d'|d$.

Note: $(a, b) = (d) \iff a = dl, b = dk$ and $d = ax + by \iff d|a, d|b$ and if $d'|a$ and $d'|b$ then $d'|d$. Indeed $(a, b) = (d) \iff d$ is a gcd of a, b. In a principal ideal domain, greatest common divisors always exist. Note that the greatest common divisors are not always unique. In $\mathbb{Z}$, $\gcd(a, b) = \pm 3$. In $\mathbb{Q}, \gcd(6, 3) = \mathbb{Q} - \{0\}$.

Proposition 2.15 *Let R be an integral domain and let d, d' be greatest common divisors of a, b. Then $d = d'u$ for $u \in R^\times$.*

Proof *$d|d'$ and $d'|d \implies (d) = (d') \implies d = d'u$ for $u \in R^\times$.*

We have the greatest common divisors exist in Euclidean Domains since these are a subset of principal ideal domains. A Euclidean Domain has a Euclidean Algorithm that domes from its Division Algorithm.

Theorem 2.16 *Let R be a Euclidean Domain and let $a, b \in R$. Consider r_n that comes from the Euclidean Algorithm then:*

1. *r_n is a greatest common divisor of a, b.*
2. *$r_n = ax + by$ for some $x, y \in R$.*

Proof *We saw that $r_n = (a, b) \implies (r_n) \subseteq (a, b) \subseteq (r_n)$ because $r_n|a$ and $r_n|b$. So $(a, b) = (r_n) \implies r_n = ax + by$.*

Example Let $R = \mathbb{Q}[x]$ and $I = (5, x) = \mathbb{Q}[x]$ since $5 \in \mathbb{Q}[x]^\times = \mathbb{Q}^\times = \mathbb{Q} - \{0\}$. We have $\gcd(5, x) = 1$ in $\mathbb{Q}[x]$.

Example Consider $\mathbb{Z}(\sqrt{d}) = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\} \subseteq \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$, so a commutative subring of an integral domain and contains identity $\implies$ an integral domain.

When $d \in \{-1, -2, -3, -7, -11\}$ then $\mathbb{Z}(\sqrt{d})$ is a Euclidean Domain.

Definition Let R be a commutative ring with identity. A nonzero, non-unit $q \in R$ is irreducible in R if $q = ab \implies a$ or b is a unit. A nonzero, non-unit is prime in R if $q|ab \implies q|a$ or $q|b$. Two elements $a, b \in R$ are associates if $a = ub$ for some unit $u \in R$. In $\mathbb{Z}$, $(-7, 7)$ are associates.

Proposition 2.17 *In an integral domain, q is prime $\implies q$ is irreducible.*

Proof *If q is prime, suppose $q = ab \implies q|ab \implies q|a$ or $q|b \implies a = qk, k \in R \implies q = qkb \implies q = 0$ or $kb = 1 \implies kb = 1 = bk$ since q is prime and R is commutative. Thus, b is a unit.*

An irreducible is not always prime. For example $\mathbb{Z}(\sqrt{-5})$ we have that $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ and all of these are irreducible.

Example Suppose $2 = ab$ then $N(2) = 4 = N(a)N(b) \implies N(a) \in \{1, 2, 4\}$. If $N(a) = 1 \implies a$ is a unit. If $N(a) = 4 \implies N(b) = 1$ so b is a unit. $N(a) = 2$ is invalid since $x^2 + y^2(5) = 2$ has no integer solutions. Therefore 2 is irreducible. But two is not prime since $2|6 = (1+\sqrt{-5})(1-\sqrt{-5})$ but two does not divide either $(1 \pm \sqrt{-5})$

Proposition 2.18 *In R a commutative ring with identity, q is prime $\iff (q)$ is a prime ideal.*

Proof *Suppose $ab \in (q) \implies q|ab \implies q|a$ or $q|b \implies a$ or $b \in (q)$. Do the other direction of the proof as an exercise.*

Lemma 2.19 *If R is a principal ideal domain then q is irreducible $\iff (q)$ is maximal.*

Proof *Suppose q is irreducible. Suppose $(q) \subseteq I \subseteq R$. Since we are in a principal ideal domain, $I = (a) \implies q = ak, k \in R \implies a$ is a unit or k is a unit. If a is a unit, $(a) = R$ or if k is a unit, $(a) = (q)$. Do the other direction of the proof as an exercise.*

Proposition 2.20 *If R is a principal ideal domain, then q irreducible $\implies q$ is prime.*

Proof *Assume q is irreducible $\implies (q)$ is maximal $\implies (q)$ is prime $\implies q$ is prime.*

Proposition 2.21 *In a principal ideal domain, prime ideals are maximal.*

Proof *Suppose P is a prime ideal $\implies P = (p)$ for some prime $p \implies p$ is irreducible $\implies (p)$ is maximal.*

Therefore, if R is a principal ideal domain, then q is irreducible $\iff q$ is prime. Then $R[x]$ is a principal ideal domain $\iff R$ is a field and $R[x]/(x) \cong R$.

Proposition 2.22 *Let R be a commutative ring with identity. Then $R[x]$ is a principal ideal domain $\iff R$ is a field.*

Proof *Suppose R is a field $\implies R[x]$ is a Euclidean Domain $\implies$ it is a principal ideal domain. Suppose $R[x]$ is a principal ideal domain $\implies R[x]$ is an integral domain $\implies R \subseteq R[x]$ is an integral domain $\implies (x)$ is a prime ideal but $R[x]$ is a principal ideal domain $\implies (x)$ is a maximal ideal $\implies R[x]/(x) \cong R$ is a field.*

Indeed, in polynomial rings, being a principal ideal domain implied a Euclidean Domain.

Definition R is a unique factorization domain if it is an integral domain such that for each nonzero, non-unit $r \in R$:

1. $r = q_1 q_2 \dots q_k$ such that the q_i are irreducible.
2. This factorization is unique up to associates such that if $r = p_1 p_2 \dots p_l$ for irreducible p_i, then $k = l$ and after possible rearrangements q_i and p_i are associates.

Example Let $R = \mathbb{Z}$. Then $105 = 3 \cdot 5 \cdot 7 = 5 \cdot (-3) \cdot (-7)$.

Example Let $R = \mathbb{Q}$. Then every element is a zero or a unit, so trivially true $\implies$ every field is a unique factorization domain.

Proposition 2.23 *In a unique factorization domain, prime $\iff$ irreducible.*

Proof *Prime implies irreducible in any integral domain. Suppose then that q is irreducible and $q|ab$. If $ab = 0$ then $a = 0$ or $b = 0$, then $q|a$ or $q|b$. If $a \in R^\times$ and $q|ab \implies qk = ab \implies a^{-1}qk = b \implies q|b$. Similarly when $b \in R^\times$ then $q|a$. Suppose then that a, b are nonzero non-units. Then $ab = (q_1 \dots q_k)(q_{k+1} \dots q_l) = qm = q(p_1 \dots p_s)$ where the q_i and p_i are irreducible $\implies q$ and q_i are associates for some $i \implies q_i = qu$ for some $u \in R^\times \implies q|q_i \implies q|a$ or $q|b \implies q$ is prime.*

Proposition 2.24 *Let R be a unique factorization domain. Then any two nonzero $a, b \in R$ have a greatest common divisor.*

Proof *Let $\{q_1, \dots, q_r\}$ be a list of irreducibles dividing a, b up to units. Notice that $a = uq_1^{e_1} \dots q_r^{e_r}, u \in R^\times, e_i \geq 0$. And $b = vq_1^{f_1} \dots q_r^{f_r}, v \in R^\times, f_i \geq 0$. Then let $d = q_1^{m_1} \dots q_r^{m_r}$ where $m_i = \min(e_i, f_i)$. Claim that d is a greatest common divisor of a, b.*

Theorem 2.25 *A principal ideal domain is a unique factorization domain.*

Proof *Let r be a nonzero, non-unit in a principal ideal domain R. If r is irreducible then there is nothing to show. Otherwise $r = r_0 s_0$ such that $r_0, s_0 R^\times$. If r_0, s_0 are irreducible, then we are done. Otherwise, without loss of generality, suppose r_0 is reducible. Then $r = r_0 s_0 = r_1 s_1 s_0 = r_2 s_2 s_1 s_0 = \dots$. We have that $(r) \subset (r_0) \subset (r_1) \subset \dots$.*

Let $I = \cup(r_i) = (a)$ since R is a principal ideal domain. Thus $a \in I$ so $a \in (r_j)$ for some $j \implies (a) \subseteq (r_j) \implies (r_j) \subseteq I \subseteq (r_j) \implies I = (r_j)$. Therefore, the chain stops are r_j so the factorization into irreducibles is finite.

Suppose $q_1 \dots q_k = p_1 \dots p_s$ for q_i, p_i irreducibles. R is a principal ideal domain $\implies$ irreducibles are prime. Thus, $q_1|(p_1 \dots p_k) \implies q_1|p_i$ for some $i \implies$ without loss of generality $q_1|p_1 \implies p_1 = q_1 u$ where u is a unit because p_1 is irreducible $\implies q_1 \dots q_k = q_1 u p_2 \dots p_s \implies q_2 \dots q_k = up_2 \dots p_s$. By induction, $k = s$ and q_i, p_i are associates up to rearranging. Therefore, a field $\implies$ a Euclidean Domain $\implies$ a principal ideal domain $\implies$ a unique factorization domain.

If F is a field and $f(x) \in F[x], f \neq 0$. Then f has a root $a \in F \iff (x - a)|f$.

Proposition 2.26 *Let F be a field, $f(x) \in F[x], f \neq 0$ then:*

1. $\deg[f] = 0 \iff f$ *is a unit in* $F[x]$ *since* $F[x]^\times = F^\times$.
2. $\deg[f] = 1 \implies f(x)$ *is irreducible since if* $f(x) = g(x)h(x)$ *then* $\deg[g] + \deg[h] = 1 \implies$ *without loss of generality* $g(x) = a_0$.
3. *If* $\deg[f] \in \{2, 3\}$ *then* f *is irreducible* $\iff f$ *has no roots in* F.

Note: $x^4 + 2x^2 + 1 = (x^2 + 1)(x^2 + 1)$ *is reducible in* $\mathbb{Q}[x]$ *but has no roots in* $\mathbb{Q}$.

Proof *Suppose that f has a root in F. Then $f(x) = (x - a)g(x)$ such that $\deg[g] \geq 1 \implies g(x)$ is not a unit $\implies f$ is reducible. Suppose f is reducible $\implies f(x) = g(x)h(x)$ with $\deg[g], \deg[h] \geq$ $\deg[g] + \deg[h] \in \{2, 3\}$. Without loss of generality, say that $\deg[g] = 1 \implies g(x) = ax + b \implies$ a root is $-ba^{-1}$.*

If a polynomial is irreducible in $\mathbb{Q}[x]$, is it also irreducible in $\mathbb{Z}[x]$? No. For example, $6x$ is irreducible in $\mathbb{Q}[x]$, but $6x = 6 \cdot x$ in $\mathbb{Z}[x]$. If $f(x)$ is irreducible in $\mathbb{Q}[x]$ is it reducible in $\mathbb{Z}[x]$? Yes. For example $f(x) = 8x^2 - 2x - 21$ has possible root $\frac{-3}{2}$ so $f(x) = \left(x + \frac{3}{2}\right)(8x - 14) = (2x + 3)(4x - 7)$, which is reducible in $\mathbb{Z}[x]$.

Lemma 2.27 ***Gauss' Lemma***. *If $f(x) \in \mathbb{Z}[x]$ is reducible in $\mathbb{Q}[x]$ then it is reducible in $\mathbb{Z}[x]$. Moreover, if $f(x) = g'(x)h'(x)$ for $g', h' \in \mathbb{Q}[x]$ then $\exists\ r, s \in \mathbb{Q}^\times$ with $g(x) = rg'(x) \in \mathbb{Z}[x]$ and $h(x) = sh'(x) \in \mathbb{Z}[x]$ and $f(x) = g(x)h(x)$.*

Lemma 2.28 *If R is a ring and $I \subseteq R$ is an ideal, then let (I) denote the ideal generated by I in $R[x]$. Then $(I) = I[x]$ which polynomials with coefficients in I. Then $R[x]/I \cong (R/I)[x]$. That is, $R[x]/I[x] \cong (R/I)[x]$. In particular, if I is a prime ideal of R then (I) is a prime ideal of $R[x]$.*

Proof *We need a homomorphism* $\phi : R[x] \to (R/I)[x]$*. Let* $\phi\left(\sum a_i x^i\right) = \sum (a_i + I)x^i$*. Then* $\ker = \left\{\sum a_i x^i | a_i \in I\right\} = I[x] = (I)$*. This is clearly surjective. Then if* I *is a prime ideal of* R*, then* R/I *is an integral domain so* $(R/I)[x]$ *is an integral domain. Therefore* $R[x]/I$ *is an integral domain so that* (I) *is prime.*

Example Consider $\mathbb{Z}[x]/(n) \cong (\mathbb{Z}/n\mathbb{Z})[x]$ and in particular $\mathbb{Z}[x]/p\mathbb{Z}[x] \cong (\mathbb{Z}/p\mathbb{Z})[x]$. We have that $p\mathbb{Z}$ is maximal in $\mathbb{Z}$ but $\mathbb{Z}/p\mathbb{Z}$ is not a field so $p\mathbb{Z}[x]$ is not maximal in $\mathbb{Z}[x]$.

Proof of Gauss' Lemma. Suppose $f(x) = g'(x)h'(x)$ with $g', h' \in \mathbb{Q}[x]$. Let d be the least common multiple of the denominators of $g'(x)$ and $h'(x)$ and their products. So $df(x) = g(x)h(x)$ with $h(x), g(x) \in \mathbb{Z}[x]$. If $d = \pm 1$ then we are done. Also note that $d \neq 0$. Then $d = q_1^{e_1} \dots q_k^{e_k}$. Further $\mathbb{Z}$ is a principal ideal domain so that the q_i are prime. Reduct $df(x) = g(x)h(x)$ mod $q_i \implies 0 = \bar{g}(x)\bar{h}(x) \implies$ without loss of generality $\bar{g}(x) = 0 \implies$ every coefficient of g is divisible by q. Thus, $q_1^{-1}g(x) \in \mathbb{Z}[x]$. Therefore, $df(x) = q_1^{e_1} \dots q_k^{e_k} f(x) \implies q_1^{e_1 - 1} \dots q_k^{e_k} = g_1^{-1} g(x)h(x) \implies$ by induction there exists $r, s \in \mathbb{Q}[x]^\times = \mathbb{Q}^\times$ such that $f(x) = rg(x)sh(x)$.

Definition Suppose $f(x) = a_0 + a_1 x + \ldots + a_n x^n$. Then f is monic if $a_n = 1$ and further f is primitive if $\gcd(a_1, \ldots, a_n) = 1$.

Example Let $f(x) = 4x^2 + 9x - 33$ is primitive in $\mathbb{Z}[x]$. All monic polynomials are primitive.

Corollary 2.29 *Let* $f(x) \in \mathbb{Z}[x]$ *with* $\deg[f] \geq 1$*. Then* $f(x)$ *is irreducible in* $\mathbb{Z}[x] \iff$ *primitive and irreducible in* $\mathbb{Q}[x]$*.*

Proof *Suppose* $f(x)$ *is not primitive* $\implies$ *reducible by pulling out a constant factor, a contradiction. Suppose* $f(x)$ *is reducible in* $\mathbb{Q}[x] \implies$ *reducible in* $\mathbb{Z}[x]$ *by Gauss. Suppose* $f(x)$ *is primitive and irreducible but reducible in* $\mathbb{Z}[x]$*. Then* $f = gh$ *with* $g, h \in \mathbb{Z}[x]$ *with* g, h *non-constant* $\implies f$ *is reducible in* $\mathbb{Q}[x]$*, a contradiction.*

Example Let $f(x) = x^3 - x - 1$ has no roots and is of degree three $\implies$ irreducible in $\mathbb{Q}[x]$.

Theorem 2.30 ***The Reduction Criterion****. Let* R *be an integral domain,* $f(x) \in R[x]$ *that is monic and non-constant. Let* $I \subset R$ *be an ideal. Let* $\phi : R[x] \to (R/I)[x]$*. If* $\bar{f}$ *cannot be factored into two non-constant polynomials in* $(R/I)[x]$ *then* f *is irreducible in* $R[x]$*.*

Proof *Suppose* $\bar{f}$ *cannot be factored into non-constant polynomials, but that* f *is irreducible in* $R[x]$*. Then* $f = gh$ *and* $g(x) = b_m x^m + \ldots + b_1 x + b_0$ *and* $h(x) = c_r x^r + \ldots + c_1 x + c_0$*. Then* $c_r b_m = b_m c_r = 1 \implies c_r, b_m \in R^\times$*. Consider* $\bar{f} = \bar{gh} = \bar{g}\bar{h}$*. Then* $\bar{g} = (b_m + I)x^m Z + \ldots + (b_0 + I), b_m \neq I$ *because then* $I = R$*. Then* $b_m + I \neq I \implies \deg[\bar{g}] = m > 0$ *and* $\deg\left[\bar{h}\right] = r > 0$*, a contradiction.*

Example Suppose $f(x) = x^3 + 19x^2 + 302$. In $(\mathbb{Z}/3\mathbb{Z})[x]$, $\bar{f} = x^3 + x^2 + \bar{2}, \bar{f}(\bar{0}) = \bar{2}, \bar{f}(\bar{1}) = \bar{1}, \bar{f}(\bar{2}) = \bar{2} \implies$ there are no roots in $\mathbb{Z}/3\mathbb{Z}$ a field and $\deg\left[\bar{f}\right] = 3 \implies \bar{f}$ is irreducible in $(\mathbb{Z}/3\mathbb{Z})[x] \implies f$ is irreducible in $\mathbb{Z}[x]$.

In $\mathbb{Q}[x, y]$, terms are of the form $ax^i y^j$ and $f(x, y) = y^3 + yx^2 - y + x - 1$. Let $I = (x)$ and then consider $R[x]/(x) \cong R \cong \mathbb{Q}[y]$. If $f(0)$ is irreducible in $\mathbb{Q}[y]$, then f is irreducible in $\mathbb{Q}[x, y]$. Since $f(0) = y^3 - y - 1$ is of degree three, we need only check the roots, but there are no roots $\implies$ irreducible in $\mathbb{Q}[y] \implies f$ is irreducible in $\mathbb{Q}[x, y]$.

Theorem 2.31 ***Eisenstein's Criterion****. Let* $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$ *with* $a_n \neq 0$ *and* $n \geq 1$*. If* $q \in \mathbb{Z}$ *is prime in* $\mathbb{Z}$ *such that* $q|a_0, \ldots, q|a_{n-1}$ *and* q *does not divide* a_n *and* q^2 *does not divide* a_0*, then* $f(x)$ *is irreducible in* $\mathbb{Q}[x]$*.*

Proof *Suppose* $f(x) = g(x)h(x)$ *where* g, h *are not units. Let* $g(x) = b_m x^m + \ldots + b_1 x + b_0$ *and* $h(x) = c_r x^r + \ldots + c_1 x + c_0$*. Then* $a_0 = b_0 c_0, q|a_0$ *and* q^2 *does not divide* $a_0 \implies q|b_0$ *or* $q|c_0$ *but not both. Without loss of generality, suppose* $q|b_0$ *but that* q *does not divide* c_0*. Then* $a_n = b_m c_r$ *and* q *does not divide* $a_n \implies q$ *does not divide* b_m *nor* c_r*. Let* b_l *be the smallest coefficient such that* q *does not divide* $b_l (0 < l \leq m < n)$*. Then* $a_l = c_l b_0 + c_{l-1} b_1 + \ldots + c_0 b_l$*. Then* $q|a_l, q|b_k \ \forall\ k < l \implies q|c_0 b_l \implies q|c_0$ *or* $q|b_l$ *but both are a contradiction.*