ALGEBRA I

G.H.

Contents

1. Introduction

These notes were taken in University of Delaware's MATH650 (Algebra I) course, taught by Dr. Ivan Todorov in Spring 2021. I typed them based on hand-written notes taken during class each week- the hope was that a typed version would provide a better record in the future and be much more useful. Dr. Todorov's lecture notes were self-contained, though we (i.e. me) took material from:

- Gallian, *Contemporary Abstract Algebra (9th Edition)*
- Dummit & Foote, *Abstract Algebra*
- Isaacs, *Algebra: A Graduate Course*

These notes are a work in progress; all mistakes are mine and mine alone (either through mistyping or a misunderstanding of the material). If you have any error corrections, tips, or general comments, please reach out to me at: ghoefer@udel.edu.

2. Group theory

2.1. **Beginnings, permutations and transpositions, examples of groups.** As a tiny bit of historical background: basics in group theory were initially tied to polynomial equations and their solutions. Working with roots of polynomials, and related questions,

Date: February 2021.

led to the basic formulation of a *group*; originally, the first groups that were studied were permutation groups, although they were not formally defined as such. Much of this work was done by Galois, Abel, and Lagrange. A question that also highly motivated development in this area was:

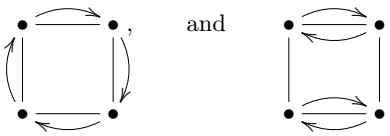
Question: Can you always solve a polynomial equation of degree greater than or equal to 5 in radicals?

It is Galois and his remarkable genius that made a connection between the question above and the "solvability" of a group.

Definition 2.1. *A group G is a nonempty set of elements endowed with a binary operation $\cdot$ such that G contains an identity element e, inverses for each $g \in G$, and is associative with respect to the operation.*

Note: The identity element depends on the operation, and is unique (easy to prove).

Motivation: Symmetries of objects in nature- as an example, look at the symmetries of a square:



In the two pictures above, we either rotate clockwise by some specified angle, or we fix an axis of reflection (as seen in the picture on the right, where our axis of reflection is the vertical line directly through our square). All others for the square can be obtained through some combination of the two.

Note: Inverses in a group are also unique; if we suppose g_1, g_2 are inverses for some element $g \in G$, then

$$g_1 = g_1 e = g_1(gg_2) = (g_1 g)g_2 = eg_2 = g_2,$$

using associativity of the group.

Notation: For $x \in G$, where G is a group, we say $x^n = \underbrace{x \cdots x}_{n \text{ times}}$, for $n \geq 1$. We set $x^0 = e$, and $x^{-n} = (x^n)^{-1}$, for all $n \in \mathbb{N}$.

Note: If $x_1, \ldots, x_k \in G$ then $(x_1 \cdots x_k)^{-1} = x_k^{-1} \cdots x_1^{-1}$ (Socks and Shoes property). This relies on extending associativity by induction.

Proposition 2.2. *(Cancellation) Let G be a group, and $x, y, z \in G$. Then*

(i) $xy = xz \Rightarrow y = z$
(ii) $yx = zx \Rightarrow y = z$

Proof. If $xy = xz$, then

$$x^{-1}(xy) = x^{-1}(xz) \Rightarrow (x^{-1}x)y = (x^{-1}x)z \Rightarrow ey = ez \Rightarrow y = z.$$

The other proof is almost identical. □

Examples:

(i) $(\mathbb{Z}, +)$
(ii) $(\mathbb{Z}_n, +)$ for $n \geq 2$

Note: For future reference/assignments, make sure to add square braces around numbers when working with $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$.

Definition 2.3. *A group G is abelian if $xy = yx$ for all $x, y \in G$.*

Other group examples:

(i) $GL_n(\mathbb{R})$: set of all invertible matrices in $M_n(\mathbb{R})$- the operation is matrix multiplication with identity element I_n. ($GL_n(\mathbb{R})$ has a lot more structure, incidentally, outside of being a group e.g. convergence of elements, etc)
(ii) The symmetric group S_n, where $n \in \mathbb{N}$. Consider the set $[n] = \{1, \ldots, n\}$; a permutation on $[n]$ is a bijection

$$\pi : [n] \to [n]$$

The operation in this group is function composition, and the identity is the identity map. There are two types of permutations:

- Transposition- $\pi \in S_n$ moves only 2 elements, fixes all others. The notation for this is (i, j) when $i \neq j$.
- Cycle- choose $i_1, \ldots, i_k$ distinct. A cycle moves

$$i_i \to i_2 \to \cdots \to i_k \to i_1.$$

The notation for this is $(i_1, \ldots, i_k)$ where k is the length of the cycle.

Definition 2.4. *The support of $\pi \in S_n$ is defined as*

$$supp(\pi) = \{i \in [n] : \pi(i) \neq i\}$$

Note: *$supp(\pi)$ is the complement of the fixed point set of π, where $\pi \in S_n$.*

Note: $|S_n| = n!$.

Definition 2.5. *For a group G, the order of the group is defined as*

$$|G| = \begin{cases} \text{the number of elements in } G \text{ if } G \text{ is finite.} \\ \infty, \text{ if } G \text{ is infinite.} \end{cases}$$

Note: If $\pi, \rho \in S_n$ where $n \geq 3$ then $\pi\rho \neq \rho\pi$ in general; however, if $\text{supp}(\pi) \cap \text{supp}(\rho) = \emptyset$, then the two commute.

Theorem 2.6. *Every permutation is the product of disjoint cycles. Furthermore, every cycle is the product of transpositions.*

Proof. (Sketch) We'll induct on $|\text{supp}(\pi)|$ for $\pi \in S_n$. Pick any $i \in \text{supp}(\pi)$; take $i, \pi(i), \pi^2(i), \ldots$. Pick the smallest k, ℓ with $k < \ell$ such that $\pi^k(i) = \pi^\ell(i)$. If $k \geq 1$, apply π^{-1} to both sides to get $\pi^{k-1}(i) = \pi^{\ell-1}(i)$. This would contradict the minimality of k, ℓ- so $k = 0$. This means we have a cycle $i, \pi(i), \ldots, \pi^{\ell-1}(i)$. Let σ be the cycle

$$i \to \pi(i) \to \cdots \to \pi^{\ell-1}(i) \to i$$

Then write $\pi = \rho\sigma$ where

$$\rho(j) = \begin{cases} \pi(j), & \text{if } j \notin \text{supp}(\sigma) \\ j, & \text{if } j \in \text{supp}(\sigma) \end{cases}$$

By induction, factor ρ into disjoint cycles; since σ is a cycle and $\text{supp}(\rho) \cap \text{supp}(\sigma) = \emptyset$, we're done. For the cycle part, note that

$$(i_1, \ldots, i_k) = (i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k).$$

□

Note: Applying the previous theorems twice, we immediately have that every permutation is the product of transpositions.

Fact: The parity of the number of transpositions τ_k where

$$\pi = \tau_1 \tau_2 \cdots \tau_m$$

does not depend on the decomposition.

Definition 2.7. *For any $\pi \in S_n$, we define the sign of π as*

$$sgn(\pi) = \begin{cases} 1, & m \text{ even} \\ -1, & m \text{ odd} \end{cases}$$

Definition 2.8. *(Alternating group) The alternating group A_n is the group of permutations π on $[n]$ where $sgn(\pi) = 1$. (i.e., the group of even permutations)*

More examples:

(i) The dihedral group D_n where $n \in \mathbb{N}$; has elements

$$D_n = \{e, r, r^2, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$$

and relations $r^n = e$, $s^2 = e$, $rs = sr^{n-1}$. We use the fact that $r^k s = sr^{n-k}$ to reduce "words" down to simplified form. We can represent the group in terms of generators and relations (this is a very powerful tool for groups). We can also take a geometric view, seeing it as the group of rotations and reflections of a polygon with n vertices (where we rotate by $\frac{2\pi}{n}$).

(ii) The free group on 2 generators. Let a, b be distinct symbols. We define a^{-1}, b^{-1} as "inverses" of a, b respectively. This gives 4 elements $\{a, b, a^{-1}, b^{-1}\}$. The free group $\mathbb{F}_2$ has elements which are "words" (aka finite strings) on a, a^{-1}, b, b^{-1} together with the empty word ϵ. The group operation is concatenation of strings. The reduced form of a word is when no cancellations can take place.

Note: There are no other relations outside of the basic stipulation that $aa^{-1} = a^{-1}a = \epsilon$- hence the name "free" group, as there are no relations constraining the group.

Note: A relation in a group is an equation involving elements of a group of the form $g_1 \cdots g_k = \epsilon$.

Special case: If we look at $\mathbb{F}_1$, we have exactly one symbol a and its inverse a^{-1}; the group has elements $\{\ldots, a^{-2}, a^{-1}, \epsilon, a, a^2, \ldots\}$. It is clear that a bijection between $\mathbb{F}_1$ and $\mathbb{Z}$ can be made- therefore, $\mathbb{F}_1 \cong \mathbb{Z}$.

Note: If $g \in G$ and $g^m = e$, then $o(g)|m$ (where $o(g)$ denotes the order of the individual element g).

Proof. Let $n = o(g)$. By the Euclidean algorithm, we have $m = nq + r$ with $q \geq 0$ and $0 \leq r \leq n - 1$. We see

$$e = g^m = g^{nq+r} = (g^n)^q \cdot g^r = (e)^q g^r = g^r.$$

If $r > 0$, this contradicts the minimality of n- therefore, $r = 0$. So $m = nq$, meaning $o(g)|m$. □

Definition 2.9. *We say a group G is generated by a subset $S \subseteq G$ if $G = \langle S \rangle := \{s_1 \cdots s_k : s_i \in S \text{ or } s_i^{-1} \in S\}$.*

Note: $\langle S \rangle \subseteq G$ obviously, so if $\langle S \rangle = G$ this means any element in G is a product of elements of S.

Examples:

(i) $\{r, s\}$ generate D_n
(ii) $\{e\}$ generates $\{e\}$
(iii) If G is finite, then G is generated by itself
(iv) $\mathbb{Z}$ generated by $\{1\}$ or $\{-1\}$
(v) $\mathbb{F}_2$ generated by $\{a, b\}$
(vi) S_n generated by transpositions

Definition 2.10. *A group G is called cyclic if there exists $g \in G$ such that $G = \langle g \rangle$.*

2.2. **Subgroups.**

Proposition 2.11. *Let G be a group and $g \in G$. Then $o(g) = |\langle g \rangle|$.*

Proof. If $o(g) = \infty$, then the elements of $\{g^n : n \in \mathbb{Z}\}$ are all distinct. This means $|\langle g \rangle| = \infty$. So assume $o(g) = n < \infty$. As $g^n = e$, then $|\langle g \rangle| \leq n$. For any $m \in \mathbb{Z}$, we have $m = nq + r$ where $0 \leq r \leq n - 1$; then

$$g^m = g^{nq+r} = (g^n)^q \cdot g^r = g^r \in \{e, g, \ldots, g^{n-1}\}.$$

However, $g, g^2, \ldots, g^n$ are mutually distinct: if $g^k = g^\ell$ for $k < \ell$, then $g^{\ell-k} = e$, with $\ell - k < n$ contradicting the minimality of n. Therefore, $n \leq |\langle g \rangle|$. This shows $|\langle g \rangle| = n = o(g)$. □

Definition 2.12. *Let G be a group. A non-empty set $H \subseteq G$ is called a subgroup of G, denoted $H \leq G$ if:*

(i) $x, y \in H \Rightarrow xy \in H$
(ii) $x \in H \Rightarrow x^{-1} \in H$

Examples:

(i) trivial subgroups $\{e\}$ and G itself
(ii) $A_n \leq S_n$
(iii) In any group G, any $g \in G$ with produce $\langle g \rangle \leq G$

Proposition 2.13. *Let $H \subseteq G$, with $H \neq \emptyset$. The following are equivalent:*

(i) $H \leq G$
(ii) $xy^{-1} \in H$ *if* $x, y \in H$

Proof.
(i) $\Rightarrow$ (ii) If $x, y \in H$, $y^{-1} \in H$ by basic axioms of a subgroup. Therefore, $xy^{-1} \in H$.
(ii) $\Rightarrow$ (i) Let $a, a^{-1} \in H$- so $aa^{-1} = e \in H$. If $a \in H$, $ea^{-1} = a^{-1} \in H$. Finally, if $a, b^{-1} \in H$ then $a(b^{-1})^{-1} = ab \in H$. This completes the proof. □

Theorem 2.14 (The Fundamental Theorem of Cyclic Groups)**.** *Every subgroup of a cyclic group is cyclic.*

Proof. Let G be a cyclic group, and $H \leq G$; we want to show that H is cyclic. As G is cyclic, it has a generator- call it $g \in G$. We'll break the proof into cases:

Case 1: The trivial case: if $H = \{e\}$, then $H = \langle e \rangle$; so H is cyclic.

Case 2: If $H \neq \{e\}$, there exists some $k \in \mathbb{Z}$ with $k \neq 0$ such that $g^k \in H$. As H is closed under inverses, we can assume $k > 0$ without loss of generality. Let $n = \min\{k \in \mathbb{N} : g^k \in H\}$. We claim $\langle g^n \rangle = H$. It is clear that as $g^n \in H$, $\langle g^n \rangle \subseteq H$. Take any $h \in H$- let $h = g^m$ for some $m \in \mathbb{Z}$. We set $m = nq + r$ (by the Euclidean algorithm), where $0 \leq r \leq n - 1$. Then

$$g^r = g^m (g^n)^{-q}.$$

As $g^m, (g^n)^{-q} \in H$, then $g^r \in H$ as well. However, as $r < n$, this forces $r = 0$- so $g^m = g^{nq}$, meaning $g^m \in \langle g^n \rangle$. Then as g^m was an arbitrary element of H, this shows $H \subseteq \langle g^n \rangle$, and so $\langle g^n \rangle = H$, and so H is cyclic. □

Definition 2.15. *(External direct product) Let G_1, G_2 be groups. On the set $G_1 \times G_2$ I define a binary operation: $(g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2)$. The neutral element under this operation is (e_1, e_2) where $e_1 \in G_1$ and $e_2 \in G_2$ (naturally). The inverse of an element $(g_1, g_2) \in G_1 \times G_2$ is (g_1^{-1}, g_2^{-1}).*

Note: Direct products give a way to split a complicated group into simpler components.

Notation: If G is a group and $H, K \subseteq G$ then $HK := \{hk : h \in H, k \in K\}$. For example:

(i) $H\{e\} = \{he : h \in H\} = H$
(ii) If $H \leq G$, then $HH = H$

Construction: (Equivalence relations from a subgroup) Let G be a group and $H \leq G$. Define

$$g \sim_r H \text{ if } gh^{-1} \in H, \quad g \sim_\ell h \text{ if } g^{-1}h \in H$$

where $g, h \in G$.

Examples:

(i) Let $H = \{e\}$; if $g \sim_r h$ then $gh^{-1} \in H$, so $gh^{-1} = e$ meaning $g = h$. Same for if $g \sim_\ell h$.
(ii) Let $H = G$. Then $g \sim_r h \iff gh^{-1} \in G$, which is always true as G is a group. Therefore, $g \sim_r h$ for all $g, h \in G$ (so its essentially useless).

The main point of equivalence classes is we want to consider only "coarse" characteristics of objects- it is not important to consider more specific details.

Note: Both $\sim_r, \sim_\ell$ are equivalence relations (easy to check- exercise!!). This means both have corresponding equivalence classes- these are called the right and the left cosets of H in G. The right cosets are precisely the sets of the form Hg, where $g \in G$. The left cosets are the sets of the form gH, with $g \in G$.

Note: Oftentimes, distinct elements in G have the same left coset.

Theorem 2.16 (Lagrange's Theorem)**.** *If G is a finite group and $H \leq G$, then $|H| \mid |G|$.*

Proof. The equivalence relation $\sim_r$ splits G into disjoint equivalence classes of the form Hx, where $x \in G$. So:

$$G = Hx_1 \cup \cdots \cup Hx_k$$

for $x_1, \ldots, x_k \in G$ where our union is disjoint. However, as $|Hx_i| = H$ for $1 \leq i \leq k$, as the map

$$h \mapsto hx_i$$

is a bijection from H to Hx_i for $1 \leq i \leq k$, then

$$|G| = |Hx_1| + \cdots |Hx_k| = \underbrace{|H| + \cdots + |H|}_{k \text{ times}} = k|H|;$$

therefore, $|H| \mid |G|$. □

Definition 2.17. *(Index) The index of a subgroup H of a finite group G is the number of distinct right cosets (i.e. the number of mutually distinct equivalence classes). We denote this as $[G : H]$.*

Note: We see $[G : H] = \frac{|G|}{|H|}$.

Note: Hg is a subgroup if and only if $Hg = H \iff g \in H$.

Corollary 2.18. *If G is a group with $|G|$ prime, then G is cyclic.*

Proof. Let $g \neq e \in G$ be arbitrary. Consider $\langle g \rangle \subseteq G$. As $\langle g \rangle$ is a subgroup, $|\langle g \rangle| \mid |G|$ (by Lagrange's Theorem). As $g \neq e$ and $|G|$ is prime, this implies $|\langle g \rangle| = |G|$. This then implies $\langle g \rangle = G$, and so G is a cyclic group. □

Note: For $g \in G$, $|g| \mid |G|$.

Aim: Start with $H \leq G$. We want to define a group operation between the right cosets of H in G. Our goal is to define this operation naturally, where $(Hx)(Hy) = H(xy)$; however, this typically does not happen.

Proposition 2.19. *Let $H \leq G$. The following are equivalent:*

(i) $(Hg)(Hh) = H(gh)$ *for all* $g, h \in G$
(ii) $g^{-1}Hg \subseteq H$ *for all* $g \in G$
(iii) $gH = Hg$ *for all* $g \in G$

Definition 2.20. *A subgroup $H \leq G$ is normal if $g^{-1}Hg \subseteq H$ for all $g \in G$.*

Notation: If H is normal in G, we denote this by $H \trianglelefteq G$.

Definition 2.21. *Let G be a group and $H \trianglelefteq G$. The quotient group (also called the factor group) G/H is the group with underlying set $\{Hg : g \in G\}$ (i.e. the set of right cosets), the operation $(Hx)(Hy) = H(xy)$ for all $x, y \in G$, and neutral element H.*

Note: The elements of G/H are *subsets* of G.

Claim: The operation on G/H is well-defined.

Proof. Assume $Hx_1 = Hx_2$ and $Hy_1 = Hy_2$; we want to show $H(x_1y_1) = H(x_2y_2)$, i.e. $(x_1y_1)(x_2y_2)^{-1} \in H$. We know that $x_1x_2^{-1} \in H$ and $y_1y_2^{-1} \in H$; this means there exists some $h \in H$ such that $h = y_1y_2^{-1}$. Then

$$(x_1y_1)(x_2y_2)^{-1} = x_1y_1y_2^{-1}x_2^{-1} = x_1hx_2^{-1}.$$

As $H \trianglelefteq G$, there exists some $h' \in H$ such that $hx_2^{-1} = x_2^{-1}h'$. So

$$(x_1y_1)(x_2y_2)^{-1} = x_1hx_2^{-1} = x_1x_2^{-1}h' \in H,$$

as H is a subgroup and therefore closed under the operation. This shows $H(x_1y_1) = H(x_2y_2)$, and so the operation is well defined. □

*Alternatively- we can also look at the quotient group by the following: let

$$\phi : G \to G'$$

be a homomorphism with kernel $H \leq G$. By the First Isomorphism Theorem (soon to be discussed), $G/H \cong \text{im}(\phi)$. So the image of G under ϕ is our quotient group.

Example: Let $\phi : \mathbb{Z} \to \mathbb{Z}_n$; the kernel of ϕ are the elements in $\mathbb{Z}$ which map to 0- so $\ker(\phi) = n\mathbb{Z}$. Then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Note: The property of being normal is an embedding property, i.e. it depends on the relation of N to G, not the internal structure of N itself (as a subgroup).

Note: The study of homomorphisms between groups is equivalent to the study of quotient groups (by the comments above)

Examples:

(i) If G is abelian, then $H \leq G$ is normal for any subgroup of G
(ii) If $[G : H] = 2$, then $H \trianglelefteq G$ (see Proof Set 2 for explanation)
(iii) $\langle r \rangle \trianglelefteq D_n$, as $[D_n : \langle r \rangle] = 2$
(iv) $\{e, s\} \leq D_n$ is *not* normal

Definition 2.22. *(Internal direct product) Let G be a group, and let $H \trianglelefteq G, K \trianglelefteq G$. We call G the internal direct product of H and K if:*

(i) $H \cap K = \{e\}$
(ii) $G = HK = \{hk : h \in H, k \in K\}$

Note: The external and internal direct products are "the same" (i.e. isomorphic)

Proposition 2.23. *Suppose G is the internal direct product of H and K. Then:*

(i) for all $g \in G$, there exists a unique $h \in H, k \in K$ with $g = hk$
(ii) If $h \in H$ and $k \in K$, then $hk = kh$ (i.e. elements of H and K commute with each other)

Proof.
(i) Write $g = h_1k_1 = h_2k_2$ (as uniqueness is the only thing we have to prove- existence is guaranteed). Then $h_2^{-1}h_1 = k_2k_1^{-1}$- so $h_2^{-1}h_1 \in H \cap K, k_2k_1^{-1} \in H \cap K$. As $H \cap K = \{e\}$, we see $h_1 = h_2, k_1 = k_2$; this proves uniqueness.

(ii) Let $h \in H, k \in K$. By normality of both groups, we have $hk = kh'$ for some $h' \in H$, with $kh' = h'k'$ for some $k' \in K$. By (i), this forces $h = h', k = k'$- and so $hk = kh$. As h, k were arbitrary elements of H and K, this shows they commute with each other. □

2.3. **Group homomorphisms.**

Definition 2.24. *Let G and H be groups. A map $\phi : G \to H$ is called a homomorphism if $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.*

Note: If $\phi : G \to H$ is a homomorphism then $\phi(e_G) = e_H$, and $\phi(x^{-1}) = \phi(x)^{-1}$.

Definition 2.25. *(Special types of homomorphisms) Let $\phi : G \to H$ be a homomorphism. We say ϕ is a(n):*

- *monomorphism, if ϕ is injective*
- *epimorphism, if ϕ is surjective*
- *isomorphism, if ϕ is bijective*
- *automorphism, if ϕ is an isomorphism and $H = G$*
- *endomorphism, if $H = G$*

Notation: We let $G \cong H$ mean G is isomorphic to H.

Examples:

(i) $(\mathbb{R}_+, \cdot) \cong (\mathbb{R}, +)$ via the log function

(ii) det: $\mathrm{GL}_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$ (only an isomorphism if $n = 1$)

(iii) $D_3 \cong S_3$ (exercise! use generators)

(iv) $HK \cong H \times K$ and $G_1 \times G_2 \cong G_2 \times G_1$ (here $G = HK$ is an internal direct product) I consider the map

$$\phi : H \times K \to G, \quad \phi((h, k)) = hk.$$

We see

$$\phi((h_1, k_1)(h_2, k_2)) = \phi((h_1h_2, k_1k_2)) = (h_1h_2)(k_1k_2) = (h_1k_1)(h_2k_2) = \phi((h_1, k_1)\phi((h_2, k_2))$$

by normality. It is easy to check for injectivity, therefore showing the two are isomorphic.

Note: $\phi : G_1 \times G_2 \to G_2 \times G_1$ where $\phi((g_1, g_2)) = (g_2, g_1)$ is the isomorphism between the two.

(v) Cyclic groups are isomorphic to one of $\mathbb{Z}$ or $\mathbb{Z}_n$ for $n \in \mathbb{N}$

(vi) If $\gcd(n, m) = 1$, then $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{mn}$

(vii) Inner automorphisms: for $a \in G$, let $\phi_a : G \to G$ where $\phi_a(x) = axa^{-1}$. Then ϕ_a is an automorphism of G (as ϕ_a is clearly a homomorphism, and to show injectivity we see if

$$axa^{-1} = aya^{-1} \Rightarrow ax = ay \Rightarrow x = y.$$

It is surjective, as $y = a(a^{-1}ya)a^{-1}$ for any $y \in G$).

Definition 2.26. *Let G be a group. The automorphism group $\mathrm{Aut}(G)$ has underlying set $\{\phi : G \to G; \phi$ is an automorphism$\}$, where the operation is composition, the neutral element is the identity map, and where each map is guaranteed to have an inverse as all automorphisms are bijective.*

Notation: $\mathrm{Inn}(G) = \{\phi_a : a \in G\}$. Here ϕ_a : the inner automorphism of G by a, as seen above.

Proposition 2.27. $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Proof. First, note that $id = \phi_e$, so $\mathrm{Inn}(G) \neq \emptyset$. If we let $\phi_a, \phi_b \in \mathrm{Inn}(G)$, then $\phi_a \circ \phi_b = abxb^{-1}a^{-1} = \phi_{ab}$- so $\phi_{ab} \in \mathrm{Inn}(G)$, as $ab \in G$. It is similarly easy to show that inverses exist for each element in $\mathrm{Inn}(G)$, and so $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$.

To prove normality, let $\phi_a \in \mathrm{Inn}(G)$ and $\theta \in \mathrm{Aut}(G)$. We see

$$(\theta \circ \phi_a \circ \theta^{-1})(x) = \theta(\phi_a(\theta^{-1}(x))) = \theta(a\theta^{-1}(x)a^{-1}) = \theta(a)\theta(\theta^{-1}(x))\theta(a)^{-1}$$
$$= \theta(a)x\theta(a)^{-1} = \phi_{\theta(a)} \in \mathrm{Inn}(G).$$

As this holds for all $x \in G$, and ϕ_a, θ were arbitrary, this proves $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. □

Definition 2.28. *Let $\phi : G \to H$ be a homomorphism. We define*

$$\ker(\phi) = \{x \in G : \phi(x) = e_H\} \subseteq G,$$
$$\mathrm{im}(\phi) = \{\phi(x) : x \in G\} \subseteq H$$

Proposition 2.29. *Let $\phi : G \to H$ be a group homomorphism. Then*

(i) $\ker(\phi) \trianglelefteq G$
(ii) $\mathrm{im}(\phi) \leq H$
(iii) *ϕ is injective* $\iff \ker(\phi) = \{e\}$

Proof.
(i) We note as ϕ is a homomorphism, $\phi(e) = e$; so $\ker(\phi) \neq \emptyset$. Let $x, y \in \ker(\phi)$. Then $\phi(x) = \phi(y) = e$. From this, we have $\phi(xy) = \phi(x)\phi(y) = e \cdot e = e$, so $xy \in \ker(\phi)$. Similarly, we see $\phi(x^{-1}) = \phi(x)^{-1} = e^{-1} = e$, so $x^{-1} \in \ker(\phi)$. This shows $\ker(\phi) \leq G$. To show normality, let $g \in G$ and $x \in \ker(\phi)$ be arbitrary. We see

$$\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g)^{-1} = \phi(g)e\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e,$$

so $gxg^{-1} \in \ker(\phi)$. Then $\ker(\phi)$ is closed under conjugation by G (as our elements were arbitrary), so $\ker(\phi) \trianglelefteq G$.

(ii) Exercise!

(iii) If ϕ is injective, then if $\phi(x) = e = \phi(e)$, we have $x = e$. Conversely, if $\ker(\phi) = \{e\}$, suppose $\phi(x) = \phi(y)$ for $x, y \in G$. Then $\phi(x)\phi(y)^{-1} = e$, so $\phi(xy^{-1}) = e$. This means $xy^{-1} \in \ker(\phi)$, and so $x = y$. Therefore, ϕ is injective. □

Theorem 2.30 (First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a group homomorphism. Then*

$$G/\ker(\phi) \cong \mathrm{im}(\phi).$$

Proof. Note- we write $[x]$ for the right coset of x in the group $G/\ker(\phi)$. Define $\psi : G/\ker(\phi) \to \mathrm{im}(\phi)$ by $\psi([x]) = \phi(x)$, for any $x \in G$. We first claim that ψ is well-defined: if $[x] = [y]$, then $xy^{-1} \in \ker(\phi)$. Then $\phi(xy^{-1}) = e \iff \phi(x) = \phi(y)$. This means if $[x] = [y]$, then $\psi([x]) = \psi([y])$, and so ψ is indeed well-defined. We next claim that ψ is a homomorphism; we see

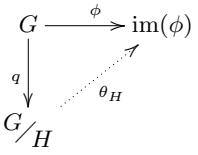
$$\psi([x][y]) = \psi([xy]) = \phi(xy) = \phi(x)\phi(y) = \psi([x])\psi([y]).$$

for arbitrary $x, y \in G$. As $x, y \in G$ were arbitrary elements, this holds for all of G and so ψ is a homomorphism. That ψ is surjective is clear, by definition. Finally, we claim ψ is injective: suppose $\psi([x]) = e$. Then $\phi(x) = e$, so $x \in \ker(\phi)$. As this is true if and only if $[x] = e \in G/\ker(\phi)$, we see ψ is injective. This proves ψ is an isomorphism, which completes the proof. □

Assume: $H \trianglelefteq G, H \leq \ker(\phi)$. Then G/H is well-defined, and let $G/H \to_\theta \text{im}(\phi)$ be defined in almost the same way, but using cosets $xH \in G/H$ instead. This is well-defined, for if $xH = yH, xy^{-1} \in H$; therefore, $xy^{-1} \in \ker(\phi)$, and so $\phi(x) = \phi(y)$.

Note: θ is not injective, unless $H = \ker(\phi)$.

Remark: Generalization- for any $H \leq \ker(\phi), H \trianglelefteq G$, there exists a homomorphism $\theta_H : G/H \to \text{im}(\phi)$ such that the following diagram is commutative:



Remark: If $H \trianglelefteq G$, then $H = \ker(\phi)$ where $\phi : G \to K$ (where K is some other group).

Note: $q : G \to G/H$ is the quotient map.

Theorem 2.31 (Second Isomorphism Theorem)**.** *Let $H \leq G$, and $K \trianglelefteq G$. Then $HK \leq G$, $K \trianglelefteq HK$, $H \cap K \trianglelefteq H$, and*

$$HK/K \cong H/H \cap K.$$

Theorem 2.32 (Third Isomorphism Theorem)**.** *Let $K \leq H \trianglelefteq G$, and $K \trianglelefteq G$. Then $K \trianglelefteq H$, $H/K \trianglelefteq G/K$, and*

$$G/K/H/K \cong G/H.$$

Theorem 2.33 (Cayley's Theorem)**.** *Every group is isomorphic to a subgroup of the symmetric group on a (possibly infinite) set.*

Recall: For any set X, $Sym(X)$ is the set of all bijections $\pi : X \to X$. It is a group under compositions- this is the symmetric group on X.

Proof. Let $\phi : G \to Sym(G)$, where $\phi(g)(x) = gx$, for $x \in G$. Clearly, $\phi(g)$ is a bijection (as if $gx = gy \Rightarrow x = y$ by cancellation, and $z = g(g^{-1}z)$). We also claim ϕ is a homomorphism: we see

$$\phi(g_1g_2)(x) = g_1g_2x = g_1(g_2x) = \phi(g_1)\phi(g_2)(x)$$
$$\Rightarrow \phi(g_1g_2) = \phi(g_1)\phi(g_2).$$

Now, assume $g \in \ker(\phi)$. Then $\phi(g) = id$, so $gx = x$ for all $x \in G$. If $x = e$, then $ge = e$, implying $g = e$. This shows $\ker(\phi) = \{e\}$, and so ϕ is injective. By the First Isomorphism Theorem, we see

$$G = G/\ker(\phi) \cong H = \text{im}(\phi),$$

where $H \leq Sym(G)$. □

Corollary 2.34. *If $|G| = n$, then G is isomorphic to a subgroup of S_n.*

2.4. **Finite abelian groups.**

Theorem 2.35 (Cauchy's Theorem for Finite Abelian Groups)**.** *Let G be a finite abelian group and p be a prime with $p \mid |G|$. Then G has elements of order p.*

Proof. We'll prove it by induction on $|G|$. For the base case, if $|G| = 2$, then clearly G contains an element of order 2 (just pick the non-identity element). Assume the statement holds for all orders less than or equal to $k-1$. Take $|G| = k$, where $k = p^r m$ with p prime and $p \nmid m$. Fix $x \in G$, with $x \neq e$. Let $|x| = q^n \ell$, where q is prime and $q \nmid \ell$. We know $x^{q^{n-1}\ell} = y$ for some $y \in G$, and so $y^q = (x^{q^{n-1}\ell})^q = x^{q^n \ell} = e$. This means there exists a $y \in G$ whose order is prime (specifically, prime q). If $q = p$, then we are done. So suppose not- consider the quotient group $G/\langle y \rangle$. As $\left|G/\langle y \rangle\right| = \frac{|G|}{q} < |G|$, by the inductive hypothesis there exists a $z \in G/\langle y \rangle$ such that $|z| = p$. We know $z = g\langle y \rangle$, where $g \in G$. Since $|z| = p$, we have $(g\langle y \rangle)^p = e_{G/\langle y \rangle} = \langle y \rangle$. Therefore, $g^p \langle y \rangle = \langle y \rangle$, and so $g^p \in \langle y \rangle$. We have two cases:

(i) $g^p = e$- then we are done.
(ii) $g^p = y^i$- then if we take g^q, we have $(g^q)^p = (g^p)^q = (y^i)^q = (y^q)^i = e$, and so $|g^q| = p$.

By induction, this completes the proof. □

Note: In the proof above, we use the fact that in a cyclic group of prime order p, any non-identity element is a generator for the group.

Theorem 2.36 (Fundamental Theorem of Finite Abelian Groups)**.** *Every finite abelian group G is isomorphic to a group of the form*

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

where $p_1, \ldots, p_k$ are primes, $n_1, \ldots, n_k \in \mathbb{N}$ and the list $p_1^{n_1}, \ldots, p_k^{n_k}$ is uniquely determined by G up to a permutation.

Example: Abelian groups of order p^n, where p is prime. Write down $n = n_1 + \cdots + n_k$ where $n_1 \leq \cdots \leq n_k$- this gives direct product decomposition.

Lemma 2.37. *Assume $|G| = p^n m$ where p is prime and $p \nmid m$. Let $H = \{x \in G : x^{p^n} = e\}$ and $K = \{x \in G : x^m = e\}$. Then $G \cong H \times K$ and $|H| = p^n$.*

Example: Take a group of order p^2- there are two abelian groups it might be isomorphic to: either $\mathbb{Z}_p \times \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$, which are non-isomorphic (as one is cyclic, the other is not). If $p \neq q$ is prime, abelian group of order pq is isormorphic to $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$.

Proof. For the proof of the Lemma above, we'll break it into steps.

Step 1: Show $H, K \leq G$- exercise!

Step 2: Show $G = HK$. Take $x \in G$; as $\gcd(p^n, m) = 1$, there exist $t, s \in \mathbb{Z}$ such that $1 = p^n s + mt$. Then

$$x = x^{p^n s + mt} = x^{p^n s} x^{mt} \Rightarrow (x^{sp^n})^m = (x^{p^n m})^s = e^s = e.$$

Similarly,

$$(x^{tm})^{p^n} = (x^{p^n m})^t = e^t = e,$$

and so $x^{p^n s} \in K$, $x^{mt} \in H$. This proves $x = hk$ for some $h \in H$, $k \in K$; as $x \in G$ was arbitrary, this means $G = HK$.

Step 3: Show $H \cap K = \{e\}$. If $x \in H \cap K$, then $|x| \mid p^n$ and $|x| \mid m$. As $\gcd(p^n, m) = 1$, this implies $|x| = 1$, and so $x = e$. As x was arbitrary, this shows $H \cap K = \{e\}$.

The last two steps together imply that as $G = HK$ is an internal direct product, we immediately have $G \cong H \times K$.

Step 4: If $|H| \neq p^k$, let $q \mid |H|$ for some prime q. By Cauchy's Theorem, there exists an $x \in H$ such that $x^q = e$. Therefore, $q \mid p^n$, which contradicts $x \in H$. This means H must have an order of some power of p. We have shown that $G \cong H \times K$, and so $G/H \cong K$. We note that $p \nmid |G/H|$- if it did, there exists a $y \in G/H$ such that $y^p = e$ (again by Cauchy's Theorem). However, as $y \in G/H \cong K$, then $|y| \mid m$- as $p \nmid m$, this is impossible. This guarantees $p \nmid |G/H|$. This implies $|H| = p^n$ (if $|H| \leq p^{n-1}$, then $|G/H| = p\ell$, which leads to the contradiction discussed above), which completes the proof. □

Note: If $G = H \times K$ then H can be seen as a subgroup of G, where $\widetilde{H} := \{(h, e) : h \in H\} \subseteq G$, with $\widetilde{H} \trianglelefteq G$. We can similarly see K as a subgroup of G, which is also normal. Then $G \cong \widetilde{H}\widetilde{K}$. We also have:

- $G/\widetilde{H} \cong \widetilde{K}$;
- $\widetilde{H} \cong H$;
- $\widetilde{K} \cong K$;
- $H \times K/H \cong K$.

Note: By the lemma above, group G splits as a direct product of groups G_i where each G_i has order a prime power.

Lemma 2.38. *Let G be abelian, $|G| = p^n$. Let $a \in G$ be an element of prime order. Then $G \cong \langle a \rangle \times K$ for some group K.*

Proof. If $|a| = p^n$, we are done (as $G = \langle a \rangle$). Assume $|a| = p^m$ with $m < n$. Set $B = \{b \in G : b \notin \langle a \rangle\}$ and choose $b \in B$ of the smallest order. We claim the following:

Claim 1: $|b| = p$;
Claim 2: $\langle a \rangle \cap \langle b \rangle = \{e\}$.

To prove the first claim, we start by noticing

$$(b^p)^{p^{m-1}} = b^{p \cdot p^{m-1}} = b^{p^m} = e.$$

Then $(b^p)^{p^{m-1}} = e$, so $|b^p| \mid p^{m-1}$- therefore, $|b^p| < |b|$. As $b \in B$ is the element of smallest order, we see $b^p \in \langle a \rangle$; if not, there would exist an element in B with order strictly smaller than b, contradicting our choice. This forces $b^p = a^i$ for some $i \in \mathbb{Z}$. Then $(a^i)^{p^{m-1}} = e$, and so a^i is not a generator of $\langle a \rangle$ (as $|a^i| < p^n$). On the other hand, a^k is a generator for $\langle a \rangle$ if and only if $p \nmid k$- this implies $p \mid i$. So there exists some $j \in \mathbb{Z}$ such that $i = pj$. Consider the element $c = ba^{-j}$; we note:

(i) $c \notin \langle a \rangle$; for if $c \in \langle a \rangle$, then $ba^{-j} \in \langle a \rangle$, so $b \in \langle a \rangle$- a direct contradiction.
(ii) $c^p = b^p a^{-jp} = b^p a^{-i} = b^p b^{-p} = e$.

Then by (i) and (ii), as b has minimal order, this implies $|b| = p$.

For the proof of Claim 2, let $g \in \langle a \rangle \cap \langle b \rangle$ by arbitrary but fixed, with $g \neq e$. Then $g = b^k$ for some k with $1 \leq k \leq p-1$. Then $g^\ell = b$ for some $\ell \in \mathbb{Z}$ (as every element in $\langle b \rangle$ is a generator). Then $b \in \langle a \rangle$, directly contradicting our choice of b. This proves $g \in \langle a \rangle \cap \langle b \rangle$ if and only if $g = e$.

Let $\overline{G} := {}^{G}\!/_{\langle b \rangle}$ and write $[g]$ for the corresponding cosets; note that $|\overline{G}| = \frac{|G|}{p} = p^{n-1}$. We make a further claim:

Claim 3: $|[a]| = p^m$, and hence $[a]$ is an element of max order in $\overline{G}$.

To prove this, we first note that $|[a]| = p^k$ for some k- also, $|[a]| \not\leq p^{m-1}$; if we assume it is, then $a^{p^{m-1}} \in \langle b \rangle$; so $a^{p^{m-1}} \in \langle a \rangle \cap \langle b \rangle$, meaning $a^{p^{m-1}} = e$. As $|a| = p^m$ and $p^{m-1} < p^m$, this contradicts our original assumption. This shows $|[a]| \geq p^m$. We also know $|[a]| \leq p^m$, as $[a]^{p^m} = [a^{p^m}] = [e]$. Therefore, $|[a]| = p^m$, so $[a]$ has maximal order in $\overline{G}$. By using induction on n, we can write $\overline{G} = \langle [a] \rangle \times \overline{K}$ for some subgroup $\overline{K} \leq \overline{G}$. Define $K := \{g \in G : [g] \in \overline{K}\}$.

Claim 4: $\langle a \rangle \cap K = \{e\}$.

To prove the previous claim, we let $g \in \langle a \rangle \cap K$. So $[g] \in \overline{K}$ and $[g] \in \langle [a] \rangle$. Then $[g] = [e] = [b]$ (by 2). This means $g \in \langle b \rangle$ and $g \in \langle a \rangle$, forcing $g = e$. Then $\langle a \rangle \cap K = \{e\}$, as g was arbitrary.

Claim 5: $G = \langle a \rangle K$.

To prove the final claim, we first recall that $|G| = p^n$- so $|\overline{G}| = p^{n-1}$. As $|[a]| = p^m$, then $|\langle a \rangle| = p^m$ as well. This means $|K| = p^{n-m-1}$, and so $|K| > |\overline{K}|$ (as we can take the non-trivial quotient)- so $|K| \geq p^{n-m}$ (as $|K|$ must be a power of p). Then $|\langle a \rangle K| \geq |\langle a \rangle||K| = p^m p^{n-m} = p^n$. This shows $G = \langle a \rangle K$, and so $G \cong \langle a \rangle \times K$. □

The Fundamental Theorem of Finite Abelian Groups is proved by induction, where we split G into an external direct product of subgroups G_i all with some prime order. If we assume $|G| = p^n$, we induct on n. By the lemma, $G \cong \mathbb{Z}_{p^m} \times K$; we know $|K| < p^n$, and so by the induction hypothesis it will decompose into an external direct product

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

meaning

$$G \cong \mathbb{Z}_{p^m} \times \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}.$$

For uniqueness, see the textbook (we didn't go over that part of the proof).

2.5. **Group actions, the class equation, Sylow's Theorems.** Question: Given a finite group G, what orders can its subgroup have? If $|G| = p^n m$, where p is prime and p does not divide m, does there exist $H \leq G$ such that $|H| = p^n$?

Answer: Yes!

Definition 2.39. *Let G be a group and Ω be a set. An action of G on Ω is a map $G \times \Omega \to \Omega$ where $(g, w) \mapsto g(w)$ such that*

$$g_1(g_2(w)) = (g_1 g_2)(w),$$
$$e(w) = w$$

for all $w \in \Omega$, and $g_1, g_2 \in G$.

Notation: Sometimes, we write $g \cdot w = g(w)$.

Equivalently, there is a homomorphism from $G \to Sym(\Omega)$.

Definition 2.40. *Given $w \in \Omega$, we say $C_G(w) = \{g \in G : g(w) = w\}$ and $\text{orb}_G(w) = \{g(w) : g \in G\}$.*

Theorem 2.41. *Let G be a finite group acting on a finite set Ω. The following hold:*

(i) $C_G(w) \leq G, w \in \Omega$
(ii) $|\text{orb}_G(w)| = [G : C_G(w)], w \in \Omega$
(iii) The relation $w \sim w'$ if $w' \in \text{orb}_G(w)$ is an equivalence relation
(iv) if $\text{orb}_G(w_1), \ldots, \text{orb}_G(w_k)$ are the distinct orbits of the action, then

$$|\Omega| = \sum_{i=1}^{k} [G : C_G(w_i)]$$

*The previous equation is called the **Class Equation**.*

Proof.
(i) First, we note that by definition $e \in C_G(w)$. If we suppose $g, h \in C_G(w)$, then

$$(gh)(w) = g(h(w)) = g(w) = w,$$

by properties of group actions. Therefore, $gh \in C_G(w)$, and so $C_G(w)$ is closed under the group operation (as g, h were arbitrary). Similarly, if $g \in C_G(w)$, then

$$gw = w \Rightarrow g^{-1}(gw) = g^{-1} \Rightarrow (g^{-1}g)w = g^{-1}w \Rightarrow w = g^{-1}w.$$

Therefore, $g^{-1} \in C_G(w)$, and so $C_G(w)$ is closed under inverses. This proves $C_G(w) \leq G$.

(ii) Consider a map $f : \text{orb}_G(w) \to \{\text{left cosets of } C_G(w)\}$ where $f(gw) = gC_G(w)$. We first want to check if f is a well-defined mapping: let $gw = hw$ for $g, h \in \text{orb}_G(w)$. Then $h^{-1}g = w$, and so $h^{-1}g \in C_G(w)$. Then $gC_G(w) = hC_G(w)$, meaning the map is well-defined. That f is surjective is clear- so we will focus on injectivity. Suppose $gC_G(w) = hC_G(w)$– so $h^{-1}g \in C_G(w)$, meaning $h^{-1}gw = w$. Then $gw = hw$, which implies f must be injective. As this shows f is a bijection between two finite sets, this proves $|\text{orb}_G(w)| = |\{\text{left cosets of } C_G(w)\}|$. However, as $[G : C_G(w)]$ is by definition the number of left cosets of $C_G(w)$ in G, this shows

$$|\text{orb}_G(w)| = [G : C_G(w)].$$

(iii) This one is fairly obvious- just follow the properties of an equivalence relation to establish that $\sim$ satisfies them all.

(iv) We first note that by (iii), Ω splits as a disjoint union of its equivalence classes. Also by (iii), it is clear that these equivalence classes are precisely its orbits- if we pick

distinct representatives $w_1, \ldots, w_k$ from each equivalence class, we know $\Omega = \bigsqcup \operatorname{orb}_G(w_k)$. Then

$$|\Omega| = \sum_{i=1}^{k} |\operatorname{orb}_G(w_i)| = \sum_{i=1}^{k} [G : C_G(w_i)].$$

□

Note: It may be the case that an action has only one orbit: then for any $w \in \Omega, w' \in \Omega$ there exists a $g \in G$ such that $gw = w'$.

Definition 2.42. *Let G be a finite group of order $p^m n$, where p is a prime that does not divide n. A subgroup of G of order p^m is called a Sylow p-subgroup. We use the notation $Syl_p(G)$ for the set of all Sylow p-subgroups in G.*

Theorem 2.43 (Sylow's Theorems)**.** *Let G be a finite group such that $|G| = p^m n$, where p is prime and p does not divide n. The following hold:*

(i) G *has a Sylow p-subgroup*
(ii) If $H, K \in Syl_p(G)$*, then there exists a* $g \in G$ *such that* $g^{-1}Hg = K$
(iii) $|Syl_p(G)| \mid n$
(iv) $|Syl_p(G)| \equiv 1 \mod p$

Proof.
(i) Let $\Omega = \{\text{subseteq of } G \text{ of cardinality } p^m\}$. We see

$$|\Omega| = \binom{p^m n}{p^m} = \frac{p^m n(p^m n - 1) \cdots (p^m n - p^m + 1)}{p^m (p^m - 1) \cdots 2 \cdot 1}.$$

If we cancel factors of p^m in the numerator and denominator, we get

$$n \cdot \frac{p^m n - 1}{p^m n - 1} \frac{p^m n - 2}{p^m - 2} \cdots \frac{p^m n - p^m + 1}{1}.$$

We note that $p^k | i$ if and only if $p^k | p^m n - i$ for $1 \leq k \leq m$. This implies we can cancel out factors of p^k in the previous product equally, leaving us with something that is no longer divisible by p while still being a product of integers. This means p does not divide $|\Omega|$. Let G act on Ω by left multiplication- so if we have set $K = \{g_1, g_2, \ldots, g_{p^m n}\}$, then G acts on Ω with $gK = \{gg_1, \ldots, gg_{p^m n}\}$. By the previous proposition, we know $|\Omega| = \sum_{i=1}^{k} [G : C_G(w_i)]$; as p does not divide the order of Ω, there exists an i such that $p \nmid [G : C_G(w_i)]$. However, $|G| = |C_G(w_i)||G : C_G(w_i)]$, and so $p^m || C_G(w_i)|$; this implies $p^m \leq |C_G(w_i)|$. Fix $h \in W_i$, where $W_i \subseteq \Omega$. The map $C_G(w_i) \to w_i$, where $g \mapsto gh$ is one-to-one, and so $|C_G(w_i)| = |W_i| = p^m$. As $C_G(w_i) \leq G$, then $C_G(w_i)$ must be our Sylow p-subgroup.

(ii) Let $\Omega = \{\text{left cosets of } K\}$. Let H act on Ω by "left multiplication"- i.e., for $h \in H$, we have $gK \mapsto hgK$. Define $\Omega_0 = \{w \in \Omega : |\operatorname{orb}_H(w)| = 1\}$. Note- $\Omega_0 \neq \emptyset$; if $|\operatorname{orb}_H(w)| > 1$ for all w, then $[H : C_H(w)] > 1$. Then $p || \operatorname{orb}_H(w)|$, meaning $p || \Omega|$; as $|\Omega| = [G : K] = n$, and $p \nmid n$, we have a contradiction. So there must exist at least one $w \in \Omega$ such that $|\operatorname{orb}_H(w)| = 1$. This means there exists a $gK \in \Omega_0$, meaning $hgK = gK$ for all $h \in H$. This means $g^{-1}hg \in K$ for all $h \in H$. Therefore, $g^{-1}Hg \subseteq K$- but as $|H| = |K|$, this forces $g^{-1}Hg = K$.

(iii) We want to prove $|Syl_p(G)| \mid n$. Let $\Omega = Syl_p(G)$, and let G act on Ω by conjugation. By (ii), for all $H, K \in \Omega$ there exists a $g \in G$ such that $g^{-1}Hg = K$ (i.e., our action

is transitive). This implies $\text{orb}_G(H) = Syl_p(G)$. We know $|\text{orb}_G(H)| = [G : C_G(H)]$; now, $H \leq C_G(H)$, as $C_G(H) = \{g \in G : gHg^{-1}\}$. Therefore, $|H| = p^m \leq |C_G(H)|$. On the other hand, $p^m n \mid |C_G(H)|[G : C_G(H)]$- so $[G : C_G(H)] \mid n \Rightarrow |\text{orb}_G(H)| \mid n \Rightarrow |Syl_p(G)| \mid n$.

(iv) Let $\Omega = Syl_p(G)$, and fix $P \in Syl_p(G)$; furthermore, let P act on Ω by conjugation: for $Q \in \Omega$, and $g \in P$ we have $Q \mapsto gQg^{-1} \in \Omega$. We want to find the fixed elements- we note that P is clearly fixed under conjugation by itself. Suppose Q is another fixed element under the action, and let $N_G(Q) = \{g \in G : gQg^{-1} = Q\}$. The subgroup $N_G(Q)$ is called the *normalizer* of Q. We note $Q \leq N_G(Q)$ (which is obvious); similarly, $P \leq N_G(Q)$ as Q is a fixed element under P by design. However, both P and Q are Sylow p-subgroups of $N_G(Q)$; as they are maximal subgroups in G, they must be maximal in subgroup $N_G(Q)$ as well. Therefore, by (ii) there exists a $g \in N_G(Q)$ such that $gQg^{-1} = P$. Then as Q is fixed, we see $Q = gQg^{-1} = P$- so if we have a fixed element, it must be *unique*. Now, by the Class Equation we see

$$|\Omega| = \sum_k |\text{orb}_P(w_k)| = 1 + \sum_k \{|\text{orb}_P(w_k)| : |\text{orb}_P(w_k)| > 1\}.$$

However, if $|\text{orb}_P(w)| > 1$, then $p \mid |\text{orb}_P(w)|$. Then p must divide the right term in the sum above, which implies

$$|Syl_p(G)| \equiv 1 \mod p.$$

□

Corollary 2.44. *Let G be a finite group. Then G has a normal Sylow p-subgroup if and only if G has a unique Sylow p-subgroup.*

Proof.
($\Rightarrow$) If $H \leq G$ is a Sylow p-subgroup, then gHg^{-1} is a Sylow p-subgroup for all $g \in G$. If H is normal, and K is a Sylow p-subgroup there exists a $g \in G$ such that $gHg^{-1} = K$ by (ii) of Sylow's Theorems. As $gHg^{-1} \subseteq H$, this forces $H = K$. Therefore, H is unique.

($\Leftarrow$) If H is unique, then $gHg^{-1} = H$ for all $g \in G$. This clearly shows $H \trianglelefteq G$. □

Example: If $|G| = 189$, then there exists a normal subgroup H in G.

Proof. We see $189 = 7 \cdot 3^3$. Let n_7 be the number of Sylow 7-subgroups in G. By Sylow's Theorems, we know $n_7 | 27$ and $n_7 \equiv 1 \mod 7$. This forces $n_7 = 1$, when looking at the divisors of 27. Then $H \leq G$ is the unique Sylow subgroup of order 7 in G, and by the previous corollary this proves $H \trianglelefteq G$. □

In the previous example, what about n_3? By Sylow's Theorems, we have two possibilities- $n_3 = 1$, or $n_3 = 7$- given only this information, we can't say for sure whether or not what Sylow 3-subgroups exist in G.

3. Ring theory

3.1. **Basic definitions and examples.**

Examples:

(i) $(\mathbb{Z}, +, \cdot)$ where $1 \cdots x = x$ for all $x \in \mathbb{Z}$
(ii) $(M_n(\mathbb{R}), +, \cdot)$ where $I \cdot A = A \cdot I = A$ for all $A \in M_n(\mathbb{R})$

Note: In the previous examples, multiplication in (i) was commutative while multiplication in (ii) is not.

Definition 3.1. *A ring is a set R, equipped with operations $+$ and $\cdot$ such that*

(i) $(R,+)$ *is an abelian group with neutral element* 0,
(ii) The operation $\cdot$ *is associative,*
(iii) $a(b+c) = ab+ac$ *and* $(a+b)c = ac+bc$ *for all* $a,b,c \in R$.

R is called unitial if there exists some $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.

Examples:

(i) $(\mathbb{Q},+,\cdot), (\mathbb{R},+,\cdot), (\mathbb{C},+,\cdot)$
(ii) $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$
(iii) $M_n(\mathbb{Z}), M_n(\mathbb{R}), M_n(\mathbb{C})$
More generally, if R is a ring, so is $M_n(R)$ for $n \in \mathbb{N}$. They are called *matrix rings*, and they have operations:

$$(a_{ij}) + (b_{ij}) := (a_{ij} + b_{ij}),$$
$$(a_{ij}) \cdot (b_{ij}) = \left(\sum_{k=1}^{n} a_{ik} b_{kj} \right)_{ij}$$

Definition 3.2. *Let R be a ring. The opposite ring R^{op} has underlying sets R, where addition is the same as in R and multiplication $a * b := ba$. If R is commutative, then $R = R^{op}$.*

Proposition 3.3. *Let R be a ring. Then for all $a,b,c \in R$*

(i) $a \cdot 0 = 0 \cdot a = 0$
(ii) $(-a)b) = -(ab) = a(-b)$
(iii) $(-a)(-b) = ab$
(iv) $(a-b)c = ac - bc, a(b-c) = ab - ac$

Proof. (i) We note $a \cdot 0 + 0 = a \cdot 0$, and so

$$a \cdot 0 + 0 = a \cdot 0 \iff a(0+0) = a \cdot 0 + a \cdot 0 \Rightarrow 0 = a \cdot 0.$$

The others are proven in similar manners- exercise!! □

Cancellation: $a + b = a + c \Rightarrow b = c$, but not always the case with multiplication.

Notation: Let $a \in R$, $n \in \mathbb{N}$. We set

(i) $na = \underbrace{a + \cdots + a}_{n \text{ times}}$
(ii) $a^n = \underbrace{a \cdots a}_{n \text{ times}}$

Definition 3.4. *Let R a unital ring. We say $a \in R$ is a unit (or invertible) if there exists a $b \in R$ such that $ab = ba = 1$. (We note such a b is unique, if one exists, and write it as a^{-1}).*

Notation: $R^* = \{a \in R : a \text{ is a unit }\}$.

Note: R^* is a group with respect to multiplication.

Recall: $M_n(\mathbb{R})^* = \mathrm{GL}_n(\mathbb{R})$.

Important types of rings

(i) R is commutative if $ab = ba$ for all $a, b \in R$
(ii) R is a domain if $ab = 0$ implies $a = 0$ or $b = 0$
(iii) R is a division ring if $R^* = R \setminus \{0\}$
(iv) R is a field if R is a commutative division ring

Examples:

(i) $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ where $[i][j] = [ij]$ for $i, j \in \mathbb{Z}$
(ii) Polynomial rings: let R be a ring $\to R[x]$ is the polynomial ring over R, where $R[x] = \{\sum_{i=0}^{n} a_i x^i : a_i \in R, n \geq 0\}$ (i.e. a polynomial with coefficients in R). Common examples are $\mathbb{Z}[x], \mathbb{R}[x], \mathbb{C}[x]$. It has mechanics:

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i,$$

$$(\sum a_i x^i)(\sum b_i x^i) = \sum_{k} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k$$

where x is our variable. More formally,

$$R[x] = \{(a_0, a_1, \ldots, a_n, 0, 0, \ldots) : a_i \in R, n \geq 0\}.$$

For polynomials in many variables:

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

(iii) Let V be a vector space over some field. Consider $\mathcal{L}(V) = \{f : V \to V : f \text{ is linear }\}$. Addition is defined pointwise (as one expects), and multiplication takes the form of function composition. One example we are already familiar with- if $V = \mathbb{R}^n$ where V is a vector space over $\mathbb{R}$, then $\mathcal{L}(V) \cong M_n(\mathbb{R})$. (We can also consider the same space but endowed with the Schur/Hadamard product- this is when we take the entrywise product of two matrices. Note that it is commutative, compared to regular matrix multiplication.)
Definition: (Algebra) We say a ring which is a vector space endowed with specific natural properties is an *algebra*.

Definition 3.5. *(Product rings) Let R_1, R_2 be rings. We know $R_1 \times R_2 = \{(a, b) : a \in R_1, b \in R_2\}$ is a group with respect to entrywise addition. We also have a zero element $(0, 0)$. If we allow entrywise multiplication as well, this turns into a ring. If both R_1, R_2 have an identity, then $(1_{R_1}, 1_{R_2})$ is the identity for $R_1 \times R_2$. More generally, let I be an index set and let R_i be a ring for each $i \in I$. The product ring is:*

$$R = \prod_{i \in I} R_i$$

where elements are $(a_i)_{i \in I}$ with $a_i \in R_i$. It has mechanics:

$$(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i + b_i)_{i \in I},$$
$$(a_i)_{i \in I}(b_i)_{i \in I} = (a_i b_i)_{i \in I}.$$

Example: Let $R_i = R_0$ for some ring R_0, for all $i \in I$. Then $R = \prod_{i \in I} R_0$. Elements of this R are functions, where

$$a : I \to R_0, \text{ with } a_i = a(i).$$

Operations are as we expect for the product ring.

Construction: For any set I and any ring R_0, consider the set $\mathcal{F}(I, R_0) = \{f : I \to R_0\}$ equipped with pointwise operations.

Examples: Let $[a, b] \subseteq \mathbb{R}$ and $C_{[a,b]}$ be the set of all continuous functions on $[a, b]$. Here we have $I = [a, b], R_0 = \mathbb{R}$, and so $C_{[a,b]} \subseteq \mathcal{F}(I, \mathbb{R})$. By what we know about continuous functions, it is clear that $C_{[a,b]}$ is a ring.

3.2. **Subrings.**

Definition 3.6. *(Subring) Let R be a ring. A nonempty set $S \subseteq R$ is called a subring if*

(i) $x + y \in S$, *for all* $x, y \in S$
(ii) $-x \in S$, *if* $x \in S$
(iii) $xy \in S$, *for all* $xy \in S$

Proposition 3.7. *(Subring criteria) Let $S \subseteq R$ with $S \neq \emptyset$. The following are equivalent:*

(i) S is a subring of R
(ii) If $x, y \in S$ then $x - y$ and $xy \in S$

Examples:

(i) $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$
(ii) Gaussian integers: $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$
(iii) $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{5}i : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}\}$
(iv) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$
(v) $C_{[0,1]}, C_{[a,b]}$
(vi) $T_2 := \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R})$
In general, triangluar matrices:

$$T_n := \{[a_{ij}] \in M_n(\mathbb{R}) : a_{ij} = 0 \text{ if } i > j\} \subseteq M_n(\mathbb{R})$$

Even more generally, we can define it over *any* ring R.
(vii) $\mathbb{H} = \left\{ \begin{bmatrix} z & w \\ \overline{w} & \overline{z} \end{bmatrix} : z, w \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C})$- the quaternions

Definition 3.8. *Let R be a ring. An element $e \in R$ is called idempotent if $e^2 = e$. An element $a \in R$ is called nilpotent if there exists an $n \in \mathbb{N}$ such that $a^n = 0$.*

Proposition 3.9. *Let R be a commutative ring. The set N of all nilpotent elements in R is a subring of R.*

Proof. Take a nilpotent element $a \in R$, where $a^n = 0$ for some $n \in \mathbb{N}$. Similarly, take any $b \in R$. Then

$$(ab)^n = a^n b^n = 0.$$

This shows $ab \in N$ (so if $b \in N$, $ab \in N$). Next, pick $a, b \in N$- without loss of generality assume $a^n = b^n = 0$ for some $n \in \mathbb{N}$. Then

$$(a + b)^{2n} = \sum_{\ell=0}^{2n} \binom{n}{\ell} a^\ell b^{2n-\ell} = 0,$$

as each term in the sum contains at least a power of a^n or b^n. So $a + b \in N$. This proves N is closed under the operations, so N is a subring. □

Definition 3.10. *(Ideals) Let R be a ring. A non-empty subset $I \subseteq R$ is called a left ideal of R if*

(i) If $a, b \in I$ then $a - b \in I$

(ii) If $a \in I$, $r \in R$ then $ra \in I$

Right ideals are defined similarly, with the order of multiplication swapped. The notation we use is

$$I \trianglelefteq_\ell R, \quad I \trianglelefteq_r R$$

for left and right ideals, respectively. We say I is a two-sided ideal, or just an ideal, if it is both a left and a right ideal. This is denoted using $I \trianglelefteq R$.

Remark: If R is commutative then $I \trianglelefteq_\ell R \iff I \trianglelefteq_r R \iff I \trianglelefteq R$.

Examples:

(i) Let $R = C_{[0,1]}$. Let $\Gamma \subseteq [0,1]$, and let
$$I_\Gamma := \{f \in C_{[0,1]} : f(x) = 0, \text{ for all } x \in \Gamma\}$$
Then $I_\Gamma \trianglelefteq C_{[0,1]}$. (In fact, any closed (in $\|\cdot\|_\infty$) ideal of $C_{[0,1]}$ has the form I_Γ for some (closed) set $\Gamma \subseteq [0,1]$- this gives a very easy way to find ideals in $C_{[a,b]}$).

(ii) The set $I = \{(x, 0) : x \in R_1\}$ is called an ideal of $R_1 \times R_2$ (where R_1, R_2 are rings)

(iii) Let $I_1 \trianglelefteq_\ell R_1, I_2 \trianglelefteq_\ell R_2$- then $I_1 \times I_2 \trianglelefteq_\ell R_1 \times R_2$ (same for right and two-sided ideals)

(iv) Let R be a ring and $I \trianglelefteq R$. Then $M_n(I) \trianglelefteq M_n(R)$
Question: Can one describe the ideals of $M_n(R)$ in terms of the ideals in R? I.e., is every ideal $J \trianglelefteq M_n(R)$ of the form $J = M_n(I)$ for some ideal I in R?

(v) Distinction between left, right, and two-sided ideals: in $M_2(\mathbb{Z})$-
$$\begin{bmatrix} \mathbb{Z} & 0 \\ \mathbb{Z} & 0 \end{bmatrix} := \left\{ \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} : x, y \in \mathbb{Z} \right\},$$
$$\begin{bmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & 0 \end{bmatrix} := \left\{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} : x, y \in \mathbb{Z} \right\}.$$
We clearly have $\begin{bmatrix} \mathbb{Z} & 0 \\ \mathbb{Z} & 0 \end{bmatrix} \trianglelefteq_\ell M_2(\mathbb{Z})$, and $\begin{bmatrix} \mathbb{Z} & \mathbb{Z} \\ 0 & 0 \end{bmatrix} \trianglelefteq_r M_2(\mathbb{Z})$, but both of them are not two-sided ideals.

(vi) In $\mathbb{Z} : n\mathbb{Z} \trianglelefteq \mathbb{Z}$ for $n \in \mathbb{N}$

(vii) Ideals vs. subrings:
Recall: In a commutative ring R, the set $N(R)$ of all nilpotent elements is a subring. In fact, $N(R) \trianglelefteq R$.

Definition 3.11. *The center $Z(R)$ of a ring R is the set*
$$Z(R) := \{a \in R : ax = xa \text{ for all } r \in R\}.$$

Note: $Z(R)$ is a subring of R, but not an ideal.

Note: If R is unital and a left ideal I of R contains the identity 1, then $I = R$.

Proof. Let $1 \in I$, and let $r \in R$. Then
$$r = r \cdot 1 \in I,$$
and so $R \subseteq I$. As $I \subseteq R$, we are done. □

Note: A non-zero left ideal $I \trianglelefteq_\ell R$, where R is unital, is equal to $R \iff 1 \in I$.

Examples: (Singly generated ideals) Let R be a ring, and $a \in R$.

(i) $aR = \{ar : r \in R\} \trianglelefteq_r R$
(ii) $Ra = \{ra : r \in R\} \trianglelefteq_\ell R$
(iii) $\langle a \rangle := \{\sum_{i=1}^{n} r_i a q_i : r_i, q_i \in R, n \in \mathbb{N}\} \trianglelefteq R$

(Note aR is closed under addition $\to ax+ay = a(x+y)$ for $x, y \in R$- others hold similarly).

Constructions:

(i) $I_\alpha \trianglelefteq R, \alpha \in A \Rightarrow \cap_{\alpha \in A} I_\alpha \trianglelefteq R$ (i.e. intersection of ideals is an ideal)
(ii) Sums of ideals: if $I, J \trianglelefteq R$ then

$$I + J := \{a + b : a \in I, b \in J\}$$

is an ideal in R

Proof. We note $(a+b)-(a'+b') = (a-a')+(b-b') \in I+J$, where $a, a' \in I$ and $b, b' \in J$. Similarly, for $r \in R, a \in I, b \in J$ we have

$$(a+b)r = \underbrace{ar}_{\in I} + \underbrace{br}_{\in J}$$

as $I, J \trianglelefteq R$. Similarly for left multiplication. □

Definition 3.12. *(Factor rings) Let R be a ring and $I \trianglelefteq R$. Since $(R, +)$ is a commutative group, I is a normal subgroup of $(R, +)$. Consider the factor group ${}^{R}\!/_{I}$, and equip it with a multiplication operation as follows:*

$$(x + I)(y + I) := xy + I, \text{ where } x, y \in R.$$

This is well defined: if we assume $x + I = x' + I, y + I = y' + I$, then

$$x'y' - xy = x'y' - xy' + xy' - xy = \underbrace{(x' - x)y}_{\in I} + \underbrace{x(y' - y)}_{\in I} \in I \trianglelefteq R.$$

So $xy + I = x'y' + I$. It is easy to check the rest of the axioms for a ring are satisfied.

Definition 3.13. *Let ${}^{R}\!/_{I}$ be a factor ring. We define the quotient map*

$$q : R \to {}^{R}\!/_{I}, \quad q(x) = x + I.$$

Note: If R is unital, then so is ${}^{R}\!/_{I}$. If R is commutative, so is ${}^{R}\!/_{I}$.

Note: $q(xy) = q(x)q(y), q(x + y) = q(x) + q(y)$ (this is a reformulation of the definition of the operations).

3.3. **Ring homomorphisms.**

Definition 3.14. *(Ring homomorphism) Let R, S be rings. A homomorphism $\varphi : R \to S$ is a map satisfying:*

(i) $\varphi(a + b) = \varphi(a) + \varphi(b)$
(ii) $\varphi(ab) = \varphi(a)\varphi(b)$

for all $a, b \in R$. If R, S are unital, we call φ unital if $\varphi(1_R) = 1_S$.

Note: If $\varphi : R \to S$ is a homomorphism and e is idempotent, then $\varphi(e)^2 = \varphi(e)$

Definition 3.15. *Let $\varphi : R \to S$ be a homomorphism between rings R and S. The kernel of φ is*

$$\ker(\varphi) = \{r \in R : \varphi(r) = 0\}$$

The image of φ is

$$\mathrm{im}(\varphi) = \{\varphi(r) : r \in R\}$$

Proposition 3.16. *Let $\varphi : R \to S$ be a ring homomorphism. Then*

(i) $\ker(\varphi) \trianglelefteq R$

(ii) $\mathrm{im}(\varphi)$ *is a subring of S*

Proof.
(i) Let $a, b \in \ker(\varphi)$. Then

$$\varphi(a - b) = \varphi(a) - \varphi(b) = 0 - 0 = 0,$$
$$\varphi(ab) = \varphi(a)\varphi(b) = 0 \cdot 0 = 0.$$

So $\ker(\varphi) \trianglelefteq R$.

(ii) Straightforward. □

Note: If $\varphi : R \to S$ is a ring homomorphism then φ is injective if and only if $\ker \varphi = \{0\}$.

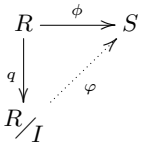
Examples:

(i) $\varphi(a) = -a$ for $a \in R$

(ii) $\phi : M_2(\mathbb{Z}) \to M_2(\mathbb{Z})$, where

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a & -b \\ -c & d \end{bmatrix}$$

Theorem 3.17 (The factor theorem)**.** *Let $\phi : R \to S$ be a ring homomorphism and $I \trianglelefteq R$, with quotient map $q : R \to R/I$. If $I \subseteq \ker \phi$, then there exists a unique homomorphism $\varphi : R/I \to S$ such that $\phi = \varphi \circ q$; in other words, the following diagram commutes:*



Proof. We define $\varphi : R/I \to S$ by letting $\varphi(x + I) = \phi(x)$ for $x \in R$. We note that φ is well-defined: if we assume $x + I = x' + I$, then $x - x' \in I$, so $x - x' \in \ker \phi$. This means $\phi(x - x') = 0$, meaning $\phi(x) - \phi(x') = 0$, and so $\phi(x) = \phi(x')$. By definition, we then have $\phi = \varphi \circ q$- so we just need to prove φ is a homomorphism. We have

$$\varphi((x + I)(y + I)) = \varphi(xy + I) = \phi(xy) = \phi(x)\phi(y) = \varphi(x + I)\varphi(y + I),$$

and

$$\varphi((x + I) + (y + I)) = \varphi((x + y) + I) = \phi(x + y) = \phi(x) + \phi(y)$$
$$= \varphi(x + I) + \varphi(y + I)$$

for any two $x + I, y + I \in R/I$. So φ is a ring homomorphism. To show uniqueness, suppose φ, ψ satisfy

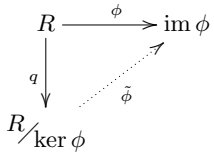
$$\varphi \circ q = \phi = \psi \circ q.$$

Then for each $x \in R$, $\varphi(x+I) = \psi(x+I) = \phi(x)$. It is clear that this forces $\varphi = \psi$, and so our homomorphism is unique. □

Theorem 3.18 (First Isomorphism Theorem)**.** *If $\phi : R \to S$ is a ring homomorphism, then*

$$R/\ker\phi \cong \operatorname{im}\phi.$$

Proof. (Sketch) In the previous theorem, consider $S = \operatorname{im}\phi$ and $I = \ker\phi$; we are allowed to do so, as $\ker\phi$ is always an ideal. From this, we have



where $\tilde{\phi}$ is unique. To finish the proof, we just need to show that $\tilde{\phi}$ is an isomorphism instead of just a ring homomorphism (this is quite easy- essentially follows by definition, the previous theorem, and the Isomorphism Theorems for groups). □

Theorem 3.19 (Second Isomorphism Theorem)**.** *Let R be a ring, $I \trianglelefteq R$ and S be a subring of R. Then*

$$S + I/I \cong S/S \cap I.$$

Note: We'd need to prove $S + I$ is a subring- we have $S \leq R$, $I \trianglelefteq R$, where $S + I = \{x + a : x \in S, a \in I\}$.

Theorem 3.20 (Third Isomorphism Theorem)**.** *Let $I \trianglelefteq R$, $J \trianglelefteq R$, with $J \subseteq I$. Then*

$$R/I/I/J \cong R/J.$$

3.4. **Integral domains and maximal ideals.**

Definition 3.21. *A commutative ring R with an identity (i.e. a unital ring) that is also a domain is called an integral domain.*

Definition 3.22. *A domain is a ring R with no non-trivial zero divisors- i.e., if $x, y \in R$ with $xy = 0$ then either $x = 0$ or $y = 0$.*

Note: From now on, we only consider rings R which are commutative and unital.

Definition 3.23. *Let $a, b \in R$. We say a is a divisor of b if there exists an $x \in R$ such that $b = ax$.*

Notation: If a is a divisor of b, we write $a \mid b$.

Definition 3.24. *An element $p \in R$ is called prime if p is not a unit, $p \neq 0$, and if $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Note: In $R = \mathbb{Z}$, prime elements are prime numbers and their "negatives" (opposites).

Definition 3.25. *If $I \trianglelefteq R$, $J \trianglelefteq R$, define*

$$IJ = \{\sum_{i=1}^{k} a_i b_i : k \in \mathbb{N},\ a_i \in I,\ b_i \in J\}.$$

Note: $IJ \trianglelefteq R$.

Definition 3.26. *An ideal $P \trianglelefteq R$ is called prime if $P \neq R$ and if for $A \trianglelefteq R$, $B \trianglelefteq R$ such that $AB \subseteq P$, then either $A \subseteq P$ or $B \subseteq P$.*

Note: If $A \subseteq P$ (or $B \subseteq P$) then $AB \subseteq P$ automatically, as P is an ideal.

Proposition 3.27. *The following are equivalent for an ideal $P \trianglelefteq R$:*

(i) P is prime;
(ii) If $ab \in P$, then $a \in P$ or $b \in P$ (for all such $a, b \in R$).

Proof.
(i) $\Rightarrow$ (ii) Let $a, b \in R$ with $ab \in P$, and assume P is prime. Then $\langle a\rangle\langle b\rangle \subseteq P$, as

$$\langle a\rangle\langle b\rangle = \{abx : x \in R\}.$$

By primality of P, we know that either $\langle a\rangle \subseteq P$ or $\langle b\rangle \subseteq P$. In either case, we have $a \in P$ or $b \in P$.

(ii) $\Rightarrow$ (i) Assume $A \trianglelefteq R, B \trianglelefteq R$ such that $AB \subseteq P$. Suppose $A \not\subseteq P$, and take $a \in A \setminus P$. Take any $b \in B$; we then have $ab \in AB \subseteq P$. This forces $b \in P$, as P is an ideal in R. As $b \in B$ was arbitrary, this implies $B \subseteq P$, which completes the proof. □

Proposition 3.28. *Let $p \in R$, where $p \neq 0$ or a unit. Then p is prime if and only if $\langle p\rangle$ is prime.*

Proof. Exercise! □

Theorem 3.29. *Let $P \trianglelefteq R$, where P is proper. Then R/P is an integral domain if and only if P is prime.*

Proof.
($\Rightarrow$) Assume R/P is an integral domain. Let $a, b \in R$ such that $ab \in P$. Then

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

in R/P; note that P is the neutral element of factor ring R/P. As R/P is an integral domain, it has no non-trivial zero divisors- this forces either $a + P = P$ or $b + P = P$. Therefore, either $a \in P$ or $b \in P$. By the proposition above, this means P must be prime.

($\Leftarrow$) Assume P is prime, and suppose $(a + P)(b + P) = P$. Then $ab + P = P$, and so $ab \in P$. Then as P is prime, either $a \in P$ or $b \in P$. This means either $(a + P) = P$ or $(b + P) = P$ are the neutral element in R/P, and so R/P must be an integral domain (as $a, b \in R$ were arbitrary elements). □

Definition 3.30. *An ideal $M \trianglelefteq R$ is called maximal if:*

(i) $M \neq R$;
(ii) If $N \trianglelefteq R$ with $M \subseteq N \subseteq R$, then either $M = N$ or $N = R$.

Examples:

(i) Let $R = \mathbb{Z}$; ideals in $\mathbb{Z}$ are the sets $n\mathbb{Z}$, where $n \in \mathbb{N} \cup \{0\}$. We note that $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if $m \mid n$. From this, we have that $M \trianglelefteq \mathbb{Z}$ is maximal if and only if $M = p\mathbb{Z}$ where p is prime.

(ii) Let $R = C_{[0,1]}$. Recall: If $F \subseteq [0,1]$, we set

$$\Gamma_F = \{f \in C_{[0,1]} : f(x) = 0, \text{ for all } x \in F\}.$$

We have $\Gamma_F \trianglelefteq C_{[0,1]}$; we note that if $F_1 \subseteq F_2 \subseteq [0,1]$, then $\Gamma_{F_2} \subseteq \Gamma_{F_1}$. Fix $t \in [0,1]$ and consider Γ_t- these are the maximal ideals in $C_{[0,1]}$ (in fact, they are the maximal ideals of *any* compact Hausdorff topological space- we'll prove this later).

Definition 3.31. *Let R be a ring. We define*

$$rad(R) = \bigcap_{\substack{M \trianglelefteq R, \\ maximal}} M$$

as the Jacobson radical of R. This is an ideal of R as well.

Note: The Jacobsen radical measures how "dense" maximal ideals are in the ring. If $rad(R) = \{0\}$, then R is called *semi-simple*. The more maximal ideals you have, the "better behaved" our ring is.

Note: From here on out, assume R is a commutative unital ring.

Theorem 3.32. *Let $A \trianglelefteq R$. Then A is a maximal ideal if and only if R/A is a field.*

Proof. First, assume A is maximal. As R is a commutative unital ring, so is R/A. Let $b + A \in R/A$ such that $b + A \neq A$ (so $b \notin A$). Let

$$B = \{\text{ideal generated by } A \text{ and } b\} = \{a + bx : x \in R,\ a \in A\}.$$

We note that $A \subset B$, and setting $a = 0, x = 1$ implies $b \in B$, with $b \in B \setminus A$. As A is maximal, this implies $B = R$. Therefore, $1 \in B$, and so $1 = a + bx$ for some $x \in R$ and $a \in A$. We have

$$(b + A)(x + A) = bx + A = (bx + a) + A = 1 + A.$$

Therefore, $b + A$ is a unit in R/A; as $b + A$ was arbitrary, this proves R/A is a field.

Next, suppose R/A is a field, and that $A \subset B \trianglelefteq R$. For $b \in B \setminus A$, we know $b + A \neq A$. As R/A is a field, there exists a $c + A \in R/A$ such that

$$bc + A = (b + A)(c + A) = 1 + A.$$

Therefore, there exists an $a \in A$ such that $bc + a = 1$. As $bc \in B$ (as $b \in B$) and $a \in B$ (as $A \subset B$), we have $1 \in B$. This forces $B = R$, which shows that A must be maximal. This completes the proof. □

Corollary 3.33. *For all $t \in [0,1]$, $\Gamma_t \trianglelefteq C_{[0,1]}$ is maximal.*

Proof. Consider the map

$$\varphi : C_{[0,1]} \to \mathbb{R}, \quad \varphi(f) = f(t).$$

Note that φ is a ring homomorphism. We have $\ker \varphi = \Gamma_t$, and $\operatorname{im} \varphi = \mathbb{R}$. By the First Isomorphism Theorem, we then have

$$C_{[0,1]}/\Gamma_t \cong \mathbb{R},$$

where $\mathbb{R}$ is a field. By the previous proposition, this shows Γ_t must be maximal. □

Definition 3.34. *A set X is called partially ordered if it is equipped with a relation $\leq$ such that*

(i) $x \leq x$ *for all* $x \in X$*;*
(ii) If $x \leq y, y \leq z$ *then* $x \leq z$ *for* $x, y, z \in X$*;*
(iii) If $x \leq y, y \leq x$ *then* $x = y$ *for* $x, y \in X$*.*

Examples:

(i) If $X = \mathbb{R}$, a partial order is $\leq$ (as usually interpreted).
(ii) Let S be a set and $\mathcal{P}(S)$ be the power set of S. Set inclusion on $\mathcal{P}$ is a partial order- we say $A \leq B$ if $A \subseteq B$ for $A, B \in \mathcal{P}(S)$.

Definition 3.35. *A subset $C \subseteq X$ such that for all $x, y \in C$ then either $x \leq y$ or $y \leq x$ is called a chain in X.*

Definition 3.36. *For set $P \subseteq S$, an element $m \in S$ such that $x \leq m$ for all $x \in P$ is called an upper bound of P.*

Definition 3.37. *If S is a set and $\leq$ a partial order on S, an element $s \in S$ such that if $t \in S$ and $s \leq t$ then $t = s$ is called a maximal element of S.*

Theorem 3.38 (Zorn's Lemma)**.** *Let $(X, \leq)$ be a partially ordered set. Assume that every chain has an upper bound. Then X under $\leq$ has a maximal element.*

Note: The above is logically equivalent to the Axiom of Choice.

Theorem 3.39. *Every unital ring has a maximal ideal.*

Proof. Let R be a unital ring. Let S be the set of all proper ideals of R. Equip S with the partial order of set inclusion: for $A, B \in S$, $A \leq B$ if $A \subseteq B$. We note that $(S, \leq)$ is a partially ordered set. Observe that $M \in S$ is a maximal element for $\leq$ precisely when M is a maximal ideal. Let $\mathcal{C} \subseteq S$ be a chain. Let

$$A = \cup\{B : B \in \mathcal{C}\}.$$

This is an ideal in R, as $\mathcal{C}$ is necessarily a nested family of ideals. Furthermore, we note $A \subset R$, as if $1 \in A$ then 1 must be in some $B \in \mathcal{C}$, forcing $B = R$- a contradiction, as $\mathcal{C}$ is a chain of *proper* subsets. Then by Zorn's Lemma, A must be a maximal ideal in R. This completes the proof. □

3.5. **Integral domains and principal ideals. Recall:** A unit in a unital ring R is an element $u \in R$ such that there exists an element $v \in R$ where $uv = 1$.

Definition 3.40 (Associates, irreducibles)**.** *Elements $a, b \in R$ are called associates if there exits a unit $u \in R$ such that $b = au$. An element $a \in R$ s called irreducible if for $a = bc$, then either b is a unit or c is a unit.*

Example: In $\mathbb{Z}$: irreducible elements are the primes, ± 1, and the negatives of primes. The units in $\mathbb{Z}$ are ± 1. Associates in $\mathbb{Z}$ are also easy to describe: if $a \in \mathbb{Z}$, then $b = a$ or $b = -a$ are the only associates of a.

Note: For prime numbers in $\mathbb{Z}$: we have $p \mid ab$ implies $p \mid a$ or $p \mid b \iff p = ab$ implies $a = 1$ or $b = 1$ (where p is prime).

Theorem 3.41. *If R is an integral domain, then every prime element of R is irreducible.*

Proof. Let $a \in R$ be a prime element. Assume that $a = bc$, with $b, c \in R$. Then $a \mid bc$; as a is prime, then either $a \mid b$ or $a \mid c$. Without loss of generality, assume $a \mid b$; then $b = ax$ for some $x \in \mathbb{R}$. From this, we have $a = axc$. By cancellation (as we are in an integral domain) we then see $1 = xc$. Therefore, c must be a unit. As a was an arbitrary prime element, this holds for every prime element. □

Note: The converse of the last theorem does not hold in general. Indeed, in the ring $\mathbb{Z}[\sqrt{-3}]$ the element $1 + i\sqrt{3}$ is irreducible but not prime (**homework exercise!**).

Recall: An ideal $A \trianglelefteq R$ is principal if there exists an $a \in R$ such that

$$A = \langle a \rangle = \{ax : x \in R\}.$$

Note: If a, b are associates, then $\langle a \rangle = \langle b \rangle$. This holds, as if $b = au$ where u is a unit, then $b \in \langle a \rangle$, so $\langle b \rangle \subseteq \langle a \rangle$. Also, $a = bt$, where $ut = 1$. This means $a \in \langle b \rangle$, which forces $\langle a \rangle \subseteq \langle b \rangle$, and so the two are equivalent. In fact,

$$\langle a \rangle = \langle b \rangle \iff a = bu \text{ for a unit } u.$$

Definition 3.42 (Principal ideal domain)**.** *A commutative, unital ring R is a PID if $A \trianglelefteq R$ implies A is principal (i.e., every ideal in R is principal).*

Theorem 3.43. *Let R be a PID. Then an element $a \in R$ is prime if and only if it is irreducible.*

Proof. We have seen (by the previous theorem) that if a is prime, it is irreducible. To prove the converse, fix an irreducible element $a \in R$. Assume $a \mid bc$, where $b, c \in R$. Let

$$I = \{ax + by : x, y \in R\}.$$

We note that $I \trianglelefteq R$. Since R is a PID, there exists a $d \in R$ such that $I = \langle d \rangle$. As $a \in I$, there exists an $r \in R$ such that $a = dr$. As a is also irreducible, one of the following holds:

Case 1: Element d is a unit, so d is an associate to 1. Then $\langle d \rangle = \langle 1 \rangle = R$, and so $1 \in I$. Then there exists $x, y \in R$ such that $ax + by = 1$. Multiplying both sides of the equation by c, we see $c = cax + bcy$. As $a \mid bc$ by assumption and as $a \mid cax$ (clearly), this means $a \mid c$.

Case 2: Element r is a unit, and so $\langle d \rangle = \langle dr \rangle = \langle a \rangle$. Therefore, $I = \langle a \rangle$; as $b \in I$, this means $b \in \langle a \rangle$, and so $b = ax$ for some $x \in R$. This shows $a \mid b$.

As we have shown either $a \mid b$ or $a \mid c$, this shows a is prime. As $a \in R$ was an arbitrary irreducible element, this completes the proof. □

Example: $\mathbb{Z}[x]$ is not a PID (**homework exercise!**).

Proposition 3.44. *If F is a field, then $F[x]$ is a PID.*

Proof. Let $I \trianglelefteq F[x]$ be an ideal. Let $f \in I$ be an element with minimal degree $deg(f)$. We claim $I = \langle f \rangle$. It is clear that as $f \in I$, then $\langle f \rangle \subseteq I$ (as I is an ideal in $F[x]$). So let $g \in I$, and assume $f \nmid g$. Using the Division Algorithm, we write $g = fq + r$ where $q, r \in F[x]$ such that $deg(r) < deg(f)$. We note that

$$r = g - fq \in I,$$

as $g, fq \in I$. As f is an element of minimal degree in I, but $deg(r) < deg(f)$, this forces $r = 0$. However, this means $g = fq$, and so $f \mid g$. This means $I \subseteq \langle f \rangle$, and so $I = \langle f \rangle$. As I was arbitrary, this shows $F[x]$ is a PID. □

Example: $\langle x^k \rangle = \{fx^k : f \in F[x]\} = \{g \in F[x] : deg(g) \geq k\}$.

Definition 3.45 (Unique factorization domain)**.** *We call a commutative unital ring R a UFD if for all $a \in R$, $a \neq 0$ there exist irreducible elements $r_1, \ldots, r_k$ such that $a = r_1 \cdots r_k$, where this factorization is unique (up to their ordering and associates- i.e., if $a = p_1 \cdots p_m$ where p_j are all irreducible then $k = m$ and $\{p_1, \ldots, p_k\}$ and $\{r_1, \ldots, r_k\}$ are equal up to multiplication by units).*

Lemma 3.46. *Let R be a PID. Every chain of ideals*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$$

terminates.

Note: Rings which have the property described in the lemma above are called *Noetherian rings.*

Proof. Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ be a chain of ideals as described above. Let $I = \cup_{k=1}^{\infty} I_k$; note that $I \trianglelefteq R$. As R is a PID, there exists an $a \in R$ such that $I = \langle a \rangle$. This means $a \in I$, and so by definition there exists a $k \in \mathbb{N}$ such that $a \in I_k$. Then $I = \langle a \rangle \subseteq I_k$; we clearly have $I_k \subseteq I$, and so $I = I_k$. This shows

$$I_k = I_{k+1} = I_{k+2} = \cdots = I,$$

so our chain terminates. □

Theorem 3.47. *Every PID is a UFD.*

Proof. Let $a \in R$, where $a \neq 0$ and a is not a unit. If a is irreducible, we are done; so assume that a is not irreducible, with $a = a_1 b_1$ where a_1, b_1 are not units and are non-zero. We claim a must contain an irreducible factor. If a_1 is irreducible, we are done- so assume not. Then $a_1 = a_2 b_2$, where a_2, b_2 are nonzero and not units. If a_2 is irreducible, we are done (as a_2 is a factor of a). Else, we continue inductively where we obtain a sequence of elements $a, a_1, a_2, a_3, \ldots$ such that $a_n = a_{n+1} b_{n+1}$ where b_{n+1} is nonzero and not a unit for all $n \in \mathbb{N}$. We note that $\langle a_n \rangle \subset \langle a_{n+1} \rangle$ for each n (as if $\langle a_n \rangle \subseteq \langle a_{n+1} \rangle$, this implies they may differ by a unit, which is impossible). Then by our previous lemma, we know this chain terminates eventually- so there exists some a_k which is irreducible, with

$$\langle a \rangle \subset \langle a_1 \rangle \subseteq \ldots \subset \langle a_k \rangle.$$

This means a_k is an irreducible factor of a.

We next claim that a has an irreducible factorization. By our initial claim, $a = r_1 b_1$ for some irreducible r_1. If b_1 is irreducible, we are done. So assume not- then $b_1 = r_2 b_2$ where r_2 is irreducible. As before, if we continue inductively we obtain a sequence $r_1, r_2, r_3, \ldots$ such that

$$\langle a \rangle \subseteq \langle r_1 \rangle \subseteq \langle r_2 \rangle \subseteq \ldots$$

Again, by the lemma this chain is finite, and so there exists a b_k which is irreducible. Therefore, $a = r_1 r_2 r_3 \cdots r_k b_k$ is an irreducible factorization of a.

Finally, we wish to prove that this factorization is unique. Suppose

$$a = p_1 \cdots p_k = q_1 \cdots q_n,$$

where p_i, q_j are irreducible. We'll prove uniqueness by induction on k. It is clear that if $k = 1$, then $p_1 = q_1 \cdots q_n$ is impossible if $n \neq 1$. Next, assume the statement is true up to $k - 1$ factors. As R is a PID, any irreducible element is prime- as p_1 is irreducible, it must be prime. Furthermore, we have $p_1 \mid q_1 \cdots q_n$- so without loss of generality, assume $p_1 \mid q_1$. Then $q_1 = p_1 u$; as q_1 is irreducible, this forces u to be a unit. This means

$$p_1 p_2 \cdots p_k = p_1 u q_2 \cdots q_n \Rightarrow p_2 \cdots p_k = (uq_2) \cdots q_n.$$

By our inductive hypothesis, this factorization is unique (as we now have $k-1$ factors). Therefore, the case holds for k factors, and so it holds in general as k was arbitrary. As $a \in R$ was arbitrary, this completes the proof. □

4. Field theory

4.1. **Polynomial rings and field extensions.**

Proposition 4.1. *For a field F, then $F[x]$ is a PID. The units of $F[x]$ are the non-zero constant polynomials.*

Note: In a polynomial ring, for $f, g \in F[x]$ we have $\deg(fg) = \deg(f) + \deg(g)$. We recall that if f is a unit in $F[x]$, there must exist some $g \in F[x]$ such that $fg = 1$ (as the identity in $F[x]$ is the constant polynomial 1).

Aim: In broad strokes, in algebra we wish to answer questions like: can I find the roots of a polynomial $f \in F[x]$, and *where*?

Theorem 4.2. *Let F be a field and $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal of $F[x]$ if and only if $p(x)$ is irreducible.*

Proof. Suppose first that $\langle p(x) \rangle$ is a maximal ideal in $F[x]$. Clearly, $p(x) \neq 0$ and is not a unit as neither $\{0\}$ nor $F[x]$ are maximal ideals. If $p(x) = g(x)h(x)$ is a factorization of $p(x)$ over F, then $\langle p(x) \rangle \subseteq \langle g(x) \rangle \subseteq F[x]$. Then $\langle p(x) \rangle = \langle g(x) \rangle$ or $F[x] = \langle g(x) \rangle$. If the first case, we have $\deg(p) = \deg(g)$. In the second case, we must have $\deg(g) = 0$, and so $\deg(h) = \deg(p)$. Then $p(x)$ cannot be written as a product of two polynomials in $F[x]$ of lower degree. This means $p(x)$ is irreducible.

Next, suppose $p(x)$ is irreducible over F. Let I be any ideal of $F[x]$ such that $\langle p(x) \rangle \subseteq I \subseteq F[x]$. As $F[x]$ is a PID we know that $I = \langle g(x) \rangle$ for some $g(x) \in F[x]$. Then $p(x) \in \langle g(x) \rangle$, and so $p(x) = g(x)h(x)$ for $h(x) \in F[x]$. As $p(x)$ is irreducible over F, then either $g(x)$ is constant or $h(x)$ is constant. In the former case, this means $I = F[x]$; in the latter case, this means $I = \langle p(x) \rangle = \langle g(x) \rangle$. In either case, this shows $\langle p(x) \rangle$ is maximal, which completes the proof. □

Corollary 4.3. *Let $p \in F[x]$; then p is irreducible if and only if $F[x]/\langle p \rangle$ is a field.*

Example 4.4. *The polynomial $x^2 + 1$ is irreducible in $\mathbb{R}[x]$. We have $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$. (We adjoin an element to $\mathbb{R}$ (i.e. a root of $x^2 + 1$)).*

Definition 4.5. *A root of $f \in F[x]$ in F is an element $\zeta \in F$ such that $f(\zeta) = 0$.*

Note: $f(x) \in F[x]$, but $f(\zeta) \in F$.

Definition 4.6. *A field E is called an extension of a field F if $F \subseteq E$ and the operations on F are the restriction of the operations on E.*

Examples:

(i) $R \subseteq \mathbb{C}$ is a field extension.
(ii) $\mathbb{Q} \subseteq \mathbb{R}$ is an extension.

Theorem 4.7 (Fundamental Theorem of Field Theory (Kronecker, 1887))**.** *Let F be a field and $f(x) \in F[x]$ be a non-constant polynomial. Then F has an extension E in which $f(x)$ has a zero.*

Proof. It suffices to consider the case where f is irreducible in $F[x]$. If f is not irreducible, we can write it as a product of irreducible polynomials of smaller degree; as every zero of our factors is a zero of f, this allows us to focus solely on when f is irreducible. Let $E = {}^{F[x]}\!/_{\langle f \rangle}$. Since f is irreducible, E is a field. We also note $F \subseteq E$; recall- if F_1, F_2 are fields with $\phi : F_1 \to F_2$, then if ϕ is a monomorphism $\{\phi(a) : a \in F_1\} \subseteq F_2$ is a subfield. Then as $F_1 \cong \{\phi(a) : a \in F_1\}$, we have $F_1 \subseteq F_2$ (in the sense of field isomorphism). Equivalently, F_2 is an extension of F_1. Based on the previous comments, the map

$$\psi : F \to E, \quad \psi(a) = a + \langle f \rangle$$

is a monomorphism. Therefore, E is an extension of F. Consider $\zeta = x + \langle f \rangle \in {}^{F[x]}\!/_{\langle f \rangle} = E$. We note that $f(\zeta) = f(x) + \langle f \rangle = 0$ in E. Therefore, ζ is a root of f in the extension E. This completes the proof. □

Notation: Let $F \subseteq E$ be a field extension. The field $F(a_1, \ldots, a_n)$ where $a_1, \ldots, a_n \in E$ is the smallest subfield of E containing both $a_1, \ldots, a_n$ and F.

Examples:

(i) $\mathbb{Q} \subseteq \mathbb{R}$, with $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is an extension;
(ii) $\mathbb{Q} \subseteq \mathbb{C}$, with $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ is a field extension.

Definition 4.8. *Let $f \in F[x]$, where F is a field. Furthermore, let E be an extension of F. We say f splits over E if there exist $a_1, \ldots, a_n \in E$ such that*

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

Example: Let $f(x) = x^2 - 2$. Then $f(x)$ splits over $\mathbb{Q}(\sqrt{2})$.

Definition 4.9. *We say that E (as an extension of F where f splits) is a splitting field for f if, in addition, $E = F(a_1, \ldots, a_n)$.*

Examples:

(i) $\mathbb{Q}(\sqrt{2})$ is the splitting field of $x^2 - 2$ over $\mathbb{Q}$;
(ii) $\mathbb{Q}(i)$ is the splitting field of $x^2 + 1$ over $\mathbb{Q}$;
(iii) For $x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$, the splitting field is $\mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + di\sqrt{2} : a, b, c, d \in \mathbb{Q}\}$.

Note: We can consider field extensions as linear spaces over the base field.

Theorem 4.10 (Existence of splitting fields)**.** *Let F be a field and $f \in F[x]$ where the degree of f is at least 1. Then there exists a splitting field for f over F.*

Proof. We will prove this by induction on the degree of f. If $\deg f = 1$, then $f(x) = x - a$ where $a \in F$; this means F is the splitting field for f. So assume the statement is true for all polynomials of degree less than n, where $n \geq 2$. Let $\deg f = n$. By Kronecker's Theorem, there exists an extension E of F and $\zeta \in E$ such that $f(x) = (x - \zeta)g(x)$, where $g(x) \in E[x]$. We note that $\deg g = n - 1$; so by the inductive hypothesis, there exists an extension $E \subseteq K$ where g splits in K. Then

$$g(x) = b_0(x - b_1) \cdots (x - b_{n-1})$$

for $b_i \in K$. Then

$$f(x) = b_0(x-\zeta)(x-b_1)\cdots(x-b_{n-1})$$

in K, and so K splits f. Then $F(\zeta, b_1, \ldots, b_{n-1})$ is the splitting field of f. □

Theorem 4.11. *Let F be a field and $p \in F[x]$ be irreducible over F. Let a be a zero of p in some extension E, where $F \subseteq E$. Then*

$$F(a) \cong {}^{F[x]}\!/_{\langle p \rangle}.$$

Furthermore, if $\deg p = n$, then every element $\zeta \in F(a)$ has a unique representation of the form

$$\zeta = c_{n-1}a^{n-1} + \cdots + c_1 a + a_0,$$

where $c_0, \ldots, c_{n-1} \in F$.

Proof. Consider the following map

$$\phi : F[x] \to E,$$
$$\phi(f) = f(a).$$

Then

(i) ϕ is a homomorphism (which is straightforward to see);

(ii) $\ker \phi = \langle p \rangle$;

Proof. We see $\phi(p) = p(a) = 0$, and so $p \in \ker \phi$. This implies $\langle p \rangle \subseteq \ker \phi$. As p is irreducible, $\langle p \rangle$ is a maximal ideal. Since $1 \notin \ker \phi$, then $\ker \phi \neq F[x]$. By the maximality of $\langle p \rangle$, this forces $\ker \phi = \langle p \rangle$. □

(iii) $\operatorname{im} \phi = \{\phi(f) : f \in F[x]\} = \{f(a) : f \in F[x]\} = F(a)$.

Then by the First Isomorphism Theorem, we see

$$F(a) \cong {}^{F[x]}\!/_{\langle p \rangle}.$$

For the second part of the theorem- **homework exercise!** (As a hint: we want to show that for all $h \in {}^{F[x]}\!/_{\langle p \rangle}$, there are unique $c_0, \ldots, c_{n-1} \in F$ such that $h = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. The representation and uniqueness of $\zeta \in F(a)$ follows from the statement after the use of ϕ). □

Corollary 4.12. *Let $p \in F[x]$ be irreducible, and let a be a root of p in extension $F \subseteq E$. Furthermore, let a' be a root of p in extension $F \subseteq E'$. Then $F(a) \cong F(a')$.*

Proof. Both $F(a)$ and $F(a')$ are isomorphic to ${}^{F[x]}\!/_{\langle p \rangle}$ by the previous theorem, and so $F(a) \cong F(a')$. □

Theorem 4.13. *The splitting field of $f \in F[x]$ is unique up to isomorphism.*

General plan for the rest of the class

- Algebraic extensions of a field
- Solvability in radicals (indication only)
- Structure of finite fields

Definition 4.14. *A zero a of $f \in F[x]$ has multiplicity k if $(x-a)^k \mid f$, but $(x-a)^{k+1} \nmid f$.*

Definition 4.15. *A zero a of f is a multiple root of f if its multiplicity is greater than* 1.

Definition 4.16. *Let $f = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with coefficients in F. The derivative f' of f is the element*

$$f' = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1$$

in $F[x]$.

Note: No analysis is used here to define the derivative- it is purely symbolic, and remains in the same ring.

Proposition 4.17. *For $f, g \in F[x]$ we have*

(i) $(f+g)' = f' + g'$;
(ii) For $a \in F$, we have $(af)' = af'$;
(iii) $(fg)' = f'g + fg'$.

Proof. Left as an **exercise!** (Fairly clear through direct computation). □

Theorem 4.18. *A root $a \in E$ of $f \in F[x]$ (where E is a field extension of F), is multiple if and only if f and f' have a common factor of degree at least 1 in $F[x]$.*

Proof. First, suppose a is a multiple root; then $f = (x-a)^2 g(x)$. Using Leibniz's Rule, we have $f' = (x-a)\Big((x-a)g'(x) + 2g(x)\Big)$. So $(x-a)$ is (clearly) a common factor of f and f'. Suppose $\gcd(f, f')$ is the non-zero constant polynomial. Then there exists $g, h \in F[x]$ such that $1 = fg + f'h$ (by Bezout's Lemma). Consider $1 = fg + f'h$ as an expression in $E[x]$; if we evaluate this expression at a, we see

$$1 = f(a)g(a) + f'(a)h(a) = 0.$$

However, $1 \neq 0$- so we have reached a contradiction. Therefore, $\gcd(f, f')$ cannot be a constant, and so it must have degree greater than 0 in $F[x]$.

Conversely, assume f and f' have a common factor of degree at least one. Let a be a root of this common factor in some extension E of F. Then $f(a) = f'(a) = 0$. Write $f(x) = (x-a)g(x)$, for some $g \in E[x]$. Then $f' = g + (x-a)g'$. Evaluating at a, we see

$$f'(a) = g(a) + (0)g'(a) = g(a) = 0.$$

Therefore, g has a as a root, and so there exists an extension K of E such that $g = (x-a)h$, for $h \in K[x]$ (Note: we can just take $K = E$, as $a \in E$. It is also possible to go to a higher extension if we want to split g completely). Therefore, $f = (x-a)^2 h$, and so a is a multiple root. □

Definition 4.19. *Let F be a field. Consider*

$$N = \{n \in \mathbb{N} : \underbrace{1 + \cdots + 1}_{n \text{ times}} = 0\}.$$

If $N = \emptyset$, define $\operatorname{char}(F) = 0$. *If $N \neq \emptyset$, let* $\operatorname{char}(F) = \min N$.

Examples:

(i) $\operatorname{char}(\mathbb{R}) = \operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{C}) = 0$;
(ii) Let p be a prime. $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ equipped with addition and multiplication modulo p is a field, with $\operatorname{char}(\mathbb{F}_p) = p$. It is a field, as we can always find multiplicative and additive inverses (use Bezout's Lemma).

Note: If $\operatorname{char}(F) > 0$, then $\operatorname{char}(F)$ must be prime.

Proof. Let $n = \text{char}(F)$, where $n \geq 1$. Take $n = pq$, where $p, q \in \mathbb{N}$ and $p, q > 1$. We then see we would have

$$0 = (pq)(1) = (p(1))(q(1)).$$

As F is a field, there are no zero divisors, which forces either $(p(1)) = 0$ or $(q(1)) = 0$; this contradicts the minimality of n. Therefore, n must be prime. □

Note: If F is a finite field, then $\text{char}(F) > 0$.

Proof. Consider the elements $\{n \cdot 1 : n \in \mathbb{N}\} \subseteq F$. Since F is finite, there exist n, m such that $n(1) = m(1)$ with $n < m$. Therefore, $(m-n)(1) = 0$, which forces $\text{char}(F) \geq m-n > 0$. □

Theorem 4.20. *Let $f \in F[x]$ be irreducible, and assume* $\text{char}(F) = 0$. *Then f does not have multiple roots.*

Proof. Assume f has a multiple root. By the previous theorem, f and f' have a common factor of degree at least 1 (Note that "a is a root of f" makes sense without mentioning which field a belongs to). As f is irreducible, then f is the only factor of f with degree at least 1. This means $f \mid f'$; however, as $\deg f' < \deg f$, this means $f' = 0$. If $f = a_n x^n + \cdots + a_1 x + a_0$ and $n \geq 1$, then $f' = n a_n x^{n-1} + \cdots + a_1$. We want to show that f must be constant. As $\text{char}(F) = 0$, $n a_n \neq 0$. But then this means $f' \neq 0$, which is a contradiction. Therefore, $\deg f = 0$, and so f is either a unit or f is 0. This contradicts the fact that f is irreducible- and so we conclude that f cannot have multiple roots. □

Proposition 4.21. *If* $\text{char}(F) = p > 0$ *and $x, y \in F$, then*

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

Proof. As F is a commutative ring (as a field), we see

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots + \binom{p}{p-1} x y^{p-1} + y^p.$$

As $p \mid \binom{p}{k}$ for all $k \in \{1, \ldots, p-1\}$ (as we are using divisors which are strictly smaller than p in $\binom{p}{k}$, leaving a factor of p in the numerator) then $\binom{p}{k} x^{p-k} y^k = 0$. This means $(x+y)^p = x^p + y^p$. □

Note: We know p must be prime in the previous proposition.

Proposition 4.22. *Let F be a finite field of* $\text{char}(F) = p > 0$. *Then $|F| = p^n$ for some $n \in \mathbb{N}$.*

Proof. Consider $\{0, 1, 2 \cdot 1, 3 \cdot 1, \ldots, (p-1) \cdot 1\}$ in F, and call it F_0. We note that $F_0 \cong \mathbb{F}_p$. Now, consider F as a vector space over F_0. Let $n = \dim_{F_0} F$ (dimension as a vector space). By previous comments, for any element in F we have p total elements to pick from in n total places, which implies $|F| = p^n$. □

Definition 4.23. *A monic polynomial is a polynomial with leading coefficient of* 1.

Definition 4.24. *Let $F \subseteq E$ be a field extension. An element $a \in E$ is called algebraic over F if there exists an $f \in F[x]$ such that $f(a) = 0$. The element is transcendental if a is not algebraic.*

Definition 4.25. *The extension $F \subseteq E$ is algebraic if every $a \in E$ is algebraic over F, and transcendental if it is not algebraic.*

Definition 4.26. *Extension $F \subseteq E$ is simple if $E = F(a)$ for some $a \in E$.*

Examples:

(i) $\sqrt[n]{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$, as $f(x) = x^n - 2$ (where $f \in \mathbb{Q}[x]$) has root $\sqrt[n]{2}$.
(ii) $\sqrt{3} + \sqrt{5} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$.
Note: A real number ζ is called algebraic if ζ is algebraic over $\mathbb{Q}$ in the extension $\mathbb{Q} \subseteq \mathbb{R}$.
(iii) e, π are transcendental (Lindemann proved this for π in 1882). $\mathbb{Q}(\pi)$ is simple and transcendental.
Note: The algebraic numbers are countable, even though the reals are not- this implies the transcendental numbers vastly "outweigh" the algebraic numbers.

Definition 4.27 (Field of quotients)**.** *Consider*

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

We can think of these as "rational functions" for field F. If we equip $F(x)$ with the natural operations of addition and multiplication, then $F(x)$ becomes a field- this is called the field of quotients.

Definition 4.28. *For an algebraic element $a \in E$ where $F \subseteq E$ is a field extension, we say $f \in F[x]$ is the minimal polynomial for a if $f(a) = 0$ and the degree of f is minimal.*

Theorem 4.29. *Let $F \subseteq E$ be a field extension and $a \in E$. Then*

(i) If a is transcendental, then $F(a) \cong F(x)$;
(ii) If a is algebraic, then $F[x]/\langle p \rangle \cong F(a)$, where p is the minimal polynomial for a over F.

Proof.
(i) Let $\phi : F[x] \to E$, where $\phi(f) = f(a)$ for each $f \in F[x]$. As a is transcendental, $\ker \phi = \{0\}$. If we extend ϕ to a map $\tilde{\phi} : F(x) \to F(a)$, where $\tilde{\phi}(\frac{f}{g}) = \frac{f(a)}{g(a)}$. Note that there is no polynomial $g \in F[x]$ such that $g(a) = 0$, as a is transcendental; this means the map is well defined. Then $\tilde{\phi}$ is a map between fields which is clearly surjective and injective, with trivial kernel. Therefore, by the First Isomorphism Theorem we see $\tilde{\phi}$ is an isomorphism. This shows $F(x) \cong F(a)$.

(ii) (Sketch) Let p be the minimal polynomial for a. If we use the same map ϕ as in (i), we have $\ker \phi = \langle p \rangle$. It is fairly clear from here that by applying the First Isomorphism Theorem that

$$F[x]/\langle p \rangle \cong F(a)$$

as rings. □

Definition 4.30. *Let $F \subseteq E$ be an extension. The degree of $F \subseteq E$ is denoted by $[E : F]$, and defined by $\dim_F E$. We say $F \subseteq E$ is finite if $[E : F] < \infty$, and infinite if $[E : F] = \infty$.*

Examples:

(i) $[\mathbb{C} : \mathbb{R}] = 2$;
(ii) $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$.

Proposition 4.31. *Let $p \in F[x]$, and a be some zero of p in E (where $F \subseteq E$ is a field extension). Furthermore, suppose p is irreducible. Then $[F(a) : F] = \deg(p)$.*

Proof.
(Sketch) We consider $1, a, a^2, \ldots, a^{n-1}$ as a basis for $F(a)$ over F. As $p(a) = 0$, this implies $a^n = \lambda_0 + \lambda_1 a + \cdots + \lambda_{n-1}a^{n-1}$ for some $\lambda_i \in F$; use this to generate any power of a using elements from the basis, and proceed inductively. □

Proposition 4.32. *Let $F \subseteq E$ be a finite extension. Then $F \subseteq E$ is algebraic.*

Proof. Let $n = [E : F]$, and let $a \in E$. Then $1, a, \ldots, a^n \in E$. As $\dim_F E = n$, then our $n + 1$ elements $1, a, \ldots, a^n$ must be linearly dependent over F. Therefore, there exist $\lambda_i \in F$ (not all zero) such that $\sum_{i=0}^{n} \lambda_i a^i = 0$. Letting $f(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_n x^n$, we see that f has a root at a, and $f \in F[x]$. □

Note: The converse of the previous statement is not true: for

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots) \subseteq \mathbb{R},$$

the extension

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \ldots)$$

is algebraic but not finite.

Theorem 4.33 (Tower formula)**.** *Let $F \subseteq E$, and $E \subseteq K$ be finite extensions. Then $F \subseteq K$ is a finite extension, with*

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

Proof. Let $X = \{x_1, \ldots, x_n\}$ be a basis for E over F, and let $Y = \{y_1, \ldots, y_m\}$ be a basis for K over E. We claim the set

$$XY = \{x_i y_j : 1 \leq i \leq n, \;\; 1 \leq j \leq m\}$$

is a basis for K over F. To show linear independence, first assume there exist $\lambda_{ij} \in F$ such that $\sum_{i,j} \lambda_{ij} x_i y_j = 0$. We see

$$\sum_{i,j} \lambda_{ij} x_i y_j = \sum_{j=1}^{m} \Big(\sum_{i=1}^{n} \lambda_{ij} x_i \Big) y_j = 0.$$

As $\sum_{i=1}^{n} \lambda_{ij} x_i \in E$ and the y_j's are linearly independent, this forces $\sum_{i=1}^{n} \lambda_{ij} x_i = 0$ for $1 \leq j \leq m$. Then as the x_i's are linearly independent over F, this forces $\lambda_{ij} = 0$ for $1 \leq i \leq n$ and $1 \leq j \leq m$. Therefore, XY is a linearly independent set. To show that XY is a spanning set, we first note that any element $k \in K$ can be expressed as a linear combination $k = \sum_{j=1}^{m} c_j y_j$; then as each c_j is expressible as a linear combination $c_j = \sum_{i=1}^{n} b_i x_i$ for $b_i \in F$, we see

$$k = \sum_{j=1}^{m} c_j y_j = \sum_{j=1}^{m} \Big(\sum_{i=1}^{n} b_i x_i \Big) y_j = \sum_{j=1}^{m} \sum_{i=1}^{n} b_i x_i y_j.$$

Therefore, $K \subseteq \text{span}XY$, and $\text{span}XY \subseteq K$. This shows XY is a spanning set, and thus a basis. Therefore, $F \subseteq K$ is a finite extension with

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

□

Example: We claim $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}] = 12$. We can create the field extension above in two ways:

- $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq Q(\sqrt[3]{2}, \sqrt[4]{3})$, or
- $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{3}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3})$.

Let $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3})$. By the previous theorem (Tower formula), for the first point we get

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

By the second point, we get

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[4]{3})][\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}].$$

This tells us $3 \mid [E : \mathbb{Q}]$ and $4 \mid [E : \mathbb{Q}]$; as $\gcd(3, 4) = 1$, this means $12 \mid [E : \mathbb{Q}]$ as well. Therefore, $[E : \mathbb{Q}] \geq 12$.

Focusing on $[E : \mathbb{Q}(\sqrt[3]{2})]$, we first claim that $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}(\sqrt[3]{2})] \leq 4$. We have

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3}) : \mathbb{Q}(\sqrt[3]{2})] = [\mathbb{Q}(\sqrt[3]{2})(\sqrt[4]{3}) : \mathbb{Q}(\sqrt[3]{2})].$$

Note that $x^4 - 3 \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\sqrt[3]{2})[x]$; as $\sqrt[4]{3}$ is a root of $x^4 - 3$, this means $[E : \mathbb{Q}(\sqrt[3]{2})] \leq 4$. Therefore, $[E : \mathbb{Q}] \leq 12$, and so $[E : \mathbb{Q}] = 12$.

Example: We claim $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$, and so this extension is simple. It is clear that $\mathbb{Q}(\sqrt{3} + \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5})$. As $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ is a field extension, then $(\sqrt{3} + \sqrt{5})^{-1} \in \mathbb{Q}(\sqrt{3} + \sqrt{5})$. As

$$(\sqrt{3} + \sqrt{5})^{-1} = \frac{1}{\sqrt{3} + \sqrt{5}} = \frac{\sqrt{5} - \sqrt{3}}{2} = \frac{1}{2}(\sqrt{5} - \sqrt{3}),$$

then

$$\sqrt{5} = \frac{1}{2}(\sqrt{3} + \sqrt{5}) + (\sqrt{3} + \sqrt{5})^{-1} \in \mathbb{Q}(\sqrt{3} + \sqrt{5}).$$

Similarly, $\sqrt{3} \in \mathbb{Q}(\sqrt{3} + \sqrt{5})$. So $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{3} + \sqrt{5})$, and so we have equality.

Theorem 4.34 (Steinitz, 1910's)**.** *Suppose F is a field with $char(F) = 0$, and $a, b \in E$ are algebraic over F. Then there exists a $c \in E$ such that $F(a, b) = F(c)$.*

Proof. Let p and q be the minimal polynomials for a and b (respectively). Let $a = a_1$, and $a_1, \ldots, a_n$ be the roots for p; similarly, let $b = b_1$, and $b_1, \ldots, b_m$ be the roots of q. Consider $\frac{a_i - a}{b - b_j}$ for $i \geq 1$, $j \geq 2$. As F is infinite (as a field of characteristic zero), there exists some $d \in F$ such that $d \neq \frac{a_i - a}{b - b_j}$ for all $i \geq 1$ and $j \geq 2$. So $a_i \neq a + d(b - b_j)$ for $i \geq 1$ and $j \geq 2$. Let $c = a + db$, and $r(x) = p(c - dx)$. It is clear that $r \in F(c)[x]$; we claim $b \in F(c)$. If the claim holds, this would imply $a = c - db \in F(c)$ as well. Then $F(a, b) \subseteq F(c)$; as the other inclusion is trivial, our proof would be complete. Therefore, we attempt to prove the previous claim. First note that $q(b) = 0$, and $r(b) = p(a) = 0$. Let s be the minimal polynomial for b over $F(c)$. As s is irreducible, s is a common factor of both q and r. This means the roots of s are among the roots $b_1, \ldots, b_m$ of q. But all roots of s are also roots of r; however, $r(b_j) = p(c - db_j)$, and $c - db_j \neq a_i$ for all $i \geq 1$ and $j \geq 2$ by our choice of d. This implies s can have only one root- namely, b- which is potentially a multiple. Therefore, $s(x) = (x - b)^\ell$ for some $\ell \in \mathbb{N}$. We wish to show that $\ell = 1$. As s is irreducible (as the minimal polynomial) over a field of characteristic zero, then it cannot have multiple roots. So $s(x) = (x - b)$. Therefore, $b \in F(c)$, and so $F(a, b) \subseteq F(c)$. This completes the proof. □

Recall: $[F(a, b) : F] = [F(a, b) : F(b)][F(b) : F] = [F(c) : F]$ (where the last equality follows by the previous theorem).

Theorem 4.35. *Let $F \subseteq E$ and $E \subseteq K$ be algebraic extensions. Then $F \subseteq K$ is an algebraic extension.*

Proof. We wish to show that any element of K is algebraic over F. Let $a \in K$. As K is algebraic over E, there exists a polynomial $f \in E[x]$ such that $f(a) = 0$. Suppose $f(x) = b_0 + b_1x + \ldots + b_nx^n$, where $b_i \in E$ for $i = 0, \ldots, n$. Let $F_1 = F(b_0), F_2 = F_1(b_1), \ldots, F_n = F_{n-1}(b_{n-1}), F_{n+1} = F_n(b_n)$, and $F_{n+2} = F_{n+1}(a)$. We have

$$F \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_{n+1} \subseteq F_{n+2}.$$

As $a \in F_{n+2}$, by the Tower Formula we see

$$[F_{n+2} : F] = [F_{n+2} : F_{n+1}][F_{n+1} : F_n] \cdots [F_1 : F].$$

As each field extension above is finite (as $F \subseteq E$ is algebraic), then $[F_k : F_{k-1}]$ is finite as well. So a belongs to a finite extension of F. However, any finite extension of a field is necessarily algebraic. Therefore, a is algebraic over F, and as $a \in K$ was arbitrary this shows $F \subseteq K$ is an algebraic extension. □

Question: By extending inductively and finitely at every step, can we arrive at an extension that cannot be extended finitely anymore?

Answer: In short- yes. We will not go too much into the specifics.

Theorem 4.36. *Let $F \subseteq E$ be an extension. Let*

$$\overline{F} = \{a \in E;\ a \text{ is algebraic over } F\}.$$

Then $\overline{F}$ is a subfield of E.

Proof. Let $a, b \in \overline{F}$. We wish to show $a + b, a - b, ab$, and $\frac{a}{b} \in \overline{F}$ (provided $b \neq 0$ in the last case). Note that, by definition, $a \pm b, ab$, and $\frac{a}{b} \in F(a, b)$. We have

$$[F(a, b) : F] = [F(a, b) : F(b)][F(b) : F].$$

As a, b are algebraic over F and $F \subseteq F(b)$, then both $[F(b) : F]$ and $[F(a, b) : F(b)]$ are finite. Therefore, $F \subseteq F(a, b)$ is a finite, hence an algebraic extension. This shows $a \pm b, ab$, and $\frac{a}{b}$ are in $\overline{F}$ as well, which completes the proof. □

Example: The set of all real numbers that are algebraic is a subfield of $\mathbb{R}$.

Definition 4.37. *A field F is called algebraically closed if $F \subseteq E$ being finite implies $F = E$.*

Theorem 4.38. *Every field F has a unique (up to isomorphism) minimal algebraically closed extension $F \subseteq \overline{F}$.*

Definition 4.39. *The extension from the previous theorem is called the algebraic closure of F.*

Theorem 4.40. *A field F is algebraically closed if every $f \in F[x]$ has a zero in F.*

Example: $\mathbb{C}$ is algebraically closed- this is just a restatement of the Fundamental Theorem of Algebra by Gauss (which we will not prove).

4.2. **Classification of finite fields.**

Theorem 4.41. *For every prime p and every $n \in \mathbb{N}$, there exists a unique field $\mathbb{F}_{p^n}$ with p^n elements.*

Example: The field $\mathbb{F}_p = \mathbb{Z}_p$ for a prime p.

Recall: For every finite field F, there exists a prime p and $n \in \mathbb{N}$ such that $|F| = p^n$.

Theorem 4.42. *Let p be a prime. For every $n \in \mathbb{N}$ there exists a unique field of order p^n, denoted by $\mathbb{F}_{p^n}$.*

Proof. Let $f(x) = x^{p^n} - x$, where $f \in \mathbb{F}_p[x]$. Let $\overline{\mathbb{F}_p}$ be the splitting field of f over $\mathbb{F}_p$. We claim f does not have multiple roots. To show this, we note $f' = p^n x^{p^n-1} - 1 \equiv -1$, as we are working over a field of characteristic p. Then $\gcd(f, f') = \gcd(f, -1) = 1$, so f and f' share no common roots. Therefore, f does not have multiple roots over $\mathbb{F}_p$. Let $\Lambda = \{a \in \overline{\mathbb{F}_p} : a^{p^n} = a\}$. We claim Λ is closed under addition, subtraction, multiplication and division. Suppose $a, b \in \Lambda$; as we are working over a field of characteristic p, we see

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n} = a \pm b.$$

So $a \pm b \in \Lambda$, showing closure under addition and multiplication. Similarly, by commutativity of $\mathbb{F}_{p^n}$ it is clear $ab, \frac{a}{b} \in \Lambda$ when $a, b \in \Lambda$ (just raise both to the power of p^n). Therefore, Λ is a subfield of $\overline{\mathbb{F}_p}$, with $\left|\Lambda\right| = p^n$. This proves the existence of a field of order p^n.

To show uniqueness, suppose K is a field with $\left|K\right| = p^n$. We claim $\mathrm{char}(K) = p$. Suppose $q = \mathrm{char}(K)$. As $\mathbb{F}_q \subseteq K$, by Lagrange's Theorem we have $\left|\mathbb{F}_q\right| \Big| \left|K\right|$; so $q \mid p^n$. As p is prime, this forces $q = p$ which means $\mathrm{char}(K) = p$. Consider the multiplicative group K^*. We have $|K^*| = p^n - 1$; this means for any $\zeta \in K^*$, $\zeta^{p^n-1} = 1$. Therefore, $\zeta^{p^n} = \zeta$ for all of K^*. As 0 satisfies this relation as well, this holds for all of K- so K contains all roots of f. This means K must be the splitting field of f. □

Structure of $\mathbb{F}_{p^n}$

Additive structure:

Proposition 4.43. $\mathbb{F}_{p^n} \cong \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ times}}$ *as groups.*

Proof. We know $(\mathbb{F}_{p^n}, +)$ is a finite abelian group by definition, with $\left|\mathbb{F}_{p^n}\right| = p^n$. By the Fundamental Theorem of Finite Abelian Groups, we have

$$\mathbb{F}_{p^n} \cong \mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \cdots \times \mathbb{Z}_{p^{k_n}}.$$

As $\mathrm{char}(\mathbb{F}_{p^n}) = p$, we must have $k_1 = k_2 = \cdots = k_n = 1$ (otherwise, there exists an element in $\mathbb{F}_{p^n}$ with order strictly greater than p). So

$$\mathbb{F}_{p^n} \cong \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ times}}.$$

□

Multiplicative structure:

Proposition 4.44. *$\mathbb{F}_{p^n}^*$ is cyclic.*

Proof. Split $\mathbb{F}_{p^n}^* = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ as a direct product of finite abelian groups (by the Fundamental Theorem of Finite Abelian Groups). We know that if n_i and n_j are relatively prime for all $i \neq j$, then

$$\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r} = \mathbb{Z}_{n_1 n_2 \cdots n_r},$$

which is clearly cyclic. We wish to show this is the case. To that end, assume towards contradiction that there exists a $d > 1$ and i, j with $i \neq j$ such that $d \mid n_i$ and $d \mid n_j$. The groups $\mathbb{Z}_{n_i}$ and $\mathbb{Z}_{n_j}$ both have subgroups of order d; so there exist $H \leq \mathbb{Z}_{n_i}$ and $K \leq \mathbb{Z}_{n_j}$ such that $|H| = |K| = d$, with $H \cap K = \{e\}$. Take any $h \in H$; considering h as an element of $\mathbb{F}_{p^n}^*$ where multiplication is the operation, we have $h^d = 1$. Similarly, $k^d = 1$ for any $k \in K$. Consider the polynomial $x^d - 1$. We note that $x^d - 1$ has at most d zeros. However, we have just shown that there are a total of $2d - 1$ zeros coming from H and K combined. Therefore, as we have reached a contradiction, we conclude that $d = 1$, and so $\mathbb{F}_{p^n}^* \cong \mathbb{Z}_{n_1 n_2 \cdots n_r}$ is a cyclic group. □

Theorem 4.45. *Let p be prime and $n \in \mathbb{N}$. For every $m \mid n$, there exists a unique subfield of $\mathbb{F}_{p^n}$ of order p^m. Furthermore, these are all subfields of $\mathbb{F}_{p^n}$.*

Note: Uniqueness here is up to *subset*, not just isomorphism- a stronger condition.

Proof. Let $m \mid n$, for $m, n \in \mathbb{N}$. Then $p^m - 1 \mid p^n - 1$; this means there exists a $t \in \mathbb{N}$ such that $p^n - 1 = (p^m - 1)t$. Let

$$K = \{a \in \mathbb{F}_{p^n} : a^{p^m} = a\}.$$

We first note that $|K| \leq p^m$, as the polynomial $x^{p^m} - x$ cannot have more than p^m zeros. We also note that K is a subfield of $\mathbb{F}_{p^n}$ (by similar reasoning as in previous proofs from this section). We know $\mathbb{F}_{p^n}^*$ is a cyclic group- so let a be a generator, with $\langle a \rangle = \mathbb{F}_{p^n}^*$. Consider the element a^t- we have

$$(a^t)^{p^m - 1} = a^{p^n - 1} = 1,$$

and so $a^t = K$. We also know $|a^t| = p^m - 1$, as an element of K. Therefore, $|K| \geq p^m$, which forces $|K| = p^m$. This proves existence.

To show uniqueness, suppose K and L are distinct subfields of $\mathbb{F}_{p^n}$ of order p^m. We note that $x^{p^m} - x$ has all elements of K and all elements of L as roots; as K, L are distinct this means we have at least $p^m + 1$ roots. However, the polynomial can clearly have at most p^m roots- a contradiction. Therefore, we conclude that there are no such distinct subfields, and so any subfield of this order is unique.

Finally, to prove exhaustiveness let K be a subfield of $\mathbb{F}_{p^n}$. We know $\text{char}(K) = p$; this implies $|K| = p^m$ for some $m \in \mathbb{N}$. We note that

$$\mathbb{F}_p \subseteq K \subseteq \mathbb{F}_{p^n}$$

where we consider these inclusions as field extensions. Then by the Tower Formula, we have

$$[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : K][K : \mathbb{F}_p] = [\mathbb{F}_{p^n} : K][\mathbb{F}_{p^m} : \mathbb{F}_p].$$

We claim $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$; this follows from considering $\mathbb{F}_{p^n} \cong \mathbb{F}_p \times \cdots \times \mathbb{F}_p$ as a vector space over $\mathbb{F}_p$ with basis $\{(1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1)\}$ consisting of n vectors. This shows $n = [\mathbb{F}_{p^n} : K]m$, and so $m \mid n$. This completes the proof. □

4.3. **Solvability and Galois miscellany.**

Definition 4.46. *We say $\sqrt[n]{\zeta}$ is a radical, for $\zeta \in \mathbb{Z}$.*

Our question: For any polynomial, can we express the roots of the polynomial in radicals using only finitely many steps?

Definition 4.47. *Let $F \subseteq E$ be a field extension. We define*

$$Gal_F(E) = \{\phi \in \mathrm{Aut}(E) : \phi(a) = a, \quad \text{for all } a \in F\}.$$

We say $\mathrm{Gal}_F(E)$ is a group under composition.

Galois duality: If $G \leq \mathrm{Gal}_F(E)$, we can form

$$E_G = \{a \in E : \phi(a) = a \text{ for all } \phi \in G\}.$$

Then $F \subseteq E_G \subseteq E$ as field extensions.

Theorem 4.48 (Galois I)**.** *There exists a bijective correspondence between the extensions $F \subseteq K \subseteq E$ (i.e. field extensions sitting between F and E) and the subgroups of $\mathrm{Gal}_F(E)$.*

Let $f \in F[x]$. Then f is solvable in radicals if: f has a splitting field $F(a_1, \ldots, a_n)$ such that $a_1^{k_1} \in F$ for some $k_1 \in \mathbb{N}$, $a_2^{k_2} \in F(a_1)$ for some $k_2 \in \mathbb{N}, \ldots, a_n^{k_n} \in F(a_1, \ldots, a_{n-1})$ for some $k_n \in \mathbb{N}$.

Definition 4.49. *A group G is called solvable if*

$$G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq \{e\}$$

and G_i/G_{i+1} is abelian.

Theorem 4.50 (Galois II)**.** *If f is solvable in radicals, then $\mathrm{Gal}_F(E)$ (where E is the splitting field of f) is solvable.*

5. Addendum

5.1. **Addendum/examples.**

Example: (Visualizing the field $\mathbb{F}_{16}$) We will use the fact that if a polynomial p is irreducible in $F[x]$, then $F[x]/\langle p \rangle$ is a field. Let $F = \mathbb{F}_2$, and consider the polynomial $p(x) = x^4 + x + 1$. We note that p has no root in $\mathbb{F}_2$ (plug in 0 and 1 to test), and cannot be factored into a product of two irreducible quadratic polynomials. Therefore, p is irreducible. Looking at the field $\mathbb{F}_2[x]/\langle p \rangle$, we use the relation $x^4 = -x - 1 = x + 1$. This implies

$$\mathbb{F}_2[x]/\langle p \rangle = \{a + bx + cx^2 + dx^3 + \langle p \rangle : a, b, c, d \in \mathbb{F}_2\}.$$

The operations on our field are as follows: for addition, it is done coefficient-wise, and always modulo 2; likewise, multiplication is done similarly while also using the reducing relation $x^4 = x + 1$. We know that as an additive group that

$$\mathbb{F}_{16} = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,$$

while $\mathbb{F}_{16}^*$ is a cyclic group of order 15. We claim $x + \langle p \rangle$ in $\mathbb{F}_2[x]/\langle p \rangle$ is a generator for a cyclic group of order 15, which establishes the connection between $\mathbb{F}_{16}$ and our field above. As all elements in $\mathbb{F}_{16}^*$ must have order $1, 3, 5$ or 15- since $x^3 = x^3$ (i.e. we cannot reduce further) and $x^5 = x(x+1) = x^2 + x$, this means it does not have order 3 or 5. It is clearly not the identity element in the cyclic group, so it must have order 15. This means x is a generator.

Theorem 5.1 (Eisenstein's Criterion)**.** *Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$, where $f \in \mathbb{Z}[x]$ and $a_n \neq 0$. Suppose p is prime, where $p \mid a_0, \ldots, a_{n-1}$, but $p \nmid a_n$ and $p^2 \nmid a_0$. Then f is irreducible in $\mathbb{Q}[x]$.*

Application: Let p be prime, and consider the polynomial

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

We claim f is irreducible over $\mathbb{Q}[x]$. To show this, first note that

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}.$$

Consider $\Phi(x) = f(x+1)$. We see

$$\begin{aligned}\Phi(x) = f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} &= \frac{x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-1}x + 1 - 1}{x + 1 - 1} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-1}.\end{aligned}$$

As we have shown before, we know $p \mid \binom{p}{k}$ when $1 \leq k \leq p-1$. Then by Eisenstein's Criterion, the polynomial $\Phi(x)$ is irreducible in $\mathbb{Q}[x]$. This therefore implies f is irreducible in $\mathbb{Q}[x]$ as well.

Theorem 5.2 (Fermat's Little Theorem)**.** *If p is prime and $a \in \mathbb{Z}$ with $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$. Equivalently- if p is prime and $a \in \mathbb{Z}$, then $a^p \equiv a \mod p$.*

Proof. Consider the field $\mathbb{F}_p$. In $\mathbb{F}_p^*$, every element has order $p-1$. The conclusions of the theorem follow easily from this. □

Theorem 5.3 (Rational Root Theorem)**.** *Let $f(x) = a_nx^n + \cdots + a_1x + a_0$, where $a_i \in \mathbb{Z}$ and $a_0, a_n \neq 0$. If $\frac{p}{q}$ is a rational root of f, where p and q are relatively prime (i.e. written in lowest form) then we must have $p \mid a_0$ and $q \mid a_n$.*

Note: What the theorem above then tells us is if we look at all possible rationals which satisfy those two constraints for a polynomial, and none of them are a zero for the polynomial then f is irreducible over $\mathbb{Q}$.