1 Groups

Definition 1.1 (Group)**.** *A Group G is a set with a binary operation $m : G \times G \to G$ $(m(g,h) := gh)$ such that*

1. $\forall a, b, c \in G$, $(ab)c = a(bc)$
2. $\exists e \in G$ *such that* $\forall a \in G$, $ea = ae = a$
3. $\forall a \in G$, $\exists a^{-1} \in G$ *such that* $aa^{-1} = a^{-1}a = e$

If only 1 is satisfied, then G is a semigroup.
If only 1 and 2 are satisfied, then G is a monoid.
If a structure has $\forall a, b \in G$, $ab = ba$, then it is abelian.

Definition 1.2 (Group Homomorphism)**.** *A map $f : G \to H$ between groups is a homomorphism if $f(ab) = f(a)f(b)$*
If the homomorphism is injective, it is a monomorphism.
If the homomorphism is surjective, it is an epimorphism.
If the homomorphism is bijective, it is an isomorphism.

Lemma 1.1. *Let $\varphi : G \to H$ be a group homomorphism. Then $\varphi(e_G) = e_H$ and $\varphi(a^{-1}) = \varphi(a)^{-1}$*

Proof. $\varphi(a) = \varphi(ae_G) = \varphi(a)\varphi(e_G)$
$\varphi(a)^{-1}\varphi(a) = \varphi(a)^{-1}\varphi(a)\varphi(e_G) = e_H = e_H\varphi)e_G) = \varphi(e_G)$
The other part is similar. □

Definition 1.3 (Kernel of a Homomorphism)**.** *The kernel of a homomorphism $f : G \to H$ is the set $\{a \in G : f(a) = e_H\}$ and is denoted* $\ker f$

Definition 1.4 (Subgroup)**.** *If G is a group and $H \subseteq G$ is itself a group under G's multiplication, then H is a subgroup of G, denoted $H < G$*

Trivially, $\ker f < G$

Lemma 1.2. *A nonempty subset $H \subseteq G$ is a subgroup iff $\forall a, b \in H$, $ab^{-1} \in G$*

Definition 1.5 ($\hom(G,H)$)**.** *If G, H are groups, then* $\hom(G,H)$ *is the set of homomorphisms from G to H.*

Definition 1.6 (Cosets)**.** *Let $H < G$. The the left coset of H containing a is $aH = \{ah : h \in H\}$.*
Right cosets are similarly defined.

Lemma 1.3. *If $|H| < \infty$ then $|aH| = |H| = |Ha|$*

Proof. Let $h : H \to aH : h \mapsto ah$. Then $ah = ah' \Rightarrow h = h'$, so f is bijective. □

Lemma 1.4. *Let $H < G$. Then for $a, b \in G$, either $aH = bH$ or $aH \cap bH = \emptyset$. Also, $aH = bH$ iff $a^{-1}b \in H$*

Proof. Suppose $aH \cap bH \neq \emptyset$. Then $\exists h, h' \in H$ such that $ah = bh'$.

So $a = bh'h^{-1}$ thus $a \in bH$. Thus $aH \subset bH$. This argument is symmetric, thus $aH = bH$.

Then, if $aH = bH$ we have $a^{-1}b = hh'^{-1} \in H$

If $a^{-1}b = h \in H$, then $b = ah$ so $b \in aH$ and $aH \cap bH \neq \emptyset$, so $aH = bH$. □

Definition 1.7 (Order of g)**.** *The order of $g \in G$ is the smallest positive n such that $g^n = e$, or ∞ is no such n exists.*

Theorem 1.5 (Lagrange's Theorem)**.** *If G is a finite group, then the order of any element divides $|G|$.*

Proof. We first check that each element has finite order.

Since $|G| < \infty$, there must be $m, n > 0$ such that $g^n = g^m$, where $n < m$

So $g^{m-n} = e$.

Suppose that g has order n. Then consider $\{e, g, g^2, \ldots, g^{n-1}\} = H$

The left cosets of H partition G, and each is size n, so $|G| = nk$, where k is the number of left cosets of G. □

Definition 1.8 (Direct Product Group)**.** *If G, H are groups, then $G \times H$ has elements $\{(g, h) : g \in G, h \in H\}$ and multiplication $(g, h)(g', h') = (gg', hh')$*

Definition 1.9 (Normal Subgroup)**.** *A subgroup H of G is said to be normal if $\forall a \in G, aH = Ha$. We write $H \trianglelefteq G$*

Lemma 1.6. *$N \trianglelefteq G$ iff $aNa^{-1} = H$ $\forall a \in G$ iff $aNa^{-1} \subseteq N$ $\forall a \in G$.*

Proof. If N is normal, then $aN = Na$, so $aNa^{-1} \subseteq N$.

Also, $\forall n' \in N$, $\exists n \in N$ such that $an = n'a$ so $ana^{-1} = n' \in N$, thus $n' \in aNa^{-1}$. Thus $aNa^{-1} = N$

If $aNa^{-1} = N$, then $\forall n \in N$, $\exists n' \in N$ such that $an'a^{-1} = n$ so $an' = na$ and thus $Na \subset aN$. This argument is symmetric, so $N \trianglelefteq G$. □

Definition 1.10 (Index)**.** *If $H < G$ then the index of H in G, written $[G : H]$ is the number of left cosets of H. This may be infinite.*

Theorem 1.7. *If $N \trianglelefteq G$ then the set $\{aN : a \in G\}$ is a group of order $[G : N]$ with operation $(aN)(bN) = (ab)N$*

Proof. If $aN = a'N$, $bN = b'N$ then $abN = a'b'N$. as $aN = a'N, a^{-1}a' \in N$, similarly $b^{-1}b' \in N$.

$(ab)^{-1}(a'b') = b^{-1}a^{-1}a'b' = b^{-1}nb$ for some $n \in N$.

Then, there is an n' such that $b^{-1}nb' = b^{-1}b'n' = n'' \in N$

Thus, $abN = a'b'N$

This multiplication is associative, because G is a group, and the other group properties follow similarly. □

Definition 1.11 (Quotient Group)**.** *The group in the theorem above is called G/N.*

Note: $f : G \to H$ a homomorphism, then $\ker f \trianglelefteq G$.

Theorem 1.8. *If $f : G \to H$ is a homomorphism and $N \trianglelefteq G$, $N \subseteq \ker f$ then $\exists! \tilde{f} : G/N \to H$ such that $\tilde{f}(aN) = f(a)\ \forall a \in G$. Then $\operatorname{Im} \tilde{f} = \operatorname{Im}(f)$ and $\ker \tilde{f} = \ker f/N$ and $\tilde{f}$ is an isomorphism iff f is surjective and $N = \ker f$.*

Proof. See Hungerford. □

Corollary 1.9 (First Isomorphism Theorem)**.** *If $f : G \to H$ is a group homomorphism, then $G/\ker f \simeq \operatorname{Im} f$*

Definition 1.12 (HK)**.** *If H and K are subsets of a group, then $HK = \{hk : h \in H, k \in K\}$*

Definition 1.13 (Join)**.** *If $H, K < G$ then $H \vee K$ is the smallest subgroup of G containing both H and K.*

Whenever the smallest subgroup of G containing some set S is mentioned, it is the subgroup $\cap H_i$, where $H_i < G$ and $S \subseteq H_i$.

Lemma 1.10. *If $N \trianglelefteq G, K < G$, then*

1. *$N \cap K \trianglelefteq K$*
2. *$N \trianglelefteq N \vee K$*
3. *$NK = N \vee K = KN$*

Proof.

1. If $n \in N \cap K$, $a \in K$, then $ana^{-1} \in N \cap K$, so $a(N \cap K)a^{-1} \subset N \cap K$, so $N \cap K \trianglelefteq K$
2. $N \trianglelefteq G$ and $N < N \vee K < G$, so $N \trianglelefteq N \vee K$.
3. Since $N \vee K$ is closed under multiplication, $NK \subseteq N \vee K$. Let $a \in N \vee K$, write $a = n_1 k_1 \ldots, n_r k_r$

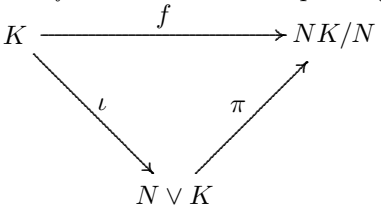
   Since N is normal, $\forall n \in N$, we can write $k_j n = n' k_j$ for some $n' \in N$.

   So $a = nk_1 \ldots k_r = nk$ with $n \in N, k \in K$. So $a \in NK$.

□

Theorem 1.11 (Second Isomorphism Theorem)**.** *If $K, N < G$ and $N \trianglelefteq G$ then $K/N \cap K \simeq NK/N$*

Proof. Define a homomorphism $f : K \to NK/N$ by $f(k) = kN$.



$\ker f = N \cap K$. By the first isomorphism theorem, $K/N \cap K \simeq \operatorname{Im} f$

Thus, it remains to show that $\operatorname{Im} f = NK/N$.

Consider $nkN \in NK/N$. Since N is normal, $\exists n'$ such that $nkN = kn'N = kN = f(k)$. □

Theorem 1.12 (Third Isomorphism Theorem)**.** *Let $K \trianglelefteq G$ and $H \trianglelefteq G$, with $K < H$. Then $H/K \trianglelefteq G/K$ and $(G/K)/(H/K) \trianglelefteq G/H$*

Proof. Define a homomorphism $f : G/K \to G/H$ by $f(aK) = aH$. f is a homomorphism, as $K \subset \ker(G \to G/H)$

$\ker f = H/K$, and f is surjective by definition, so by the first isomorphism theorem, the result follows. □

Definition 1.14 (Simple Group)**.** *A group G is a simple group if it has no proper nontrivial normal subgroups.*

Now we will determine solutions to the problem of how can a group be described.

1. Listing the elements and making a table
2. Give the generators for G as a subgroups of S_n, finite groups only.
3. Give it as $\operatorname{Aut} X$ for some structure X.
4. Build up from simpler groups
5. Give generators for G as a subgroup of GL_n (giving a homomorphism $f : G \to \mathrm{GL}_n$ is the beginning of representation theory)
6. Generators and Relations.

Theorem 1.13 (Cayley)**.** *Any finite group G is isomorphic to a subgroup of S_n for some n.*

Proof. Let $n = |G|$, and fix a bijection $\{1, \dots, n\} \to G$ such that $G = \{g_1, \dots, g_n\}$.

Given $g \in G$, $\forall i \exists j$ such that $gg_i = g_j$. Note that if $gg_i = gg_k$ then $g_i = g_k$.

Define $\sigma_g : \{1, \dots, n\} \to \{1, \dots, n\}$ by $\sigma_g(i) = j$ if $gg_i = g_j$

This is an injection from a finite set into itself, and so a bijection. We will define $\varphi : G \to S_n : g \mapsto \sigma_g$

Check that $\sigma_{gh} = \sigma_g \sigma_h$. φ is a homomorphism.

Also, if $gg_i = g_i$ then $g = e$, so $\sigma_g \neq 1$ for $g \neq e$. So φ is an injection, this $\varphi(G) \simeq G$ and is a subgroup of S_n. □

Corollary 1.14. *Every finite group is isomorphic to a subgroup of $\mathrm{GL}_n(\mathbb{R})$ for $n = |G|$.*

Proof. By Cayley's Theorem, it suffices to show that S_n is isomorphic to a subgroup of GL_n

Define $\varphi : S_n \to \mathrm{GL}_n(\mathbb{R}) : \sigma \mapsto A$ written $A_{ij} = \begin{cases} 1 & \texttt{if } \sigma(j) = i \\ 0 & \texttt{else} \end{cases}$ □

Definition 1.15 ($F(X)$)**.** *Given a set X, we choose a set X^{-1} which is disjoint from X and has the same cardinality, with a bijection $X \to X^{-1} : x \mapsto x^{-1}$, and we define an element $1 \in X \cup X^{-1}$.*

A word is a sequence $(a_1, \dots,)$ with $a_i \in X \cup X^{-1} \cup \{1\}$ such that $\exists N$ such that $a_n = 1 \forall n \geq N$.

A word is reduced if $a_i = x \Rightarrow a_{i+1}, a_{i-1} \neq x^{-1}$ and if $a_n = 1$ then $a_m = 1 \forall m \geq n$.

$F(X)$ is the set of reduced words in X.

Lemma 1.15. *$F(X)$ is a group with respect to concatenation and reduction of reduced words.*

Lemma 1.16. *If G is a group and $f : X \to G$ is a map of sets, then there is a unique homomorphism $\overline{f} : F(X) \to G$ such that $f = \overline{f} \circ \iota$, where $\iota : X \to F(X)$ is the inclusion map. That is, $F(X)$ is free in the category of groups.*

Proof. Define $\overline{f}(1) = e \in G$.

If $x_1^{\lambda_1} \dots x_n^{\lambda_n}$ is a nonempty reduced word, then $\overline{f}(x_1^{\lambda_1} \dots x_n^{\lambda_n}) = f(x_1)^{\lambda_1} \dots f(x_n)^{\lambda_n}$. $\overline{f}$ is a homomorphism. □

Corollary 1.17. *Every group is a homomorphic image of a free group.*

Proof. Let X be a set of generators for G, that is, no proper subgroup contains X.

Let $\iota : X \to G$ be the inclusion. Then $\overline{\iota} : F(X) \to G$ is a group homomorphism and is surjective. Thus, by the first isomorphism theorem, $\overline{\iota}(F(X)) \simeq G$.

That is, $G \simeq F(X)/\ker \overline{\iota}$ □

Definition 1.16 ($N(H)$)**.** *The normal subject generated by a set H is the intersection, $N(H)$, of all normal subgroups containing H.*

And so, any group can be given by generators X and relations R by $\langle X|R\rangle$ where $G \simeq F(X)/N(R)$.

G is finitely generated if X is finite.

G is finitely presented if both X and R are finite.

Definition 1.17 (Free Product of Groups)**.** *If G, H are groups, then the group $G * H$ consists of all reduced words in $G \cup H$.*

2 Structure of Groups

Recall that a free group $F(X)$ is free on X in the category of groups. What about the category of abelian groups?

If $X = \{x_1, \dots, x_n\}$ then $\mathbb{Z}^n = \bigoplus_{i=1}^n \mathbb{Z}$ is free on X is the category of abelian groups.

For X infinite, we want the restricted direct sum, that is, we have only finitely many nonzero terms.

Definition 2.1 (Basis of an Abelian Group)**.** *A basis of an abelian group F is $X \subseteq F$ such that $F = \langle X \rangle$ and $\sum n_i x_i = 0 \Rightarrow n_i = 0$, for $n_i \in \mathbb{Z}$.*

Lemma 2.1. *F has a basis X iff $F \simeq \oplus'_{x \in X} \mathbb{Z}$, where $\oplus'$ is the restricted direct sum.*

Proof. Define a map $\varphi \oplus'_{x \in X} \mathbb{Z} \to F : a \mapsto \sum_{x \in X, a_x \neq 0} a_x x$

φ is a homomorphism. φ is also surjective, as $F = \langle X \rangle$. If $a \in \ker \varphi$ then $\sum a_x x = 0 \Rightarrow a_x = 0$, so $a = 0$.

Thus, φ is an isomorphism. □

Lemma 2.2. *Assume $G \simeq \oplus_{i=1}^n G_i$, $H \trianglelefteq G$, $H \simeq \oplus_{i=1}^n H_i$ and $H_i \trianglelefteq G_i$. Then $G/H \simeq \oplus_{i=1}^n G_i/H_i$.*

Proof. Define $\pi_i : G_i \to G_i/H_i : g_i \mapsto g_i H_i$.

$\Pi\pi_i : G \to \oplus G_i/H_i : (g_i) \mapsto \oplus g_i H_i$.

$\Pi\pi_i$ is a surjective homomorphism with kernel H. □

Theorem 2.3. *If X, Y are bases of an abelian group F, then $|X| = |Y| = n$ or both are infinite. $|X|$ is the rank of F.*

Proof. We may assume $|X| = n$. Consider $2F = \{2u : u \in F\} < F$, and consider $F/2F$.

As F has basis X, $F \simeq \mathbb{Z}^n$ and $2F \simeq \oplus 2\mathbb{Z}$.

By the lemma, $F/2F \simeq \mathbb{Z}^n / \oplus 2\mathbb{Z} \simeq \oplus \mathbb{Z}/2\mathbb{Z}$, so $|F/2F| = 2^n$.

If $|Y| > n$, the same argument says $|F/2F| > 2^n$, so $|Y| = |X| = n$. □

Theorem 2.4. *If F is a free abelian group of rank n and $G < F$ is nontrivial, then $\exists$ basis $\{x_1, \ldots, x_n\}$ of F and $r (1 \leq r \leq n)$ and $d_1, \ldots, d_r \in \mathbb{N}$ such that $d_1 | \ldots | d_r$ such that G is a free abelian group with basis $\{d_i x_i | 1 \leq i \leq r\}$.*

Proof. The main ideas of the proof are the Euclidean algorithm: given $n, d \in \mathbb{Z}$, $\exists q, r \in \mathbb{Z}$ with $0 \leq r < |d|$ with $n = qd + r$ and if $\{x_1, \ldots, x_n\}$ is a basis for $\mathbb{Z}^n$, then so is $\{x_1 + \sum_{i=2}^n a_i x_i, \ldots, x_n\}$.

We proceed by induction on n.

Suppose $n = 1$. Then $F \simeq \mathbb{Z}$, $G \leq F$.

Let d be the smallest positive element of G. Let $n \in G$. Write $n = qd + r$, $0 \leq r < d$.

As $r = n - qd \in G$, and $r < d$, $r = 0$. So $n = qd \in \langle d \rangle$ so $G = d\mathbb{Z}$.

Let S be the set of $r \in \mathbb{Z}$ such that $\exists$ a basis $\{y_1, \ldots, y_n\}$ for F and $v \in G$ with $v = r y_1 + k_2 y_2 + \ldots + k_n y_n$.

As G is nonempty, S is nonempty. Since $\{y_2, y_1, \ldots, y_n\}$ is a basis, $k_2, \ldots, k_n \in S$.

Let d be the smallest positive element of S, which exists if $G \neq 0$.

So there is a basis $\{y_1, \ldots, y_n\}$ for F and $v \in G$ with $v = d_1 y_1 + \sum_{i=2}^n k_i y_i$. Write $k_i = d_1 q_i + r_i$, then $v = d_1(y_1 + \sum_{i=2}^n q_i y_i) + \sum r_i y_i$ and $\{y_1 + \sum_{i=2}^n q_i y_i, y_2, \ldots, y_n\}$ is again a basis for F so $r_i \in S$. So since $r_i < d1$, $r_i = 0$ $\forall i$.

Let $x_1 = y_1 + \sum_{i=2}^n q_i y_i$, $v = d_1 x_1$.

Let $H = \langle y_2, \ldots, y_n \rangle$, and consider $G \cap H$.

We know $F = \langle x_1 \rangle \oplus H$. We will show that $G \simeq \langle v \rangle \oplus (G \cap H)$

First $\langle v \rangle \cap (G \cap H) = \{0\}$, since $av = ad_1x_1 = \sum_{i=1}^{n} k_i y_i$. them $-ad_1x_i + \sum_{i=1}^{n} k_i y_i = 0$, so $-ad_1 = k_i = 0$ for all i, so $av = 0$.

Next let $g \in G$. Write $g = ax_1 + \sum_{i=2}^{n} k_i y_i$. Write $a = qd_1 + r$, $0 \leq r \leq d_1$.

So $g - qv \in G$ and $g - qv = rx_1 + \sum k_i y_i$ so $r \in S$, and as $r < d_1$, $r = 0$ so $q - qv = \sum k_i y_i \in G \cap H$.

Now we see $\langle v \rangle \oplus G \cap H \to G : (av, g') \mapsto av + g'$ is a surjective homomorphism with trivial kernel, and so is an isomorphism.

Since H is free abelian of smaller rank, by induction, $\exists$ a basis $x_2, \ldots, x_n$ for H such that $G \cap H = \langle d_2 x_2, \ldots, d_r x_r \rangle$ with $d_2 | \ldots | d_n$.

Now $\{x_1, \ldots, x_n\}$ is a basis for F and $G = \langle d_1 x_1, \ldots, d_n x_n \rangle$

Write $d_2 = qd_1 + r$ $0 \leq r < d_1$, then $d_2 x_2 + d_1 x_1 \in G$ and $d_2 x_2 + d_1 x_2 = qd_1 x_2 + r x_2 + d_1 x_1 = r x_2 + d_1(x_1 + q x_2)$, since $\{x_2, x_1 + q x_2, \ldots, x_n\}$ is a basis for F, $r \in S$ so $r = 0$. Thus, $d_1 | d_2$. □

Corollary 2.5 (Classification Theorem of Finitely Generated Abelian Groups)**.** *Every finitely generated abelian group is isomorphic to a finite direct sum of cyclic groups in which finite cyclic summands, if any, are of orders $m_1, \ldots, m_t$ where $m_1 | \ldots | m_t$.*

Proof. If G is generated by $n > 0$ elements, then there is a surjection $\pi : \mathbb{Z}^n \to G$.

If π is an isomorphism, then done. Else, let $K = \ker \pi$ since $K \leq \mathbb{Z}^n$, there is a basis $\{x_1, \ldots, x_n\}$ for $\mathbb{Z}^n$ such that $K = \langle d_1 x_1, \ldots, d_r x_r \rangle$, $d_r \in \mathbb{N}$, $r \leq n$.

Now $G \simeq \mathbb{Z}^n / K \simeq \oplus_{x \in X} \mathbb{Z}/d_i\mathbb{Z}$, with $d_i = 0$ if $i > r$.

If $d_i = 0$, then $\mathbb{Z}/d_i\mathbb{Z} \simeq \mathbb{Z}$, if $d_i = 1$, then $\mathbb{Z}/d_i\mathbb{Z} \simeq \{0\}$.

Let $m_1, \ldots, m_t$ in order be the number of $d_i > 1$.

Then $G \simeq \mathbb{Z}^s \oplus \mathbb{Z}/m_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_t\mathbb{Z}$. □

Corollary 2.6. *$\mathbb{Z}/m\mathbb{Z} \simeq \oplus \mathbb{Z}/p_i^{n_i}\mathbb{Z}$, where $m = \prod p_i^{n_i}$*

Corollary 2.7. *Any finitely generated abelian group is isomorphic to $\mathbb{Z}^s \oplus \bigoplus_{i=1}^{t} \mathbb{Z}/q_i\mathbb{Z}$ with $s \geq 0$ and $q_i = p_i^{n_i}$ for p_i prime.*

Definition 2.2 (Group Action)**.** *The action of a group G on a set X is a function $G \times X \to X : (g, x) \mapsto g \cdot x$ such that*

1. *$e \cdot x = x$ for all $x \in X$.*
2. *$(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$*

We say that G acts on X.

Example: Let G be a group. G acts on G by left multiplication and by right multiplication by inverses, and also by conjugation.

Definition 2.3 (Orbits)**.** *The orbit of $x \in X$ is $G \cdot x = \{g \cdot x : g \in G\}$.*

Note, if $y \in G \cdot x$ then $G \cdot x = G \cdot y$.

The orbits partition X.

Definition 2.4 (Transitive Action)**.** *We say that G acts on X transitively if $G \cdot x = X$ for any $x \in X$.*

Definition 2.5 (Conjugacy Classes)**.** *The conjugacy classes of a group G are the orbits of G acting on itself by conjugation.*

Definition 2.6 (Stabilizer Subgroup)**.** *The stabilizer of $x \in X$ is $G_x = \{g \in G : g \cdot x = x\}$. This is also called the isotropy subgroup.*

Lemma 2.8. $|G \cdot x = [G : G_x]$

Proof. $[G : G_x]$ is the number of left cosets of G_x.

Let $f : gG_x \mapsto g \cdot x$. To check that f is well defined, we need to check that if $gG_x = hG_x$ then $g \cdot x = h \cdot x$.

$gG_x = hG_x$ implies $g^{-1}h \in G_x$. Thus, $(g^{-1}h) \cdot x = x$ so $h \cdot x = (gg^{-1})h \cdot x = g(g^{-1}h) \cdot x = g \cdot x$

Now we must check that it is a bijection.

If $g \cdot x = h \cdot x$ then $g^{-1}h \cdot x = x$. So $g^{-1}h \in G_x$ so $gG_x = hG_x$, thus f is injective.

If $g \cdot x \in G \cdot x$ then $gG_x \mapsto g \cdot x$ and so f is surjective. □

Definition 2.7 (Center of G)**.** *The center of G is $C(G) = \{g \in G : gh = hg \ \forall h \in G\}$.*

Definition 2.8 (Centralizer of x in G)**.** *The Centralizer of x in G is $C_G(x) = \{g \in G : gx = xg\}$*

Corollary 2.9. *1. The number of elements in the conjugacy class of $x \in G$ is $[G : C_G(x)]$. If $|G| < \infty$ then the size of a conjugacy class divides $|G|$.*

2. If $x_1, \ldots, x_k$ are distinct conjugacy class representatives, then $|G| = \sum_{i=1}^{k} [G : C_G(x_i)] = |C(G)| + \sum_{x_i \notin C(G)} [G : C_G(x_i)] = |C(G)| + \sum_{x \notin C(G)} \frac{[G:C_G(x)]}{|G \cdot x|}$

Corollary 2.10. *If G has order p^n then the center of G is nontrivial.*

Proof. $|G| = |C(G)| + \sum_{x_i \notin C(G)} [G : C_G(x_i)]$, and p divides $|G|$ and p divides $[G : C_G(x_i)]$, thus $p|C(G)$. □

Definition 2.9. $X^g = \{x : g \cdot x = x\}$

$X^H = \cap_{h \in H} X^h$, $H < G$.

Lemma 2.11 (Burnside's Lemma)**.** *Let G be a finite group acting on a finite set X. Then the number of orbits is $\frac{1}{|G|} \sum_{g \in G} |X^g|$*

Proof. $\sum_{g \in G} |X^g|$ = the number of pairs $\{(g, x) : g \cdot x = x\} = \sum_{x \in X} |G \cdot x| = \sum_{x \in X} \frac{|G|}{|G \cdot x|} = |G| \sum_{x \in X} \frac{1}{|G \cdot x|}$

$= |G| \sum_A$ `an orbit` $\sum_{x \in A} \frac{1}{|A|} = |G| \sum_A$ `an orbit` 1, which is $|G|$ times the number of orbits. □

The above lemma is often referred to as Burnside's Lemma or "The Lemma which is not Burnside's", as it was discovered in 1900 by Burnside, 1845 by Cauchy, and in 1887 by Frobenius.

Theorem 2.12. *Let G act on a set X. Then there is a unique corresponding homomorphism $\tau : G \to \mathrm{Sym}(X) = S_X = \mathrm{Aut}(X)$ sending g to τ_g, where $\tau_g(x) = g \cdot x$.*

Corollary 2.13. *1. G acts on itself by conjugation. Therefore, conjugation by g is an automorphism.*

2. $\tau : G \to \mathrm{Aut}\, G : g \mapsto \tau_g$ such that $\tau_g(h) = ghg^{-1}$ is a homomorphism with $\ker \tau = C(G)$.

Definition 2.10 (Inner Automorphisms)**.** *We define an automorphism to be an inner automorphism if it is in $\mathrm{Im}(\tau)$. That is, it is the set of all automorphisms induced by conjugation. We will denote it by $\mathrm{Inn}(G)$.*

Lemma 2.14. $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Proof. Set $\tau_g(h) = ghg^{-1}$
Let $\varphi \in \mathrm{Aut}\, G$. We must check that $\varphi\tau_g\varphi^{-1}$ is again conjugation. Let $h \in G$.
$\varphi(\tau_g(\varphi^{-1}(h))) = \varphi(gkg^{-1})$ where $k = \varphi^{-1}(h)$.
This is, then, $\varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)h\varphi(g)^{-1} = \tau_{\varphi(g)}(h)$. □

Definition 2.11 (Outer Automorphisms)**.** *We define an outer automorphism to be an element of* $\mathrm{Out}G = \mathrm{Aut}\, G/\mathrm{Inn}G$.

Definition 2.12 (Semidirect Product)**.** *Let G, H be groups and $\tau : H \to \mathrm{Aut}\, G$ a homomorphism.*

Then we define a new group, X with set $G \times H$ and multiplication $(g, h)(g', h') = (g\tau_h(g'), hh')$. We write $X = G \rtimes_\tau H$

Theorem 2.15. *$G \rtimes_\tau H$ is a group and $(G, 1) \simeq G \trianglelefteq G \rtimes_\tau G$*

Definition 2.13. *Let G act on a set S. Then $S_0 = \{x \in S : hx = x, \forall h \in G$*

Lemma 2.16. *If G acts on a finite set S and $|G| = p^n$, p prime, then $|S| \equiv |S_0|$ mod p.*

Proof. $S = S_0 \cup G \cdot x_1 \cup \ldots \cup G \cdot x_r$ where the x_r are such that $|G \cdot x_i| > 1$
Now $|G \cdot x_i| = [G : G_{x_i}]$ so $1 < |G \cdot x_i|$ divides $|G| = p^n$. So p divides $|G \cdot x_i|$.
Thus, $|S| \equiv |S_0|$ mod p. □

Theorem 2.17 (Cauchy)**.** *If p prime divides $|G|$, then G has an element of order p.*

Proof. Consider $S = \{(a_1, \ldots, a_p) : a_1 a_2 \ldots a_p = e\}$
Let $\mathbb{Z}_p$ act on S by $k \cdot (a_1, \ldots, a_p) = (a_{k+1}, \ldots, a_p, a_1, \ldots, a_k)$
$\mathbb{Z}_p$ maps S to S as $a_1 \ldots a_p = e \Rightarrow a_2 \ldots a_p = a_1^{-1}$.
Thus, $S_0 = \{(a, \ldots, a) : a^p = e\}$. $|S_0| \geq 1$, as $(e, \ldots, e) \in S_0$.

By the lemma, $|S_0| \equiv |S| \mod p$.

$|S| = |G|^{p-1} \equiv 0 \mod p$

As $S_0 \neq \emptyset$, we have that $|S_0| = np$ for $n > 0$. Thus, $\exists a \neq e$ such that $a^p = e$. $|a| = p$ as p is prime. □

Definition 2.14 (p-groups)**.** *A group in which every element has order a power of p, p prime, is called a p-group.*

Theorem 2.18. *If $|G| < \infty$, then G is a p-group iff $|G| = p^n$ for some n.*

Proof. Necessary by Cauchy, Sufficient by Lagrange. □

Definition 2.15 (Normalizer)**.** *The normalizer of a subgroup H of G is $N_G(H) = \{g \in G : gHg^{-1} = H\}$. This is, in fact, a subgroup containing H, and if $N_G(H) = G$ then $H \trianglelefteq G$.*

Lemma 2.19. *If H is a p-subgroup of a finite group G then $[N_G(H) : H] \equiv [G : H] \mod p$*

Proof. Let S be the set of left cosets of H in G. H acts on S by left translation, $h \cdot aH = haH$.

$|S| = [G : H]$.

$xH \in S_0 \iff hxH = xH \forall h \in H \iff x^{-1}hxH = H \forall h \in H \iff x^{-1}Hx = H \iff x \in N_G(H)$

$|S_0| = [N_G(H) : H]$

By the lemma and the fact that $|H| = p^n$ and H acts on S we have $|S| \equiv |S_0| \mod p$.

So $[G : H] \equiv [N_G(H) : H] \mod p$. □

Corollary 2.20. *If H is a p-subgroup of G such that $p|[G : H]$ then $N_G(H) \neq H$.*

Proof. $0 \equiv [G : H] \equiv [N_G(H) : H] \geq 1$.

So $[N_G(H) : H] \geq 1$, thus $N_G(H) \neq H$. □

Definition 2.16 (Sylow p-subgroup)**.** *If p is prime, then a Sylow p-subgroup of G is a maximal p subgroup of G. That is, if $P \leq H \leq G$ and $|H| = p^n$ and P is a Sylow p-subgroup, then $H = P$.*

Theorem 2.21 (First Sylow Theorem)**.** *Let G be a group of order $p^n m$, $m \geq 1$ and $(p, m) = 1$. Then G contains a subgroup of order p^i for $1 \leq i \leq n$ and each subgroup of size p^i $i < n$ is normal in a subgroup of size p^{i+1}.*

Proof. By induction on i. Cauchy is the base case.

Suppose H is a subgroup of G of order p^i, $i < n$. Then $[G : H] = \frac{|G|}{|H|}$, so $p|[G : H]$. Thus $N_G(H) \neq H$.

$1 < |N_G(H)/H| = [N_G(H) : H] \equiv [G : H] \equiv 0 \mod p$, so p divides $|N_G(H)/H|$ by Cauchy, there is a subgroup $H' \leq N_G(H)/H$ with $|H'| = p$.

Let $K = \{g \in N_G(H) : gH \in H'\} \leq N_G(H) \leq G$

Then $|K| = p^{i+1}$ and $H \trianglelefteq K$. □

Corollary 2.22. *All Sylow p-subgroups have order p^n where $|G| = p^n m$, $(p, m) = 1$*

Theorem 2.23 (Second Sylow Theorem)**.** *If H is a p-subgroup of a finite group G and P is any Sylow p-subgroup, then $\exists x \in G$ such that $H < xPx^{-1}$. In particular, all Sylow p-subgroups are conjugate.*

Note, that if there is exactly one Sylow p-subgroup for some p, then it is normal.

Theorem 2.24 (Third Sylow Theorem)**.** *If G is a finite group and p prime, then the number of Sylow p-subgroups divides $|G|$ and is congruent to $1 \mod p$.*

Corollary 2.25. *If $|G| = p^2q^2$ with p, q prime and $p, p^2 \not\equiv 1 \mod q$ and $q, q^2 \not\equiv 1 \mod p$ then G is abelian.*

Definition 2.17 (Even Permutation)**.** *A permutation τ in $\S_n$ is even if it can be written as a product of an even number of transpositions. Similarly, odd permutations.*

Note: each permutation is either even or odd, not both.

It is based on the effect of τ on $\Delta = \det \begin{bmatrix} 1 & x_1 & \dots & x_1^{n-1} \\ 1 & x_2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \dots & x_n^{n-1} \end{bmatrix} = \prod_{i \le i < j \le n} (x_i - x_j)$.

Then $\tau\Delta = \pm\Delta$

Definition 2.18 (Sign of a Permutation)**.** *The sign of $\tau \in S_n$ is $+1$ is τ is even and -1 is τ is odd.*

Definition 2.19 (Alternating Group)**.** $A_n = \{\tau \in S_n : \tau \text{ is even } \}$.

A_n is a group of order $n!/2$. $A_n = \ker \varphi, \varphi : S_n \to \{\pm 1\}$, so $A_n \trianglelefteq S_n$.

Lemma 2.26. *Let $r \neq s \in [n]$. Then $A_n = \langle (rsk) : 1 \le k \le n, k \neq r, k \neq s \rangle = H$.*

Proof. Assume $n > 3$. Since every element of A_n is a product of an even number of transpositions, we must show that $(ab)(cd), (ab)(ac) \in H$

$(ab)(cd) = (acb)(acd)$, $(ab)(ac) = (acb)$. So just need all three cycles in H. This follows by brute force. □

Corollary 2.27. *If N is a normal subgroup of A_n and N contains a 3-cycle, then $N = A_n$.*

Proof. Suppose $(rsc) \in N$.

$(rsk) = (rs)(ck)(rsc)^2(ck)(rs) = aNa^{-1} \in N$.

So $(rsk) \in N$, for $1 \le k \le n, k \neq r, s$ so $A_n \subseteq N$. Thus $N = A_n$. □

Theorem 2.28. *Let $n \geq 5$. Then A_n is simple.*

Theorem 2.29. *Let N be a proper normal subgroup of A_n. By the corollary, N contains no 3-cycles.*

Proof. Suppose that N contains $\pi = c_1 \dots c_k$ disjoint cycles, and c_1 is a cycle of length $r \geq 4$. Write $c_1 = (a_1, \dots, a_r)$.

Let $\delta = (a_1 a_2 a_3) \notin N$.

$\pi = c_1\tau$, $\tau = c_2 \dots c_k$.

So $\pi^{-1}(\delta\pi\delta^{-1}) \in N$, as N is normal.

But $\pi^{-1}(\delta\pi\delta^{-1}) = \tau^{-1}(a_1 a_r a_{r-1} \dots a_2)(a_1 a_2 a_3) = (a_1 a_3 a_r)$.

Suppose $\pi \in N$, $\pi = c_1 \dots c_k = c_1 c_2 \tau$ where c_1, c_2 are 3-cycles.

$c_1 c_2 = (a_1 a_2 a_3)(a_4 a_5 a_6)$, $\delta = (a_1 a_2 a_4)$.

$\pi^{-1}(\delta\pi\delta^{-1}) \in N$, and equals $(a_1 a_4 a_2 a_6 a_3)$, which reduces to the last case.

Thus, every element of N is a product of at most 1 3-cycle and a bunch of transpositions.

Now, if $\pi = (a_1 a_2 a_3)\tau \in N$, with $\tau =$product of disjoint transpositions.

$\pi^2 = (a_1 a_2 a_3)\tau(a_1 a_2 a_3)\tau = (a_1 a_2 a_3)^2 = (a_1 a_3 a_2)$.

So every element of N is a product of disjoint transpositions.

Finally, choose $\sigma \in N$ with $\sigma = (a_1 a_2)(a_3 a_4)\tau$, $\delta = (a_1 a_2 a_3)$

So $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$ is equal to $(a_1 a_3)(a_2 a_4) = \sigma'$.

Since $n \geq 5$, $\exists b$ such that $b \notin \{a_1, a_2, a_3, a_4\}$, $\pi = (a_1 a_2 b)$.

$\sigma'(\pi\sigma'\pi^{-1}) \in N$ is $(a_1 a_3 b) \in N$. Thus, there is no proper nontrivial normal subgroup of A_n for $n \geq 5$. □

3 Rings

Definition 3.1 (Ring)**.** *A ring is a nonempty set R together with two binary operations $+, \cdot$ such that*

1. *$(R, +)$ is an abelian group.*
2. *$(ab)c = a(bc)$*
3. *$a(b + c) = ab + ac$ and $(b + c)a = ba + ca$*

If there is an element 1_R such that $a1_R = 1_R a$ for all $a \in R$ then R is a ring with identity.

If $ab = ba$ for all $a, b \in R$ then R is a commutative ring.

Theorem 3.1. *Let R be a ring.*

1. *$0a = a0 = 0 \forall a \in R$*
2. *$(-a)b = a(-b) = -(ab) \forall a, b \in R$*
3. *$(-a)(-b) = ab \forall a, b \in R$*
4. *$(na)b = a(nb) = n(ab) \forall n \in \mathbb{Z} \forall a, b \in R$*

5. $(\sum_{i=1}^{n} a_n)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_i b_j \forall a_i, b_j \in R$.

Definition 3.2 (Zero Divisors)**.** *A nonzero element, a, in a ring R is a left (respectively right) zero divisor if $\exists b \neq 0 \in R$ such that $ab = 0$ (respectively $ba = 0$)*

a is a zero divisor if it is a left and right zero divisor.

WARNING: If R has zero divisors, you cannot automatically cancel multiplication, ie, $ab = ac \not\Rightarrow b = c$

Definition 3.3 (Unit)**.** *An element $a \in R$, R a ring with identity, is a left unit (respectively right) if $\exists c \in R$ such that $ca = 1_R$ (respectively right if $\exists b$ such that $ab = 1_R$).*

The element c can be called the left inverse of a and the element b the right inverse of a.

Note: if b is a left inverse of a and c is a right inverse, then $b = c$.

Theorem 3.2. *The set of units of R form a group under multiplication.*

Definition 3.4 (Ring Homomorphism)**.** *A ring homomorphism is a function $f : R \to S$ such that $f(a) + f(b) = f(a + b)$ and $f(a)f(b) = f(ab)$.*

This is a group homomorphism from $(R, +)$ to $(S, +)$, so $f(0) = 0$. But if R, S have identity, we cannot necessarily say $f(1_R) = 1_S$

We can now define the category of rings. The objects are rings and the morphisms are ring homomorphisms.

We also have the subcategories of rings with identity and commutative rings.

Definition 3.5 (Integral Domain)**.** *If R is a commutative ring with identity and no zero divisors, then R is called an integral domain.*

Definition 3.6 (Division Ring)**.** *A ring R with identity (not 0) where every nonzero element has an inverse is called a division ring.*

Definition 3.7 (Field)**.** *A commutative division ring is a field.*

Theorem 3.3. *No zero divisor is a unit.*

Proof. $ab = 0$, $b = a^{-1}ab = a^{-1}0 = 0$ □

Definition 3.8 (Group Ring)**.** *If R is a ring and G is a group, then $R(G)$ =the set of formal R-linear combinations of group elements with coefficients in R. Addition is componentwise and multiplication is distributive and uses the group law.*

Group Rings are a part of representation theory.

Definition 3.9 (Real Quaternions)**.** *The real quaternions, $\mathbb{H} = \mathbb{R}(Q_8)$*

Definition 3.10 (Endomorphism Ring)**.** *Let A be an abelian group. Then* $\mathrm{End}(A) = \hom(A, A)$ *is a ring with* $(f + g)(a) = f(a) + g(a)$ *as addition and composition of functions as multiplication.*

Definition 3.11 (Ideal)**.** *A subset I of R is a left (right) ideal if it is an additive subgroup and $x \in I$ for all $r \in R$, $x \in I$.*

An ideal I is a left ideal and a right ideal.

Note: If R has 1_R and I contains a unit, then $I = R$.

Theorem 3.4. *If R is a ring and I is an ideal, then the addit*

If R has identity, then so does R/I.

If R is commutative, then so is R/I.

Proof. Need to show that multiplication is well defined. Suppose $a + I = a' + I$ and $b + I = b' + I$.

Then $a' = a + i$ and $b' = b + i'$ for $i, i' \in I$. So $a'b' = ab + ai + bi' + ii' \in ab + I$

Other parts follow from definition. □

Theorem 3.5. *If $f : R \to S$ is a ring homomorphism, then* $\ker f = \{r \in R : f(r) = 0\}$ *is an ideal in R.*

Proof. We know that $\ker f$ is an additive subgroup.

If $x \in \ker f, r \in R$, then $f(rx) = f(r)f(x) = f(r)0_S = 0_S$. □

The converse, that if I is an ideal, then $\pi : R \to R/I : r \mapsto r + I$ is a homomorphism with $\ker \pi = I$ is true.

Theorem 3.6 (First, Second and Third Isomorphism Theorems)**.**

1. *If $f : R \to S$ is a ring homomorphism, then $R/\ker f \simeq \mathrm{Im}\, f$.*
2. *If I, J are ideals of R, then $R/(I \cap J) \simeq (I + J)/J$*
3. *If $I \subseteq J$ are ideals, then J/I is an ideal of R/I and $(R/I)/(J/I) \simeq R/J$*

Lemma 3.7. *I is a left ideal of R iff $\forall a, b \in I, r \in R$ we have $a - b \in I$ and $ra \in I$.*

Lemma 3.8. *If $\{A_i\}_{i \in I}$ are ideals of R, then $\cap A_i$ is an ideal of R.*

Definition 3.12 (Ideal Generated by X)**.** *If $X \subset R$ then the ideal generated b X is the intersection of all ideals in R containing X. We write $\langle X \rangle$.*

Definition 3.13 (PID)**.** *An integral domain where every ideal is generated by one element is a principal ideal domain, or PID.*

Definition 3.14. *If $A, B \subseteq R$ then $AB = \{a_1 b_1 \dots a_r b_r : a_i \in A, b_i \in B\}$*

If A, B are ideals, then $AB \subseteq A \cap B$

Definition 3.15 (Prime Ideal)**.** *An ideal $P \subseteq R$ is prime if $AB \subseteq P \Rightarrow A \subseteq P$ or $B \subseteq P$ for A, B ideals of R.*

Theorem 3.9. *If P is an ideal in a ring R, $P \neq R$ and $\forall a, b \in R$ we have $ab \in P \Rightarrow a \in P$ or $b \in P$ then P is prime.*

If P is prime and R is commutative, then the converse holds.

Proof. Suppose $AB \subseteq P$, $A \not\subseteq P$ for A, B ideals.

Let $a \in A \setminus P$

Then $\forall b \in B$, $ab \in AB \subseteq P$, $a \notin P$ so $b \in P$. Thus, $B \subseteq P$, so P prime.

Let R be a commutative ring. Suppose $ab \in P$, P prime.

Consider $\langle a \rangle, \langle b \rangle$. If R is commutative, $\langle a \rangle \langle b \rangle \subseteq \langle ab \rangle$. As P is prime, $\langle a \rangle \subset P$ or $\langle b \rangle \subset P$, so $a \in P, b \in P$. □

Theorem 3.10. *If R is a commutative ring with identity, $P \subseteq R$ is prime iff R/P is an integral domain.*

Proof. Suppose P is prime, we know that R/P is commutative with identity and $1_R \neq 0$, so it is enough to show that R/P has no zero divisors.

If $(a+P)(b+P) = 0+P$ then $ab+P = 0+P$ so $ab \in P$ and R commutative, $a \in P$ or $b \in P$ so $a + P = 0 + P$ or $b + P = 0 + P$ so R/P has no zero divisors.

Conversely, suppose R/P is an integral domain. Since $0 \neq 1_R + P$, we have $P \neq R$.

If $ab \in P$ then $(a + P)(b + P) = ab + P = 0 + P$ so $a + P$ or $b + P$ is $0 + P$. Thus, P is prime. □

Definition 3.16 (Maximal Ideal)**.** *An ideal M in a ring R is maximal if $M \neq R$ and if $M \subseteq N \subseteq R$, N and ideal implies that $N = M$ or $N = R$.*

That is, M is a maximal element in the poset of proper ideals of R with $I \leq J$ iff $I \subseteq J$.

Theorem 3.11. *If R is a ring with identity, then every ideal $I \subseteq R$ contained in a maximal ideal M.*

Proof. Look at subposets P of proper ideals $J \subseteq R$ with $I \subseteq J$.

Let $I \leq I_1 \leq \ldots$ be a chain in P. Let $J = \cup_{j \geq 1} I_j$. We need to prove that J is a proper ideal.

Let $a, b \in J$. Then $a \in I_i$, $b \in I_j$ for some i, j. We can take $i \leq j$, then $a \in I_j$ as well. Thus, $a - b \in I_j$, and $ra, ar \in I_j$. So J is an ideal.

J is a proper ideal as 1_R is not in J, because $1_R \notin I_j$ for all j.

So J is an upper bound for the chain. By Zorn's Lemma, we know that P has a maximal element, which is a maximal ideal containing J. □

Theorem 3.12. *If R is a commutative ring with identity, then every maximal ideal is prime.*

Proof. Suppose M is a maximal ideal, $ab \in M$ but $a, b \notin M$.

Consider $M + \langle a \rangle, M + \langle b \rangle$ the $M + \langle a \rangle = M + \langle b \rangle = R$.

As $\langle a \rangle \langle b \rangle \subseteq \langle ab \rangle \subseteq M$ so that $R = (M + \langle a \rangle)(M + \langle b \rangle) = MM + \langle a \rangle M + M \langle b \rangle \langle a \rangle \langle b \rangle \subseteq M$, so $M = R$, contradiction. □

Theorem 3.13. *Let M be an ideal in R, a ring with identity.*
IF M is maximal, R commutative, then R/M is a field.
If R/M is a division ring, then M is maximal.

Proof. R/M is an integral domain. so it is enough to show that all nonzero elements have inverses.

Consider $a + M \in R/M$, where $a \notin M$.

Consider $\langle a \rangle + M$. As M maximal, $\langle a \rangle + M = R$.

So $1_R = ra + m$ for $m \in M, r \in R$.

So $ra - 1_R \in M$, thus $ra + M = 1_R + M$. Thus, $(r + M)(a + M) = 1_R + M$. So R/M is a field.

Assume that R/M is a division ring. Then for $a \notin M$, $\exists r$ such that $(a + M)(r + M) = 1_R + M$, and so $ar - 1_R \in M$.

Suppose M not maximal, so $\exists N$, $M \subsetneq N \subsetneq R$.

If we choose $a \in N$, then $ar - 1_R \in M \subseteq N$ so $1_R \in N$, thus $N = R$, contradiction, so M is maximal. □

In the category of rings, products exist.

Let $P = \prod A_i$ as additive groups, with product $(a_i)(b_i) = (a_i b_i)$, that is, componentwise.

Theorem 3.14 (Chinese Remainder Theorem)**.** *If $A_1, \ldots, A_n$ are ideals in R, a ring with identity, such that $A_i + A_j = R$ for all $i \neq j$, Then $R/(\cap A_i) = \prod R/A_i$*

Lemma 3.15. *If $R^2 = R$ (such as when R is a ring with identity) then M a maximal ideal implies that M is a prime ideal.*

Proof. Suppose that M is maximal, and that A, B are ideals such that $AB \subseteq M$ but $A \not\subset M$ and $B \not\subset M$.

Let $a \in A \setminus M$ and $b \in B \setminus M$.

Consider $M + \langle a \rangle = \{m + r : m \in M, r \in A\}$. As M is maximal, $M + \langle a \rangle = M + \langle b \rangle = R$.

As $R = R^2 = (M + \langle a \rangle)(M + \langle b \rangle) \subseteq M$ as $(m + r)(m' + s) = mm' + ms + rm' + rs$.

So $R \subseteq M$, thus $R = M$, contradicting M being maximal. □

Definition 3.17 (Divides)**.** *A nonzero element a of a commutative ring R divides $b \in R$ if $\exists x \in R$ such that $ax = b$.*
If $a|b$ and $b|a$ then a and b are associates. Also, $(a) = (b)$.

Theorem 3.16. *If R is an integral domain, then a, b are associates iff $a = br$, r a unit.*

Definition 3.18 (Irreducibles and Primes)**.** *Let R be a commutative ring with identity.*
c is irreducible if c is a nonzero nonunit such that $c = ab \Rightarrow a$ or b is a unit.
p is prime if p is a nonzero nonunit such that $p|ab \Rightarrow p|a$ or $p|b$.

Lemma 3.17. *R is an integral domain.*

1. *p prime iff $\langle p\rangle \neq \langle 0\rangle$ is prime.*
2. *Every prime $p \in R$ is irreducible.*
3. *c is irreducible iff $\langle c\rangle$ is maximal with respect to inclusion among principal ideals.*
4. *If R is a PID then c is prime iff c is irreducible.*
5. *Every associate of an irreducible (or prime) is irreducible (or prime).*

Proof. 1. Suppose p is prime and $ab \in \langle p\rangle$. Then $p|ab$ so $p|a$ or $p|b$, thus $a \in \langle p\rangle$ or $b \in \langle p\rangle$. So $\langle p\rangle$ is prime.

Suppose $\langle p\rangle$ is prime and $p|ab$. Then $ab \in \langle p\rangle$ so $a \in \langle p\rangle$ or $b \in \langle p\rangle$, so $p|a$ or $p|b$.

2. If p prime is equals ab then $p|a$ or $p|b$. WLOG, $p|a$. so $a = pc$. So $p = pcb$, so $cb = 1$.
3. If c irreducible, suppose $\langle c\rangle \subsetneq \langle d\rangle$, $c = de$ for some $e \in R$. As $\langle c\rangle \subsetneq \langle d\rangle$, e not a unit, but c is irreducible, so d is a unit, thus, $\langle d\rangle = R$.
4. Suppose R is a PID. Then irreducible in the PID means maximal ideal, which means prime.
5. If $c = du$ then $\langle c\rangle = \langle d\rangle$.

□

Definition 3.19 (Unique Factorization Domain)**.** *An integral domain R is a unique factorization domain if every nonzero nonunit can be written $a = c_1 \dots c_k$ with c_i irreducible and if $a = c_1 \dots c_k = d_1 \dots d_m$ with c_i, d_j irreducible, then $k = m$ and, up to reordering, c_i, d_i are associates.*

Definition 3.20 (Noetherian Ring)**.** *We say that a ring R is Noetherian if it satisfies the ascending chain condition, that is, $A_1 \subset A_2 \subset \dots$ is an ascending chain of ideals then $\exists n$ such that $A_n = A_m$ for all $m \geq n$.*

Lemma 3.18. *If R is a PID then R is Noetherian.*

Proof. Let $(a_1) \subset (a_2) \subset \dots$ be a chain of ideals. Let $A = \cup_{i\geq 1}(a_i)$.

A is an ideal. As R is a PID, $A = \langle a\rangle$ for some $a \in R$. As $a \in A$, $a \in \langle a_n\rangle$ for some n.

Thus $a \in \langle a_n\rangle \subseteq \langle a_j\rangle$ for $j \geq n$, and $\langle a_n\rangle = A$. □

Theorem 3.19. *If R is a PID then R is a UFD.*

Proof. Let S be the set of nonzero nonunits in R with no irreducible factorization.

Suppose $a \in S$. Consider $\langle a\rangle$ as a is not irreducible, $\exists x \in R$ irreducible such that $a = xa_1$ for some $a_1 \in R$.

So $a_1 \in S$, else a has irreducible factorization. We inductively construct the ascending chain $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \dots$ which contradicts R being Noetherian. So S is empty.

Suppose $a = a_1 \dots a_k = d_1 \dots d_\ell$ with c_i, d_j irreducible. As R a PID, irreducibles are prime.

So c_1 prime, so it must divide d_i for some i. Then $rc_1 = d_i$, but d_i irreducible and c_1 not unit so r is a unit.

So c_1, d_i are associates. Inductively, we obtain uniqueness. □

4 Modules

Definition 4.1 (Module)**.** *Let R be a ring. A Left R-module is an abelian group $(A, +)$ together with a map $R \times A \to A$ written as $(r, a) \mapsto ra$ such that $\forall r, s \in R, a, b \in A$ we have*

1. $r(a + b) = ra + rb$
2. $(r + s)a = ra + sa$
3. $(rs)a = r(sa)$
4. *If 1_R exists, then $1_R a = a$. Sometimes, this is called a Unitary R-module.*

Note, that if $\varphi : S \to R$ is a ring homomorphism then every R-module is also an S-module by $sa = \varphi(s)a$.

Definition 4.2 (R-module homomorphism)**.** *A function $f : A \to B$ where A, B are R-modules is an R-module homomorphism if $f(a + b) = f(a) + f(b)$ and $f(ra) = rf(a)$.*

This defines the category of R-modules.

Definition 4.3 (R-submodule)**.** *Let R be a ring and A and R-module. Then $B \subseteq A$ is an R-submodule if $B < A$ and $rb \in B$ for all $r \in R, b \in B$.*

Note, that if $f : A \to B$ is an R-module homomorphism, then $\ker f$ is a submodule of A.

Lemma 4.1. *If B is an R-submodule of an R-module A, then the group A/B is an R module via $r(a + B) = ra + B$.*

Theorem 4.2 (Isomorphism Theorems)**.** *As for groups and rings, we have the isomorphism theorems:*

1. *$f : A \to B$ an R-module homomorphism, then $R/\ker f \simeq \operatorname{Im} f$ a submodule of B.*
2. *B, C are R-submodules of A. Then $B/(B \cap C) \simeq (B + C)/C$*
3. *$C \subseteq B \subseteq A$ then $B/C \subseteq A/C$ and $(A/C)/(B/C) \simeq A/B$*

Definition 4.4 (Submodule Generated by X)**.** *Let A be an R-module and $X \subseteq A$ be a subset. Then the submodule of A generated by X is this intersection of all submodules containing X.*

Definition 4.5 (Products)**.** *If $\{A_i\}_{i \in I}$ are R-modules then the group $\oplus A_i$ is an R-module with action $r(a_i) = (ra_i)$. This is a product in the category of R-modules.*

Definition 4.6 (Exact Sequence)**.** *If $f : A \to B$ and $g : B \to C$ are R-module homomorphisms, then the sequence*

$$A \xrightarrow{f} B \xrightarrow{g} C$$

Is exact at B if $\ker g = \operatorname{Im} f$.

A sequence is exact if it exact at each term.

Definition 4.7 (Short Exact Sequence)**.** *A short exact sequence is the exact sequence*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

In any short exact sequence, f is injective and g is surjective.

Lemma 4.3 (Short 5 Lemma)**.** *Let R be a ring and*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

be a commutative diagram with both rows short exact sequences. Then

1. *If α, γ injective then β injective*
2. *If α, γ surjective then β surjective*
3. *If α, γ bijective then β bijective*

Proof. The third part clearly follows from parts 1 and 2.

Part 1: Let $b \in B$ with $\beta(b) = 0$. As $\beta(b) = 0$, $g'(\beta(b)) = 0 = \gamma(g(b))$

As γ is injective, $g(b) = 0$. Also, as $b \in \ker g$, we have $b \in \operatorname{Im} f$, so $b = f(a)$ for some $a \in A$.

$\beta(f(a)) = 0 = f'(\alpha(a))$ as f' is injective, $\alpha(a) = 0$ and as α is injective, $a = 0$.

Thus, $b = f(a) = f(0) = 0$, so β is injective.

Part 2: Let $b' \in B'$. Then consider $g'(b') \in C'$. Since γ is surjective, $g'(b') = \gamma(c)$ for some $c \in C$.

As g surjective, $c = g(b)$ for some $b \in B$. Thus $\gamma(g(b)) = g'(\beta(b)) = g'(b')$. So $g'(\beta(b) - b') = 0$.

Thus $\beta(b) - b' \in \ker g' = \operatorname{Im} f'$, so $\beta(b) - b' = f'(a')$ for some $a' \in A'$.

As α is surjective, $a' = \alpha(a)$ for some $a \in A$. Let $m = b - f(a) \in B$.

Then $\beta(m) = \beta(b) - \beta(f(a)) = \beta(b) - f'(\alpha(a)) = \beta(b) - f'(a') = b'$. □

Theorem 4.4. *Let R be a ring,* $0 \longrightarrow A_1 \longrightarrow B \longrightarrow A_2 \longrightarrow 0$ *be a short exact sequence of R-modules. Then the following are equivalent:*

1. *$\exists R$-mod homomorphism $h : A_2 \to B$ such that $g \circ h = 1_{A_2}$*
2. *$\exists R$-mod homomorphism $k : B \to A_1$ such that $k \circ f = 1_{A_1}$*
3. *The short exact sequence is isomorphic to* $0 \longrightarrow A_1 \xrightarrow{\iota_1} A_1 \oplus A_2 \xrightarrow{\pi_2} A_2 \longrightarrow 0$ *so $B \simeq A_1 \oplus A_2$*

Proof. The first implies the second easily by looking at the diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \longrightarrow & B & \longrightarrow & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1_{A_1}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_{A_2}} & & \\ 0 & \longrightarrow & A_1 & \longrightarrow & A_1 \oplus A_2 & \longrightarrow & A_2 & \longrightarrow & 0 \end{array}$$

If it is an isomorphism (ie, φ is an isomorphism), then we take $h = \varphi \circ \iota_2 \circ 1_{A_2}$ and $k = \pi_1 \circ \varphi$.

For 1 implies 3, we have a module homomorphism $\varphi : A_1 \oplus A_2 \to B$ by $\varphi(a1, a_2) = f(a_1) + h(a_2)$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{\iota_1} & A_1 \oplus A_2 & \xrightarrow{\pi_2} & A_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 1_{A_1}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_{A_2}} & & \\ \text{Consider } 0 & \longrightarrow & A_1 & \xrightarrow{f} & B & \xrightarrow{g} & A_2 & \longrightarrow & 0 \end{array}$$

If this is commutative, then the Short Five Lemma says we are done. For $a \in A_1$, $\varphi(\iota_1(a)) = \varphi(a, 0) = f(a) + h(0)$ and $f(1_{A_1}(a)) = f(a)$.

For the other square, $(a_1, a_2) \in A_1 \oplus A_2$ and $1_{A_2}(\pi_2(a_1, a_2)) = a_2$ and $g(\varphi(a_1, a_2)) = g(f(a_1) + h(a_2)) = a_2$, so commutative. □

If a sequence satisfies the above conditions, we say that the sequence splits:

$$\begin{array}{ccccccccc} 0 & \to & A & \to & A & \to & 0 \\ & & \bigoplus & & \bigoplus & & \bigoplus & & \\ & 0 & \to & C & \to & C & \to & 0 & \end{array}$$

From now on, we will assume that rings have identity and that modules are unitary.

Definition 4.8 (Linearly Independent)**.** *A subset X of an R-module is linearly independent if for distinct $x_1, \ldots, x_n \in X$ and $r_i \in R$ then $r_1x_1 + \ldots + r_nx_n = 0 \Rightarrow r_i = 0$ for all i.*

If X is not linearly independent, then it is linearly dependent.

Definition 4.9 (Spans)**.** *If $Y \subseteq A$ generates A as an R-module, then we say Y spans A.*

Definition 4.10 (Basis)**.** *A set B which is linearly independent and spans A is called a basis.*

Theorem 4.5. *Let R be a ring with identity. The following are equivalent on R an R-module.*

1. *F has a nonempty basis*
2. *$F \simeq \sum_{x \in X} R$, the direct sum, all but finitely many terms are zero.*
3. *Let $\iota : X \to F$ be the inclusion map, and given any R-module A and $f : X \to A$ as a map of sets then $\exists! \tilde{f} : F \to A$ an R-module homomorphism such that $\tilde{f} \circ \iota = f$. That is, F is free on X in the category of R-modules.*

Proof. $1 \Rightarrow 2$: Let X be a basis for F. Define $\varphi : \sum_{x \in X} \to F$ by $\varphi((r_x))sum_{x \in X} r_x x$.

This is an R-module homomorphism. As X is linearly independent and spanning φ is an injective and surjective homomorphism, so it is an isomorphism.

$2 \Rightarrow 1$: Let $e_x = (0, \ldots, 1_R, \ldots, 0)$ in the x^{th} coordinate. Then $\{e_x : x \in X\}$ is a basis for $\sum_{x \in X} R$.

$2 \Rightarrow 3$: Let $F \sum_{x \in X} R$. Suppose $f : X \to A$ is a map of sets, A an R-module, and $\iota : X \to F : x \mapsto e_x$. Then $\tilde{f}((r_x)) = \sum_{x \in X} r_x f(a)$.

$3 \Rightarrow 2$: F is free on X. $\sum_{x \in X} R$ is free on X by the above, and so X and $\sum_{x \in X} R$ both free, and so they must be isomorphic, as free objects on a set X are equivalent. □

Corollary 4.6. *Every R-module A is a homomorphic image of a free R-module F and thus isomorphic to $\sum_{x \in X} R/B$ where B is some submodule of $\sum_{x \in X} R/$*

If A is finitely generated, then we can take F to be as well.

Proof. If $(a_i)_{i \in I}$ is a generating set for A, then $f : I \to A : i \mapsto a_i$ gives a map $\tilde{f} : \sum_{x \in X} R \to A$ so $A \simeq \sum_{x \in X} R / \ker f$. □

Note: If F is a free R-module, there can be submodules which are not free R-modules.

However, if R is a division ring, then every submodule of a free R-module is free.

Warning: If X, Y are bases for a free module F then it is possible that $|X| \neq |Y|$

However, if R is a commutative ring or a division ring, then $|X| = |Y|$ necessarily.

Definition 4.11 (Invariant Dimension Property)**.** *Let R be a ring with identity. We say that R has the invariant dimension property if, for any free R-module F then any two basis for F have the same cardinality, called* $\operatorname{rank} F$

Lemma 4.7. *Let R be a ring with identity, I a proper ideal, F a free R-module with basis X and $\pi : F \to F/IF$ the canonical projection. Then F/IF is a free R/I-module with basis $\pi(X)$ and $|\pi(X)| = |X|$.*

Proof. We first show that $\pi(X)$ spans F/IF. Let $u + IF \in F/IF$. Then $u \in F$ so $u = \sum_{x\in X} r_x x$ so $u + IF = \sum_{x\in X} r_x x + IF = \sum(r_x + I)(x + IF) = \sum(r_x + I)\pi(x)$. Thus, $\pi(X)$ spans F/IF.

Now we suppose $\sum_{x\in X}(rx+I)\pi(x) = 0$ So $\sum r_x x + IF = 0$. Then $\sum r_x x \in IF$, so $\sum r_x x = \sum s_j u_j$ where $s_j \in Iu_j \in F$.

X is a basis, so each u_j is a linear combination of elements of X, so $\sum s_j u_j = \sum c_x x$ with $c_x \in I$.

Sp $\sum r_x x = \sum c_x x$ since x is a basis, $r_x = c_x$ for all $x \in X$.

So $r_x \in I$ and thus, $c_x + I = 0 + I$. So $\pi(X)$ is linearly independent, and $x \neq x' \Rightarrow \pi(x) \neq \pi(x')$. Thus $\pi(X)$ is a basis for F/IF over R/I and $|\pi(X)| = |X|$. □

Lemma 4.8. *If $f : R \to S$ is a surjective ring homomorphism, and S has the invariant dimension property, then so does R.*

Proof. $S \simeq R/I$ for some ideal I of R with bases X and Y. Then F/IF is a free S-module with bases $\pi(X)$ and $\pi(Y)$. As S has the invariant dimension property, $|X| = |\pi(X)| = |\pi(Y)| = |Y|$. □

Corollary 4.9. *Every commutative ring has the invariant dimension property.*

Proof. Let M be a maximal ideal. Then R/M is a field, which has the invariant dimension property. Thus R has the invariant dimension property. □

We will now assume R is a PID.

Theorem 4.10. *Let F be a free R-module where R is a PID. Let G be a submodule of F. Then G is a free R-module and* $\operatorname{rank} G \leq \operatorname{rank} F$.

Proof. For $F < \infty$.

Let $X = \{x_1, \ldots, x_n\}$ be a basis for F.

Let F_i be the sub,module generated by $\{x_1, \ldots, x_i\}$.

Let $G_i = G \cap F_i$, note, $G_i \subset G_{i+1}$ and $G_i = G_{i+1} \cap F_i$, $G_n = G$.

Also, $F_{i+1}/F_i \simeq R$ and $G_1 \subset F1 \simeq Rx_i \simeq R$.

So G_1 is isomorphic to an ideal, thus $G_1 = \langle c\rangle = Rc \simeq R$ is $c \neq 0$.

Thus, $G_1 \simeq 0$ or R, so G_1 is free of rank $\leq \operatorname{rank} F$.

Consider $0 \to G_i \to G_{i+1} \to G_{i+1}/G_i \to 0$. Then $G_{i+1}/G_i \simeq G_{i+1}/(G_{i+1} \cap F_i) \simeq (G_{i+1} \cap F_i)/F_i < F_{i+1}/F_i$

So $G_{i+1}/G_i \simeq 0$ or R. By induction, G_i is free of rank less than $\operatorname{rank} F_i = i$.

If $G_{i+1}/G_i = 0$ then $G_{i+1} = G_i$ so done.

If $G_{i+1}/G_i = R$ then $0 \to G_i \to G_{i+1} \to R \to 0$ so $\operatorname{rank} G_{i+1} \leq \operatorname{rank} G_i + 1 \leq i + 1$, so $G = G_n$ has rank $\leq \operatorname{rank} F_n = n$. □

Definition 4.12 (Θ_a)**.** *Let A be a module over an integral domain R. Then for $a \in A$, let $\Theta_a = \{r \in R : ra = 0\}$*

Lemma 4.11. *1. Θ_a is an ideal in R.*

2. $A_t = \{a \in A : \Theta_a \neq 0\}$ is a submodule of A.

3. $\forall a \in A$, $R/\Theta_a = Ra = \{ra : r \in R\}$

Proof. Part 2: Let $a, b \in A_t$. Then $\exists r, s \in R$ such that $ra = sb = 0$. Then $rs(a-b) = rsa - rsb = s0 - r0 = 0$.

And, if $a \in A_t$ with $sa = 0$, $s \neq 0$ then $s(ra) = (sr)a = 0$. So $s \in \Theta_{ra} \neq \{0\}$. So $ra \in A_t$. □

Definition 4.13 (Torsion)**.** *A_t is called the torsion submodule of A. A is called a torsion module if $A = A_t$. A is called torsion free if $A_t = 0$.*

Theorem 4.12. *1. Free modules over integral domains are torsion free*

2. $\exists A$, a torsion free module, which is not free.

Proof. Part 1: Let X be a basis for some free module F. If $f = \sum r_i x_i$ then $rf = \sum rr_i x_i = 0$. Then $rr_i = 0$ for all i, so $r = 0$.

Part 2: $\mathbb{Q}$ as a $\mathbb{Z}$-module. □

Theorem 4.13. *A finitely generated torsion free module A over a PID R is free.*

Proof. Assume $A \neq 0$. Let X be a finite set of generators for A.

If $x \in X$ then $rx = 0 \Rightarrow r = 0$ as A is torsion free.

So $\exists S \subset X$ nonempty which is maximal with respect to $\sum_{x \in S} r_x x = 0 \Rightarrow r_x = 0 \forall x$.

That is, S is maximal with respect to "the submodule of A generated by S is free".

Let $y \in X \setminus S$. Then $\exists r_y, r_x$ and $x \in S$ such that $r_y y + \sum_{x \in S} r x_x = 0$. That is, $r_y y = -\sum_{x \in S} r_x x \in \operatorname{span} S = F$. Note, $r_y \neq 0$, as otherwise $\sum_{x \in X} r_x x = 0$ with some $r_x \neq 0$, contradicting linear independence.

So $ra \in F$ for all $a \in A$.

But consider $\varphi : A \to A : a \mapsto ra$. φ is an R-module homomorphism. Then $\ker \varphi = \{0\}$ as A is torsion free. $\varphi(A) \subseteq F$ is a submodule, so $A \simeq \varphi(A)$ which is a submodule of a free module over of a PID. □

Theorem 4.14. *Let A be a finitely generated module over a PID R. Then $A \simeq A_t \oplus F$ with F free.*

Proof. Let $F = A/A_t$. F is finitely generate if A is.

If $r(a + A_t) = 0$ then $ra \in A_t$., so $s(ra) = 0$ for some $s \neq 0$ in R.

Thus $(sr)a = 0$. so $a \in A_t$ or $sr = 0 \Rightarrow r = 0$ as R integral domain $s \neq 0$.

So F is torsion free, thus, F is free.

$0 \to A_t \to A \to F \to 0$ splits, so $A \simeq A_t \oplus F$. □

Definition 4.14 ($A(p)$)**.** *Let A be a torsion module over a PID R. If $p \in R$ is prime, then $A(p) = \{a \in A : \Theta_a = \langle p^i \rangle$ for some $i \in \mathbb{N}\} = \{a \in A : p^i a = 0$ for some $i \in \mathbb{N}\}$.*

Lemma 4.15. *Let A be a torsion module over a PID R. Then $A(p)$ is a submodule of A for each prime p of R.*

Proof. Let $a, b \in A(p)$, then $p^i a = 0 = p^j b$. WLOG, $i \leq j$. Then $p^j(a-b) = 0$ so $a - b \in A(p)$.

$p^i(ra) = r(p^i a) = ra = 0$ so $ra \in A(p)$. □

Theorem 4.16. *Let A be a torsion R-module, R a PID. Then $A = \sum A(p)$ where the sum is over all distinct primes p. If A is finitely generated, then all but finitely many $A(p)$ are zero.*

Proof. We first show that $a \in A \Rightarrow a_1 + \ldots + a_k$ where $a_i \in A(p_i)$. We write $\Theta_a = \langle r \rangle$.

$r = up_1^{n_1} \ldots p_k^{n_k}$ where p_i prime and $n_i > 0$.

Let $r_i = \frac{r}{p_i^{n_i}}$. Consider $\langle r_1, \ldots, r_k \rangle = \langle d \rangle$ for some $d \in R$.

Then $d | r_i$ for all i, thus d is a unit. Thus, $\langle r_1, \ldots, r_k \rangle = \langle 1_R \rangle = R/$

Thus $1 = s_1 r_1 + \ldots + s_k r_k$ so $a = 1_R a = \sum_{i=1}^k s_i r_i a$

But $p_i^{n_i}(s_i r_i a) = s_i(p_i^{n_i} r_i)$, so $s_i r_i a \in A(p_i)$.

Thus, $a \in A \Rightarrow a = \sum a_i$ with $a_i \in A(p_i)$, p_i prime.

Fix a prime $p \in R$ and let A_1 be the submodule of A spanned by the $A(q)$, $q \neq p$.

Let $a \in A_1 \cap A(p)$. Then $p^i a = 0$ and $a = \sum a_i$, $a_i \in A(p_i)$, $p_i \neq p$

So $\forall i$, $\exists n$ such that $p_i^{n_i} a_i = 0$.

Let $d = \prod_{i=1}^k p_i^{n_i}$, then $da = 0$. Consider $\langle d, p^i \rangle = \langle c \rangle$.

Now $c|d$ and $c|p^i$ so c is a unit. Thus $\langle d, p^i \rangle = \langle 1_R \rangle = R$, so $\exists s, t \in R$ such that $sd + tp^i = 1_R$.

So $a = 1_R a = (sd + tp^i)a = s(da) + t(p^i a) = 0 + 0 = 0$ so $A_1 \cap A(p) = \{0\}$.

Consider the homomorphism $\varphi : \sum A(p) \to A : (a_i) \mapsto \sum a_i$. This is surjective by the first part and injective by the second part, this φ is an isomorphism. □

Lemma 4.17. *Let A be a module over a PID R such that $p^n A = 0$, $p^{n-1} A \neq 0$ for some prime p, $n > 0$. Let $a \in A$ have $\Theta_a = \langle p^n \rangle$, then*

1. *If $A \neq Ra$ then $\exists b \in A$, $b \neq 0$ such that $Ra \cap Rb = \{0\}$*
2. *$\exists$ submodule C of A such that $A \simeq C \oplus Ra$*

Proof. 1. If $A \neq Ra$ then $\exists s \in A \setminus (Ra)$, since $p^n c \in p^n A = 0$, $\exists$ a least $j > 0$ such that $p^j c \in Ra (1 \leq j \leq n)$

So $p^{j-1} c \notin Ra$, $p^j c = r_1 a$ for some $r_1 \in R$, $r_1 = rp^k$ with $k \geq 0$ $p \not| r$

So $k \geq j \geq 1$.

Write $b = p^{j-1} c - rp^{j-1} a$. We will check that $Ra \cap Rb = \{0\}$. Note $b \neq 0$ as $p^{j-1} c \notin Ra$ but $rp^{k-1} a \in Ra$.

Also note that $pb = p^j c - rp^k a = r_1 a - r_1 a = 0$. Suppose $sb \in Ra$ for some $s \in R$, $sb \neq 0$.

Then $pb = 0$ and $sb \neq 0$, so $p \not| s$.

So p^n, s relatively prime, so $\langle p^n, s\rangle = \langle 1_R\rangle$, so $\exists x, y$ such that $yp^n + xs = 1_R$.

$b = 1_R b = sxb + yp^n b = x(sb) \in Ra$. $b = p^{j-1}c - rp^{k-1}a \in Ra$ so $p^{j-1}c \in Ra$ contradiction, so $Ra \cap Rb = \{0\}$.

2. If $A = Ra$ take $C = 0$. If $A \neq Ra$ then let S be the set of all submodules b such that $Ra \cap B = \{0\}$.

   By part 1, we know that S is nonempty, so we order it by $\subseteq$. We claim that S has a maximal element.

   Check that if $\{A_i\}$ is an increasing chain then $\cup A_i$ is a submodule. Apply Zorn's Lemma. So let C be a maximal element of S. Consider A/C.

   So $p^n(A/C) = 0$, thus $p^n(a + C) = 0$ but $p^{n-1}(a + C) \neq C$ as $p^{n-1}a \neq 0$ and $Ra \cap C = \{0\}$

   Apply part 1 to A/C so $A/C \simeq R(a + C)$ or $\exists b + C \neq 0 + C$ such that $R(a + C) \cap R(b + C) = 0 + C$.

   Consider $C' = R(b + C)$. Then $Ra \cap C' = \{0\}$ as $Ra \cap C = \{0\}$ and $R(a + C) \cap R(b + C) = 0 + C$ so $C' \in S$, contradiction. So $A = Ra \oplus C$. □

Theorem 4.18. *Let A be a finitely generated module over a PID R. Then $A \simeq R^k \oplus \bigoplus_{i=1}^{\ell} R/(p_i^{n_i})$, p_i prime and $n_i \in \mathbb{N}$ not necessarily distinct.*

Proof. We know that $A \simeq F \oplus A_t$, with F free and A_t torsion.

$\pi_1 : A \to F$ and $\pi_2 : A \to A_t$. F is generated by π_1(generators of A) and A_t is generated by π_2(generators of A). So $F \simeq R^k$. Thus, $A \simeq R^k \oplus A_t$.

We know $A_t = \oplus_{j=1}^{s} A(p_j)$, p_j distinct primes. So again, each $A(p_j)$ is finitely generated. It remains to check that each $A(p_j) \simeq \oplus_{k=1}^{m} R/p_j^{n_k}$. This proof is by induction on the number of generators of $A(p_j)$. If this is one, then $A(p_j) \simeq Rc \simeq R/\Theta_c \simeq R/p_j^n$ for some n.

We suppose that this is true for all cases with generators, that $p_j^n A(p_j) = 0$ and $p_j^{n-1} A(p_j) \neq 0$.

By lemma, $\exists a, C$ such that $A(p_j) \simeq Ra \oplus C$ and C has fewer generators. We can take a to be a generator of $A(p_j)$.

So $C \simeq \oplus_{k=1}^{\ell-1} R/p_j^{n_k}$ and $Ra \simeq R/p_j^n$ so $A(p_j) = \oplus_{k=1}^{\ell} R/p_j^{n_k}$ as required. □

Definition 4.15 (Middle Linear Map)**.** *Let A, B be R-modules, A a right R-module (denoted A_R) and B a left R-module (denoted ${}_R B$). Consider $f : A \oplus B \to C$ a homomorphism of groups such that $f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b)$, $f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2)$ and $f(ar, b) = f(a, rb)$. Then f is said to be middle linear.*

We want to find a module, which we will call $A \otimes_R B$ such that every middle linear map factors through it.

Definition 4.16 (Tensor Product)**.** *Let A_R and ${}_RB$ be R-modules, let F be the free abelian group with basis $A \otimes B$ and let K be the subgroup of F generated by $(a+a',b)-(a,b)-(a',b), (a,b+b')-(a,b)-(a,b'), (ar,b)-(a,rb)$ for each $a,a' \in A, b,b' \in B$*

The quotient group, F/K is called the tensor product and is written $A \otimes_R B$.

The element $(a,b)+K$ is written $a \otimes b$ and $(0,0)+K$ is written as 0.

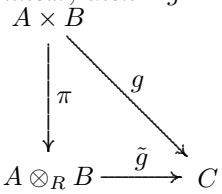
Warning: $A \otimes_R B$ is GENERATED by $\{a \otimes b : a \in A, b \in B\}$, a general element is $\sum n_i(a_i, b_i)$.

Definition 4.17 (S,R-bimodule)**.** *A is an S,R-bimodule if A is a left S-module and a right R-module, and $s(ar) = (sa)r$. We can denote this as ${}_SA_R$*

If B is a left R-module and A is an S,R-bimodule, then $A \otimes_R B$ is a left S-module by $s(a \otimes b) = (sa) \otimes b$.

Let $f : A \times B \to C$ be a middle linear map of groups. Let $\pi : A \times B \to A \otimes_R B : (a,b) \mapsto a \otimes b$. π is middle linear.

Theorem 4.19. *Let A_R and ${}_RB$ be R-modules. If $g : A \times B \to C$ is middle linear, then $\exists! \tilde{g} : A \otimes_R B \to C$ a homomorphism such that $\tilde{g} \circ \pi = g$.*



Proof. Let F be free on $A \times B$. So $\exists! g_1 : F \to C$ homomorphism such that $g_1(a,b) = g(a,b)$. As g is middle linear, and a homomorphism, $K \subseteq \ker g_1$.

Thus $\tilde{g_1} : F/K \to C$ is well defined. $\tilde{g}(a \otimes b) = g(a,b)$. □

In general, if A is a finitely generated abelian group $A \simeq \mathbb{Z}^r \oplus A_t$, then $A \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}^r$, that is, tensor product removes torsion.

Lemma 4.20. *Let $A_R, {}_RB$ be R-modules, R has identity. Then $A \otimes_R R \simeq A$ as right R-modules, $R \otimes_R B \simeq B$ as left R-modules.*

Proof. Let $f : A \times R \to A$ by $(a,r) \mapsto ar$. f is middle linear, so $\exists \tilde{f} : A \otimes_R R \to A : a \otimes r \mapsto ar$

As R is an (R,R)-bimodule, $A \otimes R$ is a right R-module and $\tilde{f}(a \otimes rr') = arr' = (ar)r' = f(a \otimes r)r'$ so $\tilde{f}$ is an R-module homomorphism.

$\tilde{f}$ is surjective, as $\tilde{f}(a \otimes 1_R) = a$. If $\tilde{f}(\sum n_i(a_i \otimes r_i)) = 0 \Rightarrow \sum n_i a_i r_i = 0 \Rightarrow \sum a_i(n_i r_i) = 0$.

Then $\sum n_i(a_i \otimes r_i) = \sum a_i(n_i r_i) \otimes 1_R = (\sum a_i(n_i r_i)) \otimes 1_R = 0 \otimes 1_R = 0$ □

Theorem 4.21. *1.* $\mathbb{Z}[x] \otimes_{\mathbb{Z}} \mathbb{R} \simeq \mathbb{R}[x]$

2. $\mathbb{Z}/m \otimes \mathbb{Z}/n \simeq \mathbb{Z}/(m,n)$

3. *If $A_R, {}_RB_S, {}_SC$ are modules, then $A \otimes_R B$ is a right S-module, $B \otimes_S C$ s a left R-module and $(A \otimes_R B) \otimes_S C \simeq A \otimes_R (B \otimes_S C)$.*

4. *If $\{A_i\}_{i \in I}$ are right R-modules and B is a left R-module, then $(\sum A_i) \otimes_R B \simeq \sum (A_i \otimes_R B)$*

5. *If F, G are free R-modules with bases X and Y respectively, then $F \otimes_R G$ is a free R-module with basis $\{x \otimes y : x \in X, y \in Y\}$.*

6. *If $f : A \to A'$ and $g : B \to B'$ are R-module homomorphisms, then $\exists!$ group homomorphism $A \otimes_R B \to A' \otimes_R B'$ denoted $f \otimes g$ such that $f \otimes g(a \otimes b) = f(a) \otimes g(b)$.*

7. *Tensor product is right exact. That is, if D is an R-module, R commutative and $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact, then $A \otimes D \xrightarrow{f \otimes 1} B \otimes D \xrightarrow{g \otimes 1} C \otimes D \to 0$ is also.*

Definition 4.18 (k-Algebra)**.** *Let k be a commutative ring with identity 1_k. A k-algebra A is a ring such that $(A, +)$ is a left k-module and $k(ab) = (ka)b = a(kb)$.*

If A is a division ring then we call it a division algebra.

Definition 4.19 (k-algebra Homomorphism)**.** *An algebra homomorphism is a ring homomorphism that is also a k-module homomorphism.*

Definition 4.20 (Subalgebra)**.** *A subalgebra is a subring of A that is a k-submodule of A.*

We now have a category whose objects are k-algebras and whose morphisms are k-algebra homomorphisms. There is also the category of commutative k-algebras.

The subalgebra generated by $X \subseteq A$ is the intersection of all subalgebras containing X.

A is finitely generated if $\exists$ a finite set X such that $\langle X \rangle = A$.

Theorem 4.22. *If A is a finitely generated commutative k-algebra with identity, k a field, then $A \simeq k[x_1, \ldots, x_n]/I$ for some $n \in \mathbb{N}$ and some $I \subseteq k[x]$.*

Proof. If $X \subset A$ then there is a k-algebra homomorphism $f : k[X] \to A : x \mapsto x$.

If A is finitely generated with generating set X then $f : k[X] \to A$ is surjective, as $\operatorname{Im} f$ is a subalgebra of A containing X. So $A \simeq k[X]/\ker f \simeq k[X]/I$ as k-algebras. □

5 Fields and Galois Theory

We know that the solutions to $ax^2 + bx + c = 0$ are $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. There is also a cubic and a quartic formula.

Galois Theory shows that there is no quintic formula.

Field Extensions

Definition 5.1 (Extension Field)**.** *A field F is an extension of a field K iff K is a subfield of F. In this case, we can regard F as a K-vector space. We define $[F : K] = \dim_K F$.*

If $[F : K] < \infty$ we say F is a finite extension. Otherwise we say F is an infinite extension.

For example, as $z \in \mathbb{C}$ an be expressed uniquely as $z = r + is$ with $r, s \in \mathbb{R}$, then $[\mathbb{C} : \mathbb{R}] = 2$.

Proposition 5.1 (Analogue of Lagrange's Theorem)**.** *Suppose that $K \subseteq E \subseteq F$ are field extensions.*

1. *If $\{x_i : i \in I\}$ is a basis of E over K and $\{y_j : j \in J\}$ is a basis of F over E, then $\{x_i y_j : i \in I, j \in J\}$ is a basis of F over K.*
2. $[F : K] = [F : E][E : K]$

Proof. Let $z \in F$, then there exist $\alpha_j \in E$, almost all zero, such that $z = \sum_j \alpha_j y_j$. For each j there exists β_{ji}, almost all zero, such that $\alpha_j = \sum_i \beta_{ji} x_i$. Substituting in, we get $z = \sum_j \sum_i \beta_{ji} x_i y_j$.

Thus, $x_i y_j$, $i \in I, j \in J$ generates F over K as a vector space.

To see that they are independent, suppose $\sum_{i,j} \gamma_{ij} x_i y_j = 0$, where $\gamma_{ij} \in K$, almost all zero. Since $\{y_j : j \in J\}$ are independent over E, for each j, $\sum_i \gamma_{ij} x_i = 0$. Similarly, since $\{x_i : i \in I\}$ are independent over K, we get $\gamma_{ij} = 0$ for all i, j. □

Question: Is the analogue of Cauchy also true? That is, if we've got $[F : \mathbb{Q}] = 10$, we know any K which is an intermediate field must have degree 2 or 5. Can we say that there is an E such that $[E : \mathbb{Q}] = 5$?

Definition 5.2 (Algebraic over K)**.** *Let F be an extension of K. Then $\alpha \in F$ is algebraic over K iff there exists a nonzero polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$. Otherwise, α is transcendental.*

The extension F of K is algebraic iff every $\alpha \in F$ is algebraic over K.

e.g. $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since it is a root of $x^2 - 2 = 0$, while π, e are transcendental over $\mathbb{Q}$.

Proposition 5.2. *If F is a finite extension of K, then F is an algebraic extension of K.*

Proof. Suppose $[F : K] = n$. Let $\alpha \in F$.

Then the elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ can't be distinct and independent over K. Hence, there exist $a_i \in K$ not all zero such that $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$ so α is algebraic over K. □

Remark: As we will soon see, the converse doesn't hold. For example, $\mathbb{Q}(\sqrt{2})(\sqrt{3})\ldots$ is an infinite algebraic extension.

Notation. Suppose F is an extension of K and $S \subseteq F$.

$K[S]$ is the subring of F generated by $K \cup S$.

$K(S)$ is the subfield of F generated by $K \cup S$.

When $S = \{s_1, \ldots, s_t\}$ we will just write $K[s_1, \ldots, s_t]$ and $K(s_1, \ldots, s_t)$.

Suppose now that F is an extension of K and $\alpha \in F$ is algebraic over K. Consider the corresponding ring epimorphism $\varphi : K[x] \to K[\alpha] : f(x) \mapsto f(\alpha)$. $\ker \varphi$ is nontrivial. Since $K[x]$ is a PID, there exists a nonzero polynomial $0 \neq p(x) \in K[x]$ such that $\ker \varphi = (p(x))$

Furthermore, we can assume $p(x)$ is monic, as K is a field. Since $K[x]/(p(x)) \simeq K[\alpha]$ is an integral domain, it follows that $p(x)$ is irreducible. Hence, $(p(x))$ is actually a maximal ideal. Hence $K[x]/(p(x))$ is a field, and so $K[\alpha] = K(\alpha)$.

Definition 5.3. *$p(x)$ is the irreducible polynomial of α over K, denoted by* $\mathrm{Irr}(\alpha, K, x)$.

Continuing out analysis, let $\deg(p(x)) = n$. Then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ are linearly independent over K. If not, then there exist $a_i \in K$ not all zero, such that $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} = 0$, then α is a root of $f(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ so $f(x) \in (p(x))$. This means $p(x) | f(x)$, contradiction.

To see that these elements generate $K(\alpha)$, let $\beta \in K(\alpha)$. Then, there exists a polynomial $f(x) \in K[x]$ such that $\beta = f(\alpha)$. By the division algorithm, there exist $q(x), r(x)$ with $\deg r(x) < n$ such that $f(x) = q(x)p(x) + r(x)$. Thus, $\beta = f(\alpha) = r(\alpha)$ so $\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$ for some $b_i \in K$.

Summing up...

Theorem 5.3. *Suppose α is algebraic over K and that $p(x) = \mathrm{Irr}(\alpha, K, x)$.*

1. $K(\alpha) = K[\alpha]$
2. $K(\alpha) \simeq K[x]/(p(x))$
3. $[K(\alpha) : K] = \deg p(x)$

Definition 5.4 (Finitely Generated Extension)**.** *Let F be an extension of K. Then F is finitely generated over K iff there exist $\alpha_1, \ldots, \alpha_n \in F$ such that $F = K(\alpha_1, \ldots, \alpha_n)$.*

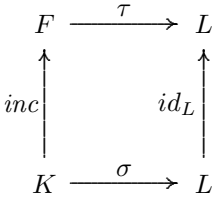
Proposition 5.4. *Let $F = K(\alpha_1, \ldots, \alpha_n)$ be a finitely generated extension of K. If each α_i is algebraic over K, then F is a finite algebraic extension.*

Proof. It is enough to show that $[F : K] < \infty$. Let $K_0 = K$ and $K_i = K(\alpha_1, \ldots, \alpha_i)$. Consider the tower of extensions $K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_N$.

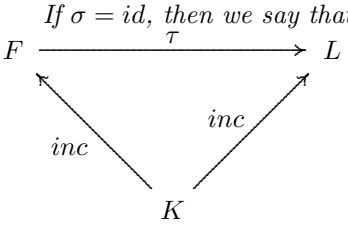
Then $K_{i+1} = K_i(\alpha_{i+1})$ and α_{i+1} is algebraic over K_i. Hence $[K_{i+1} : K_i] < \infty$.

Thus, $[F : K] = [K_n : K_{n-1}] \ldots [K_1 : K_0] < \infty$. □

Definition 5.5. *Suppose that F is an extension of K and let $\sigma : K \to L$ be an embedding of fields. Then an embedding $\tau : F \to L$ extends σ iff the following diagram commutes:*



If $\sigma = id$, then we say that τ is an embedding of F over K.



Definition 5.6. *Suppose that $\sigma : K \to L$ is an embedding of fields. Then we can extend σ to an embedding of the corresponding polynomial rings $\sigma : K[x] \to L[x] : \sum_{i=1}^{n} a_i x^i \mapsto \sum_{i=1}^{n} \sigma(a_i) x^i$. We denote the image of each $f \in K[x]$ by σf.*

Theorem 5.5. *Suppose $\sigma : K \to L$ is an isomorphism of fields and that $f(x) \in K[x]$ is irreducible. Let u, v be roots of $f, \sigma f$ respectively. Then σ extends uniquely to an isomorphism $\tau : K(u) \to L(v)$ such that $\tau(u) = v$.*

Proof. Clearly, there is at most one such map. To see that such an isomorphism exists, note that the isomorphism $\sigma : K \to L$ induces an isomorphism $K[x] \to L[x]$. This map induces an isomorphism $K[x]/(f) \to L[x]/(\sigma f)$.

Recalling the proof of Theorem 1, we can define the desired isomorphism

$K(u) \to K[x]/(f) \to L[x]/(\sigma f) \to L(v)$

$u \mapsto x + (f) \mapsto x + (\sigma f) \mapsto v$ □

Theorem 5.6. *Let $f(x) \in K[x]$ be a polynomial of degree $n \geq 1$. Then there exists an extension $F = K(u)$ satisfying*

1. *$u \in F$ is a root of f*
2. *$[F : K] \leq n$*
3. *If f is irreducible, then $[F : K] = n$ and $F = K(u)$ is uniquely determined up to isomorphism.*

Proof. Let $p(x)$ be a monic irreducible factor of f. Then identify K with the canonical subfield of $K[x]/(p)$, we can take $F = K[x]/(p)$ and $u = x + (p)$. □

Corollary 5.7. *If $f_1, \ldots, f_n \in K[x]$ are nonconstant polynomials, then there exist an extension E of K in which each f_i has a root.*

Definition 5.7 (Algebraically Closed)**.** *The field F is algebraically closed if every nonconstant polynomial $f(x) \in F[x]$ has a root. Equivalently, each nonconstant $f(x) \in F[x]$ splits into a product of not necessarily distinct linear factors.*

Theorem 5.8. *For each field K, there exists an extension L of K such that L is algebraically closed.*

Proof. The theorem is an easy consequence of the following result:

Claim - If E is any field, then there exists an extension F such that each nonconstant $f(x) \in E[x]$ has a root in F.

Assuming the claim, we can complete the proof as follows:

Define inductively a tower of extensions $K = E_0 \subset E_1 \subset \ldots \subset E_n \subset \ldots$ $n \in \mathbb{N}$, such that each nonconstant $f(x) \in E_n[x]$ has a root in E_{n+1}. Clearly, $L = \cup_{n\in\mathbb{N}} E_n$ is an algebraically closed extension of K.

Proof of Claim (E. Artin):

Let $S = \{x_f : f \in E[x] \text{ is a nonconstant polynomial}\}$.

Consider $I = (f(x_f) : x_f \in S)$ of the polynomial ring in infinitely many variables $E[S]$.

Claim: $I \neq E[S]$. Suppose not, then there exists an equality $g_1 f_1(x_{f_1}) + \ldots + g_n f_n(x_{f_n}) = 1$ where $g_i \in E[S]$.

Then, there exist finitely many variables $x_1, \ldots, x_N$ with $n \leq N$ such that each g_i only involves x_1 up to x_N. thus, the equality becomes $\sum_{i=1}^{n} f_i(x_1, \ldots, x_N) f_i(x_{f_i}) = 1$.

Let E' be an extension of E in which each f_i has a root α_i. Let $\alpha_i = 0$ for $n < i \leq N$. Then working in $E'[S]$ and substituting α_i for x_i, we obtain $0 = 1$, the classical contradiction.

Thus, I is a proper ideal. By Zorn's lemma, there exists a maximal ideal M such that $I \subseteq M \subsetneq E[S]$. Thus, $E[S]/M$ is a field in which each nonconstant polynomial $f(x) \in E[x]$ has the root $x_f + M$. Identifying E with the obvious subfield of $E[S]/M$, we are done. □

Definition 5.8 (An Algebraic Closure)**.** *An extension E of K is an algebraic closure if*

1. *E is an algebraic extension of K*
2. *E is algebraically closed.*

Corollary 5.9. *If K is any field, then there exists an algebraic closure K^{alg} of K.*

Proof. Let E be an algebraically closed extension of K.

Define $K^{\text{alg}} = \{\alpha \in E : \alpha \text{ is algebraic over } K\}$

Claim 1: K^{alg} is a field. Let $\alpha, \beta \in K^{\text{alg}}$. Then $K(\alpha, \beta)$ is a finite algebraic extension of K. Since $\alpha - \beta$ and α/β are in $K(\alpha, \beta)$, given $\beta \neq 0$, it follows that $\alpha - \beta$, α/β are in K^{alg}.

Claim 2: K^{alg} is algebraically closed. Let $f(x) \in K^{\text{alg}}[x]$ be a nonconstant polynomial. Let $\alpha \in E$ be a root of f. Let $f(x) = \beta_0 + \beta_1 x + \ldots + \beta_n x^n$ where $\beta_i \in K^{\text{alg}}$. Then $[K(\beta_0, \ldots, \beta_n) : K] < \infty$. Since α is algebraic over $K(\beta_0, \ldots, \beta_n)$, we have $[K(\beta_0, \ldots, \beta_n, \alpha) : K(\beta_0, \ldots, \beta_n)] < \infty$, hence $[K(\beta_0, \ldots, \beta_n, \alpha) : K] < \infty$ and so $\alpha \in K^{\text{alg}}$. □

Theorem 5.10. *If E and E' are algebraic closures of K then E and E' are isomorphic over K.*

We will use:

Lemma 5.11. *Let $\sigma : F \to L$ be an embedding of the field F into the algebraically closed field L. Suppose α is algebraic over F and $f(x) = \mathrm{Irr}(\alpha, F, x)$. Then the number of extensions of σ to an embedding of $F(\alpha)$ into L is equal to the number of distinct roots of σf in L.*

Proof. Let β be any root of σf in L. By Theorem 2, there is a unique embedding $\tau : F(\alpha) \to \tau$ such that $\tau(\alpha) = \beta$.

Conversely, if τ is any embedding extending σ, then $\tau(\alpha)$ must be a root of σf. □

Now, we prove Theorem 5.

Proof. Clearly, Theorem 5 is an immediate consequence of the following (slightly) more general statement. □

Theorem 5.12 (AC)**.** *Suppose E is an algebraic extension of K and that $\sigma : K \to L$ is an embedding into an algebraically closed field L.*

1. *There exists an extension of σ to an embedding of E into L.*
2. *If E is algebraically closed and L is algebraic over $\sigma(K)$ then any such extension is an isomorphism E and L.*

Proof. 1. Let $\mathbb{P}$ be the partially ordered set consisting of all pairs (τ, F) where $K \subseteq F \subseteq E$ is a subfield and $\tau : F \to L$ is an extension of σ ordered by $(\tau, F) \leq (\tau', F')$ iff $F \subseteq F'$ and $\tau'|_F = \tau$.

Then $(\sigma, K) \in \mathbb{P}$ and so $\mathbb{P} \neq \emptyset$.

Suppose that $\{(\tau_i, F_i) : i \in I\}$ is a linearly ordered subset of $\mathbb{P}$. Let $F = \cup_{i \in I} F_i$ and $\tau = \cup_{i \in I} \tau_i$. Then $(\tau, F) \in \mathbb{P}$ and $(\tau_i, F_i) \leq (\tau, F)$ for all $i \in I$.

By Zorn's Lemma, there exists a maximal element (τ, F) of $\mathbb{P}$

Claim: $E = F$.

Suppose not, let $\alpha \in E \setminus F$. Then $\exists$ an extension of τ to the algebraic extension $F(\alpha)$ of F. But this contradicts the maximilaity of (τ, F).

2. Suppose that E is algebraically closed and L is algebraic over $\sigma(K)$. Let $\tau : E \to L$ extend σ. Then $\tau(E)$ is algebraically closed and L is algebraic over $\tau(E)$. Hence, $L = \tau(E)$.

□

Convention: From now on, K^{alg} will denote some fixed algebraic closure of K.

Definition 5.9. *Suppose $K \subseteq E \subseteq K^{\text{alg}}$. Then*

1. *$e_K(E, K^{\text{alg}})$ is the set of embeddings of E into K^{alg} over K.*
2. *$\text{Aut}_K(K^{\text{alg}})$ is the group of automorphisms of the algebraic closure such that $\pi(\alpha) = \alpha$ for all $\alpha \in K$.*

Theorem 5.13. *Suppose that $K \subseteq E \subseteq K^{\text{alg}}$.*

1. *Each $\sigma \in e_K(E, K^{\text{alg}})$ extends to an automorphism $\tau \in \text{Aut}_K(K^{\text{alg}})$.*
2. *If $[E : K] < \infty$ then $|e_K(E, K^{\text{alg}})| \leq [E : K]$.*

Proof. 1. Immediate consequence of Theorem 6.

2. Let $E = K(\alpha_1, \ldots, \alpha_n)$. Consider the tower of extensions $K \subseteq K(\alpha_1) \subseteq \ldots \subseteq K(\alpha_1, \ldots, \alpha_n) = E$.

   Let $K_0 = K$ and $K_i = K(\alpha_1, \ldots, \alpha_i)$. Suppose inductively that $|e_K(K_i, K^{\text{alg}})| \leq [K_i : K]$. Fix some $\sigma \in e_K(K_i, K^{\text{alg}})$. Then the number of ways of extending σ to $K_{i+1} = K_i(\alpha_{i+1})$ is equal to the number r_{i+1} of distinct roots of $\text{Irr}(\alpha_{i+1}, K_i, x)$.

   Hence, $|e_K(K_{i+1}, K^{\text{alg}})| \leq |e_K(K_i, K^{\text{alg}})| r_{i+1} \leq [K_i : K][K_{i+1} : K_i] = [K_{i+1} : K]$.

□

Remark: If $r_i = \deg \text{Irr}(\alpha_i, K_{i+1}, x)$, for $1 \leq i \leq n$ then $|e_K(E, K^{\text{alg}})| = [E : K]$.

Galois Theory

Definition 5.10 (Galois Group)**.** *Let F be a finite extension of K. Then, the corresponding Galois Group is* $\text{Aut}_K(F) = \{\sigma \in \text{Aut}(F) : \sigma|_K = \text{id}_K\}$.

Remark: Clearly, we can suppose that $K \subseteq F \subseteq K^{\text{alg}}$ and so each $\sigma \in \text{Aut}_K(F)$ extends to an automorphism $\tau \in \text{Aut}_K(K^{\text{alg}})$.

Also clearly, $\text{Aut}_K(F) \subseteq e_K(F, K^{\text{alg}})$ and so $|\text{Aut}_K(F)| \leq [F : K]$. In particular, $\text{Aut}_K(F)$ is a finite group.

Basic idea of Galois Theory: The finite group $\text{Aut}_K(F)$ encodes lots of useful information about the extension of F over K.

Counterexamples:

1. Consider $F = \mathbb{Q}(2^{1/3})$ then $2^{1/3}$ is the unique root of $x^3 - 2 = 0$ in F. Hence $\text{Aut}_{\mathbb{Q}}(F) = 1$.
2. Let $K = \mathbb{F}_p(t)$, where t is transcendental over $\mathbb{F}_p$. Let α satisfy $\alpha^p = t$ and consider $F = K(\alpha)$. Since $x^p - t = x^p - \alpha^p = (x - \alpha)^p$, α is the unique root of $x^p - t = 0$ in K and so $\text{Aut}_K(F) = 1$.

The first says that we need to adjoin all the roots of an irreducible equation, the second is also something to be wary of.

Definition 5.11 (Fixed Field)**.** *Let F be a field and let $G \leq \operatorname{Aut} F$. Then the corresponding fixed field of G is $F^G = \{\alpha \in F : \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}$*

Definition 5.12 (Galois Extension)**.** *Let F be a finite extension of K and let $G = \operatorname{Aut}_K(F)$. Then F is a Galois extension of K iff $F^G = K$.*

Clearly, this is an attempt to capture the idea that G is "large" in the sense that it moves as many elements as possible. Another way of capturing this idea would be that $|G| = [F : K]$. Fortunately, we'll eventually see that the two notions coincide.

Example: $F = \mathbb{Q}(\sqrt{2})$ is a Galois Extension of $\mathbb{Q}$ with Galois Group $\operatorname{Aut}_{\mathbb{Q}} F \simeq C_2$

Proof. First note that we can define an automorphism $\sigma \in \operatorname{Aut}_{\mathbb{Q}} F$ by $r+s\sqrt{2} \mapsto r - s\sqrt{2}$ for $r, s \in \mathbb{Q}$. Clearly $\sigma(\alpha) = \alpha$ iff $\alpha \in \mathbb{Q}$. Since $[F : \mathbb{Q}] = 2$, we must have $\operatorname{Aut}_{\mathbb{Q}} F \simeq C_2$. □

Example: Consider the irreducible polynomial $p(x) = x^3 - 2$. Let $\alpha = 2^{1/3}$ and let ω be a primitive third root of unity, ie $\omega \neq 1$ and $\omega^3 = 1$. So $\omega^2+\omega+1 = 0$. Then the roots of $p(x)$ are $\{\alpha, \omega\alpha, \overline{\omega}\alpha\}$. Let $F = \mathbb{Q}(\alpha, \omega\alpha, \overline{\omega}\alpha)$. Then F is a Galois extension of $\mathbb{Q}$ and $\operatorname{Aut}_{\mathbb{Q}} F \simeq S_3$.

Proof. We have already seen that $G = \operatorname{Aut}_{\mathbb{Q}} F \simeq S_3$. To see that $F^G = \mathbb{Q}$ consider the tower of extensions $\mathbb{Q} \overset{3}{\subseteq} \mathbb{Q}(\alpha) \overset{2}{\subseteq} \mathbb{Q}(\alpha, \omega) = F$. Thus $[F : \mathbb{Q}] = 6$. Finally note that if $E = F^G$ then $\mathbb{Q} \subseteq E \subseteq F$ and $6 = |G| \leq |\operatorname{Aut}_E F| \leq [F : E] \leq [F : \mathbb{Q}] = 6$, so all are equal. □

Remark: This argument shows that if $|\operatorname{Aut}_K F| = [F : K]$ then F is a Galois Extension of K.

Open Question: Let G be any finite group. Does there exist a Galois extension F of $\mathbb{Q}$ such that $\operatorname{Aut}_K F \simeq G$.

Remark: We will soon see that if G is any finite group, then there exists a finite extension K of $\mathbb{Q}$ and a Galois Extension F of K such that $\operatorname{Aut}_K F \simeq G$.

We next try to understand which finite extensions are Galois.

$|\operatorname{Aut}_K(E)| \leq |e_K(E, K^{\text{alg}})| \leq [E : K]$. E is Galois if both are equalities. The first will be done with splitting fields/normal extensions, and the second will be done with the number of roots of irreducible equations/separable extensions.

Definition 5.13 (Splitting Field)**.** *Let $\{f_i : i \in I\}$ be a family of nonconstant polynomials in $K[x]$. Then the extension F of K is a splitting field of $\{f_i : i \in I\}$ iff*

1. *Each polynomial f_i splits into a product of linear factors in $F[x]$*
2. *For each i, let R_i be the set of roots of f_i in F. Then $F = K(\cup_i R_i)$*

Example: Using our previous notation, $E = \mathbb{Q}(\alpha, \omega\alpha, \overline{\omega}\alpha)$ is a splitting field of $x^2 - 2 \in \mathbb{Q}[x]$.

Remark: Up to isomorphism, the splitting field of $\{f_i : i \in I\}$ is the subfield of K^{alg} generated by all roots of the f_i in K^{alg}.

Theorem 5.14. *If $K \subseteq E \subseteq K^{\text{alg}}$, then the following are equivalent.*

1. *For all $\sigma \in \text{Aut}_K K^{\text{alg}}$, $\sigma[E] = E$.*
2. *For all $\tau \in e_K(E, K^{\text{alg}})$, $\tau[E] = E$.*
3. *E is the splitting field of a family of polynomials in $K[x]$*
4. *Every irreducible polynomial in $K[x]$ which has a root in E splits into linear factors in $E[x]$.*

Proof. $1 \Rightarrow 2$: Every $\tau \in e_K(E, K^{\text{alg}})$ extends to a $\sigma \in \text{Aut}_K K^{\text{alg}}$.

$2 \Rightarrow 4$: Suppose $p(x) \in K[x]$ is irreducible and $\alpha \in E$ is a root of $p(x)$. Let $\beta \in K^{\text{alg}}$ be any root of $p(x)$. Then the isomorphism $K(\alpha) \to K(\beta)$ extends to an embedding $\tau : E \top K^{\text{alg}}$. Since $\tau[E] = E$, we see that $\beta \in E$. Since E contains the roots of $p(x)$ in K^{alg}, it follows that $p(x)$ splits into linear factors in $E[x]$.

$4 \Rightarrow 3$: Clearly, E is the splitting field of $\{\text{Irr}(\alpha, K, x) : \alpha \in E\}$.

$3 \Rightarrow 2$: Let E be the splitting field of $\{f_i : i \in I\}$. For each $i \in I$, let R_i be the finite set of roots of f_i in E. If $\tau \in e_K(E, K^{\text{alg}})$. Then $\tau[R_i] \subseteq R_i$ and so $\tau[R_i] = R_i$. Since $E = K(\cup_i R_i)$, it follows that $\tau[E] = E$.

$2 \Rightarrow 1$: If $\sigma \in \text{Aut}_K(K^{\text{alg}})$ then $\tau = \sigma|_E \in e_K(E, K^{\text{alg}})$. □

Definition 5.14 (Normal Extension)**.** *The extension E of K is normal iff it satisfies the conditions of Theorem 8.*

Corollary 5.15. *Suppose that $K \subseteq E \subseteq K^{\text{alg}}$ and that E is a normal extension of K. Then if $K \subseteq F \subseteq E$, then E is also a normal extension of F.*

Proof. Take your pick of any condition in Theorem 8. □

Remark: Of course, if $K = \mathbb{F}_p(t)$ and $\alpha = t^{1/p}$, then $E = K(\alpha)$ is a normal extension of K.

We can eliminate this problem as follows:

Definition 5.15 (Separable Polynomial)**.** *An irreducible polynomials $f(x) \in K[x]$ is separable if f has no repeated roots in K^{alg}.*

Theorem 5.16. *If $p(x) \in K[x]$ is irreducible, then the following are equivalent:*

1. *$p(x)$ is separable*
2. *The formal derivative $p'(x) \neq 0$.*

Proof. Reading Exercise, Hungerford III.6.10. □

Let $K = \mathbb{F}_p(t)$ and $f(x) = x^p - t$, then $f'(x) = px^{p-1} = 0$.

Corollary 5.17. *If the characteristic of K is zero, then every irreducible polynomial is separable.*

Definition 5.16 (Separable Extension)**.** *Suppose that $K \subseteq E \subseteq K^{\text{alg}}$.*

1. *The element $\alpha \in E$ is separable over K if $\text{Irr}(\alpha, K, x)$ is separable*
2. *The extension E of K is separable if every $\alpha \in E$ is separable over K.*

Theorem 5.18. *Suppose that $K \subseteq F \subseteq E \subseteq K^{\text{alg}}$.*

1. *If $\alpha \in E$ is separable over K, then α is separable over F.*
2. *If E is a separable extension of K, then E is also a separable extension of F.*

Proof. 1: $\text{Irr}(\alpha, F, x) | \text{Irr}(\alpha, K, x)$.
2: Immediate from 1. □

Theorem 5.19. *If E is a finite extension of K, then the following are equivalent:*

1. *E is a separable extension of K.*
2. *$E = K(\alpha_1, \ldots, \alpha_n)$ where each α_i is separable over K*
3. *$|e_K(E, K^{\text{alg}}) = [E : K]$.*

Proof. $1 \Rightarrow 2$: Utterly obvious.

$2 \Rightarrow 3$: Consider the tower of extensions $K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \ldots, \alpha_n)$. Let $K_0 = K$ and $K_i = K(\alpha_1, \ldots, \alpha_i)$. Suppose inductively that $|e_K(K_i : K^{\text{alg}})| = [K_i : K]$. Let $\tau \in e_K(K_i, K^{\text{alg}})$, then the number of extensions of τ to $K_{i+1} = K_i(\alpha_{i+1})$ is equal to the number of distinct roots r_{i+1} of $\text{Irr}(\alpha_{i+1}, K_i, x)$. Since $\alpha_{i+!}$ is separable over K_{i+1}, we have $r_{i+1} = \deg \text{Irr}(\alpha_{i+1}, K_i, x) = [K_{i+1}, K_i]$ So $|e_K(K_{i+1}, K^{\text{alg}})| = [K_i : K][K_{i=1} : K_i] = [K_{i+1} : K]$.

$3 \Rightarrow 1$: Suppose that E is not a separable extension of K. Choose $\alpha \in E$ such that α is not separable over K. Let $E = K(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1 = \alpha$, then $|e_K(K, K^{\text{alg}})| < [K(\alpha_1) : K]$ and arguing as above, we find $|e_K(K, K^{\text{alg}})| < [E : K]$. □

We can now characterize Galois Extensions

Theorem 5.20. *If E is a finite extension of K, then the following are equivalent:*

1. *E is a Galois Extension of K.*
2. *E is a separable normal extension of K.*
3. *$|\text{Aut}_K(E)| = [E : K]$.*

Proof. $2 \Rightarrow 3$: Since E is normal over K, $e_K(E, K^{\text{alg}}) = \operatorname{Aut}_K E$; and since E is separable over K, $|e_K(E, K^{\text{alg}})| = [E : K]$.

$3 \Rightarrow 1$: Let $G = \operatorname{Aut}_K(E)$ and let $F = E^G$. Then $K \subseteq F \subseteq E$. Also $[E : K] = |G| \leq |\operatorname{Aut}_F E| \leq [E : F] \leq [E : K]$, so $F = K$ thus E is a Galois Extension.

$1 \Rightarrow 2$: Let $G = \operatorname{Aut}_K(E)$, Then $E^G = K$. Let $\alpha \in E$ and let $f(x) = \operatorname{Irr}(\alpha, K, x)$. Let R be the set of roots of $f(x)$ in E. Consider the polynomial $g(x) = \prod_{\beta \in R}(x - \beta)$. Since every $\sigma \in G$ permutes the set R it follows that the coefficients of $g(x)$ are G-invariant. Hence, $g(x) \in K[x]$ and so $f(x)|g(x)$. Also, it is clear that $g(x)|f(x)$. Since both are monic, it follows that $g(x) = f(x)$. In particular, $\operatorname{Irr}(\alpha, K, x)$ is separable and so α is separable over K. Furthermore, $\operatorname{Irr}(\alpha, K, x)$ splits into linear factors in $E[x]$. It follows that E is a normal extension of K. □

Theorem 5.21 (The Fundamental Theorem of Galois Theory)**.** *Let E be a finite Galois Extension of K and let $G = \operatorname{Aut}_K E$ be the Galois Group. Then there exist mutually inverse bijections between $\operatorname{Sub}(G) = \{H | H < G\}$ and $\operatorname{Sub}_K(E) = \{F : F$ is a subfield such that $K \subseteq F \subseteq E\}$ defined by $H \mapsto E^H$ the fixed field, $F \mapsto \operatorname{Aut}_F E$, the corresponding Galois Group. Furthermore*

1. *$H \subseteq H'$ iff $E^H \supseteq E^{H'}$*
2. *If $H \subseteq H'$ then $[H' : H] = [E^H : E^{H'}]$*
3. *If $K \subseteq F \subseteq E$, then F is a Galois Extension of K iff $\operatorname{Aut}_F E \trianglelefteq \operatorname{Aut}_K E$. In this case, $\operatorname{Aut}_K F \simeq \operatorname{Aut}_K E / \operatorname{Aut}_F E$*

We begin the proof of The Fundamental Theorem.

Proof. Suppose F is a subfield with $K \subseteq F \subseteq E$. Then E is also a Galois extension of F. If $H = \operatorname{Aut}_F E$, then $E^H = F$. Thus, $F \mapsto H = \operatorname{Aut}_F E \mapsto E^H = F$. Thus the map $F \mapsto \operatorname{Aut}_F E$ is certainly injective. The surjectivity is an immediate consequence of a result of Artin which will be proved following this.

This result of Artin suggests the following question: What are the finite subgroups of $\operatorname{Aut} \mathbb{C}$?

Continuing with the proof, let $H, H' \leq G = \operatorname{Aut}_K E$. Then there exist corresponding subfields F, F' such that $H = \operatorname{Aut}_F E$ and $H' = \operatorname{Aut}_{F'} E$. Suppose that $H \subseteq H'$. Then clearly $F = E^H \supseteq E^{H'} = F'$.

Conversely, assume $F \supseteq F'$. Then $\operatorname{Aut}_F E \subseteq \operatorname{Aut}_{F'} E$. Thus, (1) holds.

For (2), suppose that $H \subseteq H'$. Recall that $|H| = [E : F]$ and $|H'| = [E : F']$. Thus $[H' : H] = |H'|/|H| = [E : F']/[E : F] = [F : F']$.

For (3), we suppose that $K \subseteq F \subseteq E$. Clearly F is a separable extension of K. Thus, the following are equivalent:

1. F is a Galois extension of K
2. F is a normal extension of K

3. $\sigma[F] = F$ for all $\sigma \in \mathrm{Aut}_K K^{\mathrm{alg}}$

4. $\sigma[F] = F$ for all $\sigma \in \mathrm{Aut}_K E$

Suppose now that F is a Galois extension of K. Then we can define a homomorphism $\mathrm{Aut}_K E \xrightarrow{\pi} \mathrm{Aut}_K F : \sigma \mapsto \sigma|_F$. Clearly $\ker \pi = \mathrm{Aut}_F E \trianglelefteq \mathrm{Aut}_K F$. To see that $\mathrm{Aut}_K F \simeq \mathrm{Aut}_K E / \mathrm{Aut}_F F$ we must show that π is surjective. Let $\tau \in \mathrm{Aut}_K F$.

Then, there exists $\varphi \in \mathrm{Aut}_K K^{\mathrm{alg}}$ such that $\varphi|_F = \tau$. Thus, if $\sigma = \varphi|_E \in \mathrm{Aut}_K E$ we have $\sigma|_F = \tau$ as required.

Finally, suppose that F isn't a Galois extension of K. Then there exists $\sigma \in G = \mathrm{Aut}_K E$ such that $F' = \sigma[F] \neq F$. It is easily checked that $\mathrm{Aut}_{F'} E = \sigma \mathrm{Aut}_F E \sigma^{-1}$. Since $F' \neq F$, $\mathrm{Aut}_{F'} E \neq \mathrm{Aut}_F E$ and so $\mathrm{Aut}_F E$ is not a normal subgroup of $G = \mathrm{Aut}_K E$. □

Lemma 5.22 (Artin)**.** *Let E be any field and let H be a finite subgroup of* $\mathrm{Aut}\, E$*. Let $F = E^H$. Then E is a finite Galois extension of F and $H = \mathrm{Aut}_F E$.*

We shall require the following (interesting) result.

Theorem 5.23 (Primitive Element Theorem)**.** *If E is a finite separable extension of K, then there exists an element $\alpha \in E$ such that $E = K(\alpha)$.*

Proof. First suppose that K is a finite field. Then E is also a finite field and hence E^* is cyclic. Let $\alpha \in E^*$ be a generator, then clearly $E = K(\alpha)$.

Hence, we can suppose that K is infinite. Arguing by induction, it is enough to consider the case when $E = K(\beta, \gamma)$. Let $[E : K] = n$. Since E is a separable extension of K, there exist exactly n distinct embeddings of E into K^{alg}, say $\sigma_1, \ldots, \sigma_n$. Consider the polynomial $f(x) = \prod_{i \neq j}([\sigma_i \beta + x \sigma_i \gamma] - [\sigma_j \beta + x \sigma_j \gamma])$. Then $f(x)$ isn't the zero polynomial, and so has only finitely many roots. Choose some $a \in K$ such that $f(a) \neq 0$. Let $\alpha = \beta + a\gamma$. Then $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ are all distinct. Thus, there are at least n distinct embeddings of $K(\alpha)$ into K^{alg}. So $[K(\alpha) : K] \geq n$ and so $K(\alpha) = E$. □

Corollary 5.24. *Let E be a separable algebraic extension of F. Suppose there exists $n \geq 1$ such that $[G(\alpha) : F] \leq n$ for all $\alpha \in E$. Then $[E : F] \leq n$.*

Proof. Choose $\alpha \in E$ such that $[F(\alpha) : F] = m$is maximal. Suppose there exists $\beta \in E \setminus F(\alpha)$.

Let $\gamma \in F(\alpha, \beta)$ satisfy $F(\gamma) = F(\alpha, \beta)$. Then $[F(\gamma) : F] > m$, contradiction. □

Now we can prove Lemma 2 by Artin.

Proof. Let $\alpha \in E$ and let $\sigma_1, \ldots, \sigma_r \in H$ be a maximal subset such that $\sigma_1(\alpha), \ldots, \sigma_r(\alpha)$ are distinct. Then if $\tau \in H$, by maximality, $\{\tau\sigma_1(\alpha), \ldots, \tau\sigma_r(\alpha)\} = \{\sigma_1(\alpha), \ldots, \sigma_r(\alpha)\}$.

Consider the polynomial $f(x) = \prod_{i=1}^{r}(x - \sigma_i(\alpha))$. Then α is a root of f and $\tau f = f$ for all $\tau \in H$. Hence, the coefficients of f lie in $E^H = F$.

Furthermore, f is separable and splits into linear factors in $E[x]$. Applying Corollary 5, we also see that $[E : F] \leq |H|$.

Thus, E is a finite Galois extension of F. Finally, $|G| \leq |\operatorname{Aut}_F E| = [E : F] \leq |H|$, and so $H = \operatorname{Aut}_F E$ is the Galois group. □

The following easy observation is often useful.

Proposition 5.25. *Assume that F is a finite separable extension of K. Then there exists a finite Galois extension E of K such that $K \subseteq F \subseteq E$.*

Proof. Choose $\alpha \in F$ with $F = K(\alpha)$. Let $f(x) = \operatorname{Irr}(\alpha, F, x)$ and let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x)$ ins F^{alg}. Then $E = K(\alpha_1, \ldots, \alpha_n)$ satisfies our requirements. □

Lemma 5.26. *1. Each positive $r \in \mathbb{R}$ has a square root in $\mathbb{R}$.*

2. If $p(x) \in \mathbb{R}[x]$ has odd degree, then $p(x)$ has a root in $\mathbb{R}$.

3. Each $z \in \mathbb{C}$ has a square root in $\mathbb{C}$.

4. There doesn't exist a field $E \supsetneq \mathbb{C}$ such that $[E : C] = 2$.

Proof. (1) and (2) are the intermediate value theorem, (3) obvious.

(4): Suppose E exists. Then $E = \mathbb{C}(\alpha)$ for any $\alpha \in E \setminus \mathbb{C}$.

Set $f(x) = x^2 + bx + c = \operatorname{Irr}(\alpha, \mathbb{C}, x)$. Then the roots of $f(x)$ are $z = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$, contradiction. □

Theorem 5.27. $\mathbb{C}$ *is algebraically closed.*

Proof. It is enough to show that $\mathbb{C}$ has no proper algebraic extensions. Suppose that F is a finite algebraic extension of $\mathbb{C}$. Then F is a finite separable extension of $\mathbb{R}$ and hence there exists a finite Galois extension E of $\mathbb{R}$ such that $\mathbb{R} \subseteq \mathbb{C} \subseteq F \subseteq E$.

Let $G = \operatorname{Aut}_{\mathbb{R}} E$ be the corresponding Galois group and let $|G| = 2^n m$ where m is odd.

By Sylow, there is a subgroup $H < G$ with $|H| = 2^n$. Let $K = E^H$. Then $[K : \mathbb{R}] = [G : H] = m$. Suppose $m > 1$. Then there exists $\alpha \in K$ such that $K = \mathbb{R}(\alpha)$ and hence $\deg \operatorname{Irr}(\alpha, \mathbb{R}, x) = [K : \mathbb{R}] = m$, which is odd, so it has a root, contradicting irreducibility. So $m = 1$.

Next note that $\mathbb{C}$ is a Galois extension of $\mathbb{R}$, so $\operatorname{Aut}_{\mathbb{R}} \mathbb{C} \simeq \operatorname{Aut}_{\mathbb{R}} E / \operatorname{Aut}_{\mathbb{C}} E$, hence $P = \operatorname{Aut}_{\mathbb{C}} E$ has order 2^{n-1}. We claim that $n = 1$, so that $E = \mathbb{C}$ as required.

We suppose not. By Sylow there exists $N < P$ such that $[P : N] = 2$. Let $K = E^N$, then $[K : \mathbb{C}] = [P : N] = 2$, contradiction. □

Definition 5.17 (Galois Group of a Polynomial)**.** *Let $f(x) \in K[x]$. Then the Galois group of f over K is $\operatorname{Aut}_K E$ where E is the splitting field of f over K.*

Remark: We usually work with separable polynomials, so that E is a Galois extension.

Lemma 5.28. *Let $f(x) \in K[x]$ be a polynomial with Galois group G.*

1. *If $f(x)$ has exactly n distinct roots, in K^{alg}, then G is isomorphic to a subgroup of S_n.*
2. *If $f(x)$ is a separable irreducible polynomial of degree n, then G is isomorphic to a transitive subgroup of S_n.*

Example: Consider $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. By Eisenstein, $f(x)$ is irreducible. Let $\alpha = \sqrt[4]{2}$. Then, the roots are $\pm\alpha, \pm i\alpha$. Letting E be the splitting field of f over $\mathbb{Q}$, we have $E = \mathbb{Q}(\alpha, i)$, so considering $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, i)$ we see that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and $[\mathbb{Q}(\alpha, i) : \mathbb{Q}] = 2$, since $i \notin \mathbb{Q}(\alpha) \subseteq \mathbb{R}$.

Hence $[E : \mathbb{Q}] = 8$. Thus, the Galois Group G of f over $\mathbb{Q}$ satisfies $|G| = 8$ and $G < S_4$, and $|S_4| = 4 \times 3 \times 2$, it follows that G is the Sylow two subgroup of S_4, so $G \simeq \langle (1234) \rangle \rtimes (24)$.

Theorem 5.29. *Suppose p is a prime and that $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial of degree p with exactly 2 nonreal roots in $\mathbb{Q}^{\text{alg}}$. Then, the Galois group of f over $\mathbb{Q}$ is isomorphic to S_p.*

Proof. Let $\alpha_1, \ldots, \alpha_p \in \mathbb{Q}^{\text{alg}}$ be the roots of $f(x)$. then G is isomorphic to a subgroup of $Sym(\{\alpha_1, \ldots, \alpha_p\})$. Since G acts transitively on the roots, $p||G|$ and so G contains a p-cycle. Also, complex conjugation induces a transposition. So, after suitably ordering the roots, we can suppose G contains $\tau = (12)$ and $\sigma = (1i_2 \ldots i_p)$, hence, there exists $1 \leq k \leq p-1$ such that $\sigma^k = (12j_3 \ldots j_p)$, as p is prime.

Thus, again relabeling the roots, we can suppose G contains $\tau = (12)$ and $\sigma = (12 \ldots p)$. So G also contains $\mathscr{O}(12)\mathscr{O}^{-1} = (23)$ and so on. Since G contains $(12), (23), \ldots, (p-1p)$, it follows that $G = S_p$. □

Example: consider $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$. By Eisenstein, $f(x)$ is irreducible. By Calc 1, it is easily checked that $f(x)$ has exactly three real roots. Thus, the Galois group of f over $\mathbb{Q}$ is S_5.

Example: Consider $f(x) = x^5 + 3x + 15 \in \mathbb{Q}[x]$. By Eisenstein, f is irreducible. Then $f(x)$ has exactly one real root. This time, complex conjugation induces a product of two transpositions. So if G is the Galois Group of f over $\mathbb{Q}$, then G contains both a five cycle and a product of two transpositions.

Unfortunately, this still leaves at least three candidates: S_5, A_5, $\langle (12345) \rangle \rtimes \langle (25)(34) \rangle \simeq D_5$

We will use the following, but put off the proof until later:

Theorem 5.30. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial and let p be a prime. Let $\overline{f}(x) = f(x) \pmod{p}$, the polynomial obtained by reducing the coefficients $\bmod p$. Suppose that $\overline{f}(x)$ has no multiple roots in $\mathbb{F}_p^{\text{alg}}$. Then, there exists a bijection $\{\overline{\alpha}_1, \ldots, \overline{\alpha}_n\} \to \{\alpha_1, \ldots, \alpha_n\}$ between the roots of $\overline{f}(x)$ and the roots of $f(x)$ together with an embedding of the Galois group $\overline{G}$ of $\overline{f}$ over $\mathbb{F}_p$ into the Galois group G of f over $\mathbb{Q}$ which gives an embedding of the actions of these groups on the roots.*

Reducing mod 2, we get $\overline{f}(x) = x^5 + x + 1 \in \mathbb{F}_2$. Now working in $\mathbb{F}_2[x]$, we get $x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$. These have no linear factors, and thus are irreducible over $\mathbb{F}_2$. $\overline{f}(x)$ has five distinct roots in $\mathbb{F}_2^{\text{alg}}$. Furthermore, the splitting field of $\overline{f}$ over $\mathbb{F}_2$ is $\mathbb{F}_{2^6}$. Hence, the corresponding Galois group of $\overline{f}$ is $\text{Aut}_{\mathbb{F}_2} \mathbb{F}_{2^6} \simeq C_6$.

Let $\overline{\sigma} \in \text{Aut}_{\mathbb{F}_2} \mathbb{F}_{2^6}$ be a generator. Then $\overline{\sigma}$ permutes the roots of $x^2 + x + 1$ and $x^3 + x^2 + 1$ so is a 2-cycle times a 3-cycle.

Hence, the Galois group G of f over $\mathbb{Q}$ contains an element σ which is a product of a 2-cycle and a 3-cycle. So σ^3 is a transposition, thus $G = S_5$.

Problem: We find an irreducible $f(x) \in \mathbb{Q}[x]$of degree seven with Galois group S_7.

Solution: We claim that the polynomial $\overline{a}(x) = x^5 + x^2 + 1 \in \mathbb{F}_2[x]$ is irreducible. But $\overline{b}(x) = x^2 + x + 1$ is the only irreducible quadratic, and it doesn't divide $\overline{a}(x)$, which has no linear factors.

Consider $\overline{f}(x) = \overline{a}(x)\overline{b}(x) = x^7 + x^5 + x^4 + 1$. The splitting field over $\overline{f}$ is $E = \mathbb{F}_{2^{10}}$. Thus, the Galois Group $\overline{G}$ of $\overline{f}$ over $\mathbb{F}_2$ is cyclic of order 10. Let $\overline{\sigma} \in \overline{G}$ be a generator. Clearly $\overline{\sigma}$ is the product of a 5-cycle and a 2-cycle. Let $f(x) = x^7 + 3x^5 + 3x^4 + 3 \in \mathbb{Q}[x]$.

Let G be the Galois group of f over $\mathbb{Q}$. Then G contains a product σ of a 5-cycle and a 2-cycle. Raise it to the fifth power, and we get a 2-cycle, $\sigma^5 \in G$. As G also contains a 7-cycle, $G \simeq S_7$.

Theorem 5.31. *For each $n \geq 2$, there exists an irreducible poynomail $f(x) \in \mathbb{Q}[x]$ of degree n with Galois group S_n.*

Clearly, we can suppose that $n \geq 4$.

Lemma 5.32. *SUppose the $n \geq 4$ and $G \leq S_n$ satisfies:*

1. *G is transitive*
2. *G contains a $(n-1)$-cycle*
3. *G contains a transposition.*

Then $G = S_n$.

Proof. Let $\Omega = \{1, \ldots, n\}$. Let $\sigma \in G$ be an $(n-1)$-cylce and let $\alpha \in \Omega$ be the fixed point of σ. Then G_α acts transitively on $\Omega \setminus \{\alpha\}$, it follows that for all $\beta \in \Omega$, G_β acts transitively on $\Omega \setminus \{\beta\}$.

This means that G acts 2-transitively on Ω; ie, if $\alpha \neq \beta$, $\gamma \neq \delta$, then there exists $g \in G$ such that $g(\alpha) = \gamma$ and $g(\beta) = \delta$.

Hence, if $\tau \in G$ is a transposition, then we can conjugate τ to any other transposition by a suitable element of G. Since G contains every transposition, $G = S_n$. □

Lemma 5.33. *For each prime p and $d \geq 1$, there exists an irreducible $f(x) \in \mathbb{F}_p[x]$ of degree d.*

Proof. Reading Exercise □

We will now prove the Theorem.

Proof. Let $\overline{a}(x) \in \mathbb{F}_2[x]$ be irreducible of degree $n-1$ and let $\overline{b}(x) = (x+1)\overline{a}(x) = x^n + \overline{b}_{n-1}x^{n-1} + \ldots + \overline{b}_0 \in \mathbb{F}_2[x]$.

Similarly, let $\overline{c}(x) = x^n + \overline{c}_{n-1}x^{n-1} + \ldots + \overline{c}_0 \in \mathbb{F}_3[x]$ be chosen so that it factors as either $\overline{g}(x)\overline{h})(x)$ where $\overline{g}$ is an irreducible quadratic and $\overline{h}$ is irreducible of odd degree or $\overline{g}\overline{h}_1\overline{h}_2$ where $\overline{g}$ is an irreducible quadratic and $\overline{h}_1, \overline{h}_2$ are distinct irreducible of odd degree.

By the Chinese Remainder Theorem, for each $0 \leq i \leq n-1$, there exists $0 \leq \ell_i < G$ such that $\ell_i \equiv \overline{b}_i(\mod 2) \equiv \overline{c}_i(\mod 3)$.

Consider $f(x) = x^n + 7\ell_{n-1}x^{n-1} + \ldots + 7$. By Eisenstein, $f(x)$ is irreducible.

Hence, the Galois group G is transitive. Reducing mod 2, G contains an $n-1$ cycle. Reducing mod 3, we see that G must also contain a transposition. Thus, $G = S_n$. □

Corollary 5.34. *If G is any finite group, then there exists a finite extension K of $\mathbb{Q}$ and a Galois extension E of K such that $G \simeq \mathrm{Aut}_K E$.*

Proof. Let $|G| = n$. By Cayley, we can suppose that $G \leq S_n$. Let $f(x) \in \mathbb{Q}[x]$ be irreducible of degree n with Galois group S_n and let E be the splitting field of $f(x)$.

Then $K = E^G$ satisfies our requirements. □

We will now begin our discussion of Solvable groups and radical extensions. In this section we will study Galois groups of prescribed type: cyclic, abelian and solvable

Definition 5.18 (Cyclic/Abelian Extension)**.** *a finite extension E of K is cyclic/abelian if E is a Galois Extension of K and $\mathrm{Aut}_K E$ is cyclic/abelian.*

Let $\alpha \in \mathbb{Q}^{\mathrm{alg}} \setminus \mathbb{Q}$, and $E \subseteq \mathbb{Q}^{\mathrm{alg}}$ is maximal such that $\alpha \notin E$. Then any finite extension of E is cyclic.

Let K be a field of characteristic $p \geq 0$ and let $n \geq 1$ satisfy $p \not| n$. Then the polynomial $x^n - 1$ has n distinct roots in K^{alg}, since $x^n - 1$ and nx^{n-1} have no common roots. These roots form a finite multiplicative subgroup of $(K^{\mathrm{alg}})^*$ and hence form a cyclic group. A generator of this group is called a primitive n^{th} root of unity.

e.g., working over $\mathbb{Q}$, we have $x^3 - 1 = (x-1)(x^2 + x + 1)$. The primitive 3^{rd} roots of unity are $\frac{-1 \pm \sqrt{-3}}{2}$.

Let α be a primitive n^{th} root of unity. Then if $1 \leq r \leq n$, then α^r is also a primitive root iff $(r, n) = 1$. So there are exactly $\varphi(n)$ primiitive roots of unite. Of course, this is also the order of $\mathbb{Z}_n^*$. If fact, α^r is primitive iff $r \in \mathbb{Z}_n^*$.

Definition 5.19 (Cyclotomic Extension)**.** *With the above hypotheses, the splitting field of $x^n - 1$ over K is called the cyclotomic extension of order n.*

Theorem 5.35. *With the above hypotheses, let F be the cyclotomic extension of order n:*

1. *$F = K(\xi)$, where ξ is any primitive n^{th} root of unity.*
2. *F is an abelian extension of K of dimension d for some $d|\varphi(n)$. Furthermore, if n is prime, then F is a cyclic extension.*
3. *$\mathrm{Aut}_K F$ is isomorphic to a subgroup of order d in $\mathbb{Z}_n^*$.*

Remark: It is possible that $d < \varphi(n)$. For example, let ω be a primitive 5^{th} root of unity. Then $[\mathbb{R}(\omega) : \mathbb{R}] = [\mathbb{C} : \mathbb{R}] = 2$.

Note that $|\mathbb{F}_{2^3}^*| = 7$, hence $\mathbb{F}_{2^3}$ contains a primitive 7^{th} root of unity. In particular, $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ isn't irreducible over $\mathbb{F}_2$.

Proof. Clearly the irreducible factors of $x^n - 1$ are separable and so F is a Galois extension of K. Let $\xi \in F$ be a primitive n^{th} root of unity. Then $F = K(1, \xi, \xi^2, \ldots, \xi^{n-1}) = K(\xi)$. Also, if $\sigma \in \mathrm{Aut}_K F$, then σ is uniquely determined by its value $\sigma(\xi) = \xi^r$. Clearly ξ^r is also a primitive n^{th} root and so $r \in \mathbb{Z}_n^*$. So we obtain an injective homomorphism $\mathrm{Aut}_K F \to \mathbb{Z}_n^* : \sigma \mapsto r$. Hence $\mathrm{Aut}_K F$ is isomorphic to a subgroup of $\mathbb{Z}_n^*$ of order $d|\varphi(n)$. So $\mathrm{Aut}_K F$ is abelian, and cyclic if n is prime, since Z_n is now a field.

Finally, by Galois Theory, $[F : K] = |\mathrm{Aut}_K F| = d$. □

Theorem 5.36. *Let K be a field of $\mathrm{char}\, p \geq 0$ and let $n \geq 1$ with $p \not| n$. Suppose that K contains a primitive n^{th} root of unity. Let $a \in K$ and let α be a root of $x^n - a$. Then $K(\alpha)$ is a cyclic extension of dimension d for some $d|n$. Furthermore, $\alpha^d \in K$. Hence if $b = \alpha^d \in K$ then $\mathrm{Irr}(\alpha, K, x) = x^d - b$.*

Proof. Let $\zeta \in K$ be a primitive n^{th} root of unity. Then $\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha$ are distinct roots of $x^n - \alpha$. If follows that $K(\alpha)$ is a Galois extension of K.

Let $G = \mathrm{Aut}_K K(\alpha)$ be the corresponding Galois group. If $\sigma \in G$, then $\sigma(\alpha) = \omega_\sigma \alpha$ where ω_σ is a not necessarily primitive n^{th} root of unity.

Thus, we obtain an injective homomorphism $\pi : G \to \{\zeta^i : 0 \leq i \leq n-1\} \simeq C_n$. Thus G is cyclic of order d for some $d|n$. Let $\sigma \in G$ be a generator, then $\sigma(\alpha) = \omega_\sigma \alpha$ for some primitive d^{th} root of unity ω_σ.

Furthermore, $\sigma(\alpha^d) = \sigma(\alpha)^d = (\omega_\sigma \alpha)^d = \alpha^d$. Thus, $\alpha^d \in K(\alpha)^G = K$. □

Remark: This theorem no longer holds if K doesn't contain a primitive n^{th} root of unity. eg, consider $x^3 - 2 \in \mathbb{Q}[x]$. Then $\mathbb{Q}(\sqrt[3]{2})$ isn't a Galois extension of $\mathbb{Q}$.

We next work towards

Theorem 5.37. *Let K be a field of $\mathrm{char}\, K = 0$ which contains a primitive n^{th} root of unity. If E is a cyclic extension of K of dimension n, then there exists $\alpha \in E$ such that $E = K(\alpha)$ and α is a root of $x^n - a \in K[x]$.*

Until further notice, we restrict our attention to fields of characteristic zero.

Definition 5.20. *Let K be a field of characteristic zero and let E be a finite extension of K with $[E:K]=n$. Let $e_K(E,K^{\text{alg}})=\{\sigma_1,\ldots,\sigma_n\}$. For each $\alpha\in E$, the corresponding norm is $N_K^E(\alpha)=\sigma_1(\alpha)\ldots\sigma_n(\alpha)$ and the corresponding trace is $\text{tr}_K^E(\alpha)=\sigma_1(\alpha)+\ldots+\sigma_n(\alpha)$.*

Lemma 5.38. *If E is a finite Galois Extension of K and $\alpha\in E$, then*

$$N_K^E(\alpha)=\prod_{\sigma\in\text{Aut}_K\,E}\sigma(\alpha)$$

and

$$\text{tr}_K^E(\alpha)=\sum_{\sigma\in\text{Aut}_K\,E}\sigma(\alpha),$$

and both are in K.

Proof. Under these hypotheses, $e_K(E,K^{\text{alg}})=\text{Aut}_K\,E$. Clearly $N_K^E(\alpha)$, $\text{tr}_K^E(\alpha)$ are fixed by each $\text{Aut}\in\text{Aut}_K\,E$. So $N_K^E(\alpha)$ and $\text{tr}_K^E(\alpha)$ lie in K. □

Lemma 5.39. *Suppose that E is a finite extension of K and $\alpha,\beta\in E$. Then $N_K^E(\alpha\beta)=N_K^E(\alpha)N_K^E(\beta)$ and $\text{tr}_K^E(\alpha+\beta)=\text{tr}_K^E(\alpha)+\text{tr}_K^E(\beta)$.*

Futhermore, if $\gamma\in K$ then $N_K^E(\gamma)=\gamma^{[E:K]}$ and $\text{tr}_K^E(\gamma)=[E:K]\gamma$.

So what is the kernel of $N_K^E:E^*\to K^*$? Well, if $[E:K]=n$, and $\zeta\in K$ is an n^{th} root of unity, then ζ is in the kernel.

Definition 5.21 (Characters)**.** *Let G be a group and let K be a field. Then a character of G is a homomorphism $\chi:G\to K^*$.*

Theorem 5.40 (Artin)**.** *If $\chi_1,\ldots,\chi_n$ are distinct characters of a group G in the field K, then $\chi_1,\ldots,\chi_n$ are linearly independent over K. ie, if $a_1,\ldots,a_n\in K$ are not all zero, then the function $\sum_{i=1}^n a_i\chi_i$ is not identically zero.*

Proof. Suppose not and that $\chi_1,\ldots,\chi_n$ is chosen with n minimal say $a_1\chi_1+\ldots+a_n\chi_n=0$ where $a_1,\ldots,a_n\in k$. Then clearly $n>1$ and each $a_i\neq 0$. Since $\chi_1\neq\chi_2$, there exists a $z\in G$ such that $\chi_1(z)\neq\chi_2(z)$. But we have for all $x\in G$ $a_1\chi_1(zx)+\ldots+a_n\chi_n(zx)=0$ ie, $a_1\chi_1(z)\chi_1+\ldots+a_n\chi_n(z)\chi_n=0$.

Multiplying the original formula by $\chi_1(z)$, we obtain $a_1\chi_1(z)\chi_1+\ldots+a_n\chi_1(z)\chi_n=0$. Subtracting this from the first, we obtian $a_2(\chi_2(z)-\chi_1(z))\chi_2+\ldots+a_n(\chi_n(z)-\chi 1(z))\chi_n=0$. Since $a_2(\chi_2(z)-\chi_1(z))\neq 0$, this contradicts the minimality of n. □

Corollary 5.41. *If K is any field and $\sigma_1,\ldots,\sigma_n\in\text{Aut}\,K$ are distinct, then $\sigma_1,\ldots,\sigma_n$ are linearly independent over K.*

Proof. We regard each σ_i as an isomorphism from K^* to K^*. □

Theorem 5.42 (Hilbert's Theorem 90)**.** *Let K be a field of characteristic zero and let E by a cyclic extension of K of dimension n. Let $\sigma\in\text{Aut}_K\,E$ be a generator. If $\alpha\in E$ then $N_K^E(\alpha)=1$ iff there exists $\beta\in E^*$ such that $\alpha=\beta/\sigma(\beta)$.*

Proof. Let $G = \mathrm{Aut}_K E$ be the cyclic Galois group.

$\Leftarrow$: Suppose there exists $\beta \in E^*$ such that $\alpha = \beta/\sigma(\beta)$. Then

$$N_K^E(\alpha) = N_K^E(\beta)/N_K^E(\sigma(\beta)) = N_K^E(\beta)/N_K^E(\beta) = 1$$

.

$\Rightarrow$: Conversely, suppose that $N_K^E(\alpha) = 1$. To make this proof easier to read, we shall use exponential notation as follows: if $\tau, \sigma \in G$ and $\eta \in E$, then we write η^τ instead of $\tau(\eta)$. Thus $\eta^{\tau+\theta} = \eta^\tau \eta^\theta = \tau(\eta)\theta(\eta)$, etcetera.

In particular, for each $\eta \in E$, $N_K^E(\eta) = \eta^{1+\sigma+\sigma^2+\ldots+\sigma^{n-1}}$. By Artin's Theorem on Characters, the map on E defined by $id + \alpha\sigma + \alpha^{1+\sigma}\sigma^2 + \ldots + \alpha^{1+\sigma+\ldots+\sigma^{n-2}}\sigma^{n-1}$ is not identically zero.

Hence, there exists $\theta \in E$ such that $\theta+\alpha\theta^\sigma+\alpha^{1+\sigma}\theta^{\sigma^2}+\ldots+\alpha^{1+\ldots+\sigma^{n-2}}\theta^{\sigma^{n-1}} \neq 0$. Notice that $\alpha\beta^\sigma = \alpha\theta^\sigma + \alpha^{1+\sigma}\theta^{\sigma^2} + \alpha^{1+\sigma}\theta^{\sigma^3} + \ldots + \alpha^{1+\ldots+\sigma^{n-1}}\theta^{\sigma^n}$. Since $\alpha^{1+\sigma+\ldots+\sigma^{n-1}} = N_K^E(\alpha) = 1$ and $\sigma^n = 1$ we see that $\alpha\beta^\sigma = \beta$, and so $\alpha = \beta/\sigma(\beta)$. □

We can now prove Theorem 21

Proof. Let K be a field of characteristic zero which contains a primitive n^{th} root of unity ζ and let E be a cyclic extension of K of dimension n with Galois group G. Let $\sigma \in G$ be a generator.

Since $[E : K] = n$, we have that $N_K^E(\zeta^{-1}) = (\zeta^{-1})^n = 1$. Hence, by Hilbert's Theorem 90, there exists $\alpha \in K^*$ such that $\zeta^{-1} = \alpha/\sigma(\alpha)$ and so $\sigma(\alpha) = \zeta\alpha$. Since $\zeta \in K$, we have $\sigma^2(\alpha) = \sigma(\zeta\alpha) = \zeta^2\alpha$. Continuing in this fashion, we obtain $\sigma^i(\alpha) = \zeta^i\alpha$ for $1 \leq i \leq n$. Thus $\{\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha\}$ is a set of n distinct elements under the action of G. Hence $[K(\alpha) : K] \geq n$ and so $E = K(\alpha)$.

Also, $\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta\alpha)^n = \alpha^n$. Thus $a = \alpha^n \in E^G = K$. Clearly α is a root of $x^n - a \in K[x]$. □

We continue to work with fields of characteristic zero.

Definition 5.22 (Radical Extension)**.** *An extension F of a field K is a radical extension iff there exists a tower $K \subseteq K(u_1) \subseteq \ldots \subseteq K(u_1, \ldots, u_n) = F$ such that for each $1 \leq i \leq n$, there exists a $d_i \geq 1$ such that $u_i^{d_i} \in K(u_1, \ldots, u_{i-1})$.*

Example: Let $\alpha = \sqrt[4]{2}$ and $i = \sqrt{-1}$ then $\mathbb{Q}(\alpha, i)$ is a radical extension of $\mathbb{Q}$ as $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, i)$.

Definition 5.23 (Solution by Radicals)**.** *Let $f(x) \in K[x]$ and let E be the splitting field of f over K. Then the equation $f(x) = 0$ is solvable by radicals iff there exists a radical extension F of K such that $K \subseteq E \subseteq F$.*

Remark: We have no required that F should be a radical Galois extension, but the next lemma says that we can assume it is also Galois.

Recall that if F is a separable extension of K then there exists a Galois extension E of K such that $E \subseteq F \subseteq E$. In fact, there exists a minimal one called the normal closure.

Lemma 5.43. *If F is a radical extension of K and N is the normal closure of F, then N is also a radical extension of K.*

Proof. Let $F = K(\alpha)$ and let $g(x) = \mathrm{Irr}(\alpha, K, x)$. Then N is the splitting field of $g(x)$ over K. Let $\{\alpha_1, \ldots, \alpha_r\}$ be the distict roots of $g(x)$ in N. Let $K \subset K(u_1) \subset \ldots \subset K(u_1, \ldots, u_n) = F = K(\alpha)$ wirness that F is a radical extnesion of K. For each $1 \leq q \leq r$, let $\sigma_i \in \mathrm{Aut}_K N$ satisfy $\sigma_i(\alpha) = \alpha_i$. Then $K \subset K(\sigma_i(u_1)) \subset \ldots K(\sigma_i(u_1), \ldots, \sigma_i(u_n)) = K(\alpha)$ witnesses that $K(\alpha_i)$ is a radical extension of K. Hence the following tower witnesses that N is a radical extension of K.

$$K \subset K(u_1) \subset \ldots \subset K(u_1, \ldots, u_n) = K(\alpha_1) \subset K(\alpha_1, \sigma_2(u_1)) \subset \ldots \subset K(\alpha_1, \sigma_2(u_1), \ldots, \sigma_2(u_n)) = K(\alpha_1, \alpha$$

$$\ldots \subset K(\alpha_1, \ldots, \alpha_n) = N$$

□

Suppose that K is a field of characteristic zero. We wish to characterize those $f(x) \in K[x]$ which are solvable by radicals. Let E be the splitting field of f and suppose that F is a radical Galois extension such that $K \subseteq E \subseteq F$. Since E is Galois over K, we have $\mathrm{Aut}_K E \simeq \mathrm{Aut}_K F / \mathrm{Aut}_E F$. In particular, $\mathrm{Aut}_K E$ is a homomorphic image of $\mathrm{Aut}_K F$.

Thus, it is enough to understand the structure of $\mathrm{Aut}_K F$. Let $K = K_0 \subset K_1 \subset \ldots \subset K_n = F$ withness that F is a radical extension of K. To simplify matters, suppose that K contains all relevant roots of unity. Then each $K_i \subset K_{i+1}$ is a cyclic extension. IN particular, consider the special case where $K = K_0 \subset K_1 \subset K_2 = F$.

Then $\mathrm{Aut}_{K_0} K_1, \mathrm{Aut}_{K_1} K_2$ are cyclic, $\mathrm{Aut}_{K_0} K_1 \simeq \mathrm{Aut}_{K_0} K_2 / \mathrm{Aut}_{K_1} K_2$. Thus $\mathrm{Aut}_{K_0} K_2$ is an extension of $\mathrm{Aut}_{K_0} K_1$ by $\mathrm{Aut}_{K_1} K_2$, that is, $1 \to \mathrm{Aut}_{K_1} K_2 \triangleleft \mathrm{Aut}_{K_0} K_2 \to \mathrm{Aut}_{K_0} K_1 \to 1$ where the outer pair are cyclic.

Thus, we must study the smallest class of groups $\mathscr{S}$ such that each abelian group is in $\mathscr{S}$ and such that $\mathscr{S}$ is closed under taking extensions and homomorphic images.

Definition 5.24 (Commutator)**.** *Let G be a group. If $a, b \in G$ then the corresponding commutator is $[a, b] = aba^{-1}b^{-1}$.*

The commutator subgroup of G is $G' = \langle [a, b] : a, b \in G \rangle$.

Example: If G is abelian, then $G' = 1$.

Theorem 5.44. *Let G be a group.*

1. *$G' \trianglelefteq G$*
2. *G/G' is abelian*
3. *if $N \trianglelefteq G$, then G/N is abelian iff $G' \leq N$.*

Proof. 1. If $a, b \in G$, and $\pi \in \operatorname{Aut} G$, then $\pi([a,b]) = [\pi(a), \pi(b)]$ Hence $\pi[G'] = G'$. In particular, this is true if π is an inner automorphism, hence, $G' \trianglelefteq G$.

2. Let $a, b \in G$. Since $(ab)(ba)^{-1} = aba^{-1}b^{-1} = [a,b] \in G'$ it follows that $abG' = baG'$, and so G/G' is abelian.

3. Finally, suppose $N \trianglelefteq G$. If $G' \leq N$, then the above argument shows that G/N is abelian. Conversely, suppose that G/N is abelian. Let $a, b \in G$. Since $abN = baN$, it follows that $[a,b] = (ab)(ba)^{-1} \in N$.

□

Examples: Clearly, if S is a simple nonabelian group then $S' = S$. Hence if $n \geq 5$, then $A_n' = A_n$.

Definition 5.25 (Perfect)**.** *G is perfect if $G = G'$.*

Let $n \geq 5$, since $S_n/A_n \simeq \mathbb{Z}_2$ it follows that $S_n' \leq A_n$, since A_n is perfect, it follows that $S_n' = A_n$.

Consider S_3. The normal subgroups of S_3 are 1, A_3, S_3. As S_3 is not abelian, and $S_3/A_3 \simeq \mathbb{Z}_2$, $S_3' = A_3$ and $S_3'' = A_3' = 1$.

The normal subgroups of S_4 are $1, A_4, S_4$ and $V = \{1, (12)(34), (13)(24), (14)(23)\}$. Clearly $1 < V < A_4 < S_4$.

As $S_4/A_4 \simeq \mathbb{Z}_2$, A_4 contains S_4'. Since $[(12),(23)] = (12)(23)(12)^{-1}(23)^{-1} = (13)(23) = (132) \notin V$. So $S_4' = A_4$.

Since $A_4/V \simeq \mathbb{Z}_3$, so $A_4' = V$, and so $V' = 1$. Thus, S_4 is an iterated extension of abelian groups.

Definition 5.26 (Derived Subgroups)**.** *For each $i \geq 0$, the i^{th} derived subgroup $G^{(i)}$ of G is defined by $G^{(0)} = G$ and $G^{(i+1)} = G^{(i)'}$.*

Definition 5.27 (Solvable Group)**.** *G is solvable iff there exists $n \in \mathbb{N}$ such that $G^{(n)} = 1$.*

If G is abelian, then G is solvable. S_4 is solvable. If $n \geq 5$, then S_5 is not solvable.

Theorem 5.45. *1. If G is solvable, then every subgroup of G is solvable, and every homomorphic image of G is solvable.*

2. Suppose G is a group and $N \trianglelefteq G$. If $N, G/N$ are solvable, then so is G.

Proof. 1. First suppose that $H \leq G$. An easy induction shows that $H^{(i)} \leq G^{(i)}$ for all $i \geq 0$. It follows that H is also solvable.

Next suppose that $f : G \to H$ is an epimorphism. An easy induction shows that $f[G^{(i)}] = H^{(i)}$ for all $i \geq 0$. It follows that H is also solvable.

2. Let $f : G \to G/N$ be the canonical surjection. Then there exists $n \geq 0$ such that $f[G^{(n)}] = (G/N)^{(n)} = 1$. Hence $G^{(n)} \leq N$. By the first part, $G^{(n)}$ is also solvable, and hence, there exists $k \geq 0$ such that $G^{(n+k)} = G^{(n)(k)} = 1$.

□

Definition 5.28. *A subnormal series of G is a chain of subgroups $G = G_0 > G_1 > G_2 > \ldots > G_n = 1$ such that $G_{i+1} \trianglelefteq G_i$ for all $0 \leq i \leq n-1$ and the quotients G_i/G_{i+1} are called the factors of the series.*

A subnormal series is a composition series if G_i/G_{i+1} is simple for all $0 \leq i \leq n-1$.

A subnormal series is a solvable series if G_i/G_{i+1} is abelian.

Examples, let $V =< a > \oplus < b >$ where $< a > \simeq < b > \simeq \mathbb{Z}_n$ and let $G = V \rtimes < c >$ where $< c > \simeq C_2$ and $cac^{-1} = b$. Then $G > V > \langle a \rangle > 1$. Note that $< a > \not\trianglelefteq G$.

This is why it is called a subnormal series.

Suppose that G is solvable and n is minimal such that $G^{(n)} = 1$. Then $G = G^{(0)} > G^{(1)} > \ldots > G^{(n)} = 1$. This is actually a normal series, and a solvable series.

"Clearly", every finite group has a composition series. To see this, let G be finite, and inductively let G_{i+1} be a maximal normal subgroup of G_i. This gives a composition series.

Of course, not every group has a composition series. For example, $\mathbb{Z}$, has no such series.

Theorem 5.46. *A group G is solvable iff G has a solvable series.*

Proof. The above shows $\Rightarrow$.

So, we suppose that $G = G_0 > G_1 > \ldots > G_n = 1$ is a solveable series. We claim that $G^{(i)} \leq G_i$ for $0 \leq i \leq n$. Clearly this is true when $i = 0$. Suppose inductively that $G^{(i)} \leq G_i$. Since G_i/G_{i+1} is abelian, it follows that $G^{(i)'} \leq G_{i+1}$, hence, $G^{(i+1)} \leq G_{i+1}$. □

Theorem 5.47. *A finite group G is solvable iff G has a composition series all of whose factors are cyclic of prime order.*

Proof. $\Leftarrow$, by theorem 26.

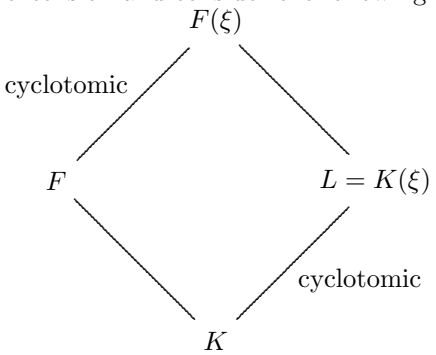
$\Rightarrow$, we have already seen the finite group G has a composition series $G = G_0 > \ldots > G_n = 1$. Since G is solvable, it follows that each factor G_i/G_{i+1} is also solvable. Since G_i/G_{i+1} is simple and abelian, it is $\mathbb{Z}_p$ for some p prime. □

Theorem 5.48. *If K is a field of characteristic zero, and $f(x) \in K[x]$, then the following are equivalent:*

1. *The equation $f(x) = 0$ is solvable by radicals.*
2. *The Galois group of $f(x)$ over K is solvable.*

Proof. 1 $\Rightarrow$ 2: Suppose that $f(x) = 0$ is solvable by radicals. Let E be the splitting field of f over K. Then there exists a radical Galois extension F of K such that $K \subseteq E \subseteq F$. Since $\mathrm{Aut}_K E \simeq \mathrm{Aut}_K F / \mathrm{Aut}_E F$, it is enough to show that $\mathrm{Aut}_K F$ is solvable. Since F is a radical extension of K, there exists a tower $K \subset K(u_1) \subset \ldots \subset K(u_1, \ldots, u_n) = F$ such that for each $1 \leq i \leq n$, there exists $d_i \geq 1$ such that $u_i^{d_i} \in K(u_1, \ldots, u_{i-1})$ Let $d = d_1 \ldots d_n$ and let ξ

be a primitive d^{th} root of unity. Let $L = K(\xi)$ be the corresponding cyclotomic extension and consider the following diagram of extensions.



Then $F(\xi)$ is a Galois extension of K. Since $\mathrm{Aut}_K F \simeq \mathrm{Aut}_K F(\xi)/\mathrm{Aut}_F F(\xi)$, it is enough to show that $\mathrm{Aut}_K F(\xi)$ is solvable. Finally, since $\mathrm{Aut}_K L \simeq \mathrm{Aut}_K F(\xi)/\mathrm{Aut}_L F(\xi)$, it is enough to show that $\mathrm{Aut}_L F(\xi)$ is solvable. Consider the tower of extensions $L \subset L(u_1) \subset \ldots \subset L(u_1, \ldots, u_n) = F(\xi)$.

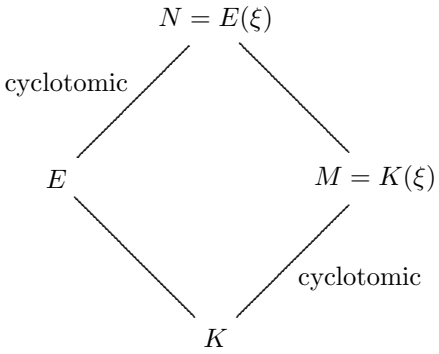
Let $L_0 = L$ and $L_i = L(u_1, \ldots, u_i)$ for $1 \leq i \leq n$. For each $0 \leq i \leq n-1$, L_i contains a primitive d_{i+1}^{th} root of unity and $L_{i+1} = L_i(u_{i+1})$ where $u_{i+1}^{d_{i+1}} \in L_i$. It follows that L_{i+1} is a cyclic extension of L_i, that is, L_{i+1} is a Galois extension of L_i such that $\mathrm{Aut}_{L_i} L_{i+1}$ is cyclic.

Suppose inductively that $\mathrm{Aut}_L L_i$ is solvable. $L \subset L_i \subset L_{i+1}$. Then $\mathrm{Aut}_L L_i \simeq \mathrm{Aut}_L L_{i+1}/\mathrm{Aut}_{L_i} L_{i+1}$. By hypothesis $\mathrm{Aut}_L L_i$ is solvable and $\mathrm{Aut}_{L_i} L_{i+1}$ is cylic, hence $\mathrm{Aut}_L L_{i+1}$ is also solvable. Thus $\mathrm{Aut}_L F(\xi)$ is solvable.

To prove that 2 implies 1, it is enough to prove the following theorem: □

Theorem 5.49. *Suppose K is a field of characteristic 0 and F is a finite Galois Extension of K. If the Galois Group $\mathrm{Aut}_K E$ is solvable, then there exists a radical Galois Extension F of K such that $K \subseteq E \subseteq F$.*

Proof. We argue by induction on $n = [E : K]$, the case $n = 1$ being trivial. Suppose inductively that the result holds for al such extensions $K' \subseteq K'$ with $k = [E' : K'] < n$. Since $G = \mathrm{Aut}_K E$ is a finite solvable group, G has a composition series, all of whose factors are cyclic of prime order. In particular, there exists $H \trianglelefteq G$ such that $[G : H] = p$ for some prime p. Let ξ be a primitive p^{th} root of unity and let $N = E(\xi)$ be the corresponding cyclotomic extension. Also let $M = K(\xi)$ and consider the following diagram.

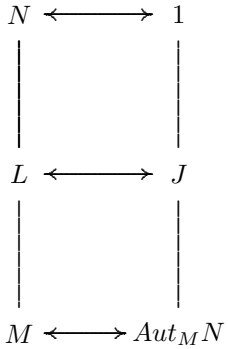


Clearly M is a radical extension of K. Hence it is enough to find a radical extension of M which contains N. Next onbserve $N = E(\xi)$ is a Galois extension of K. Since E is a Galois Extension of K, it follows that $\sigma[E] = E$ for every $\sigma \in \operatorname{Aut}_M N \leq \operatorname{Aut}_K N$. Hence, we can define a homomorphism $\theta : \operatorname{Aut}_M N \to \operatorname{Aut}_K E = G$ by $\sigma \mapsto \sigma|_E$. Since each $\sigma \in \operatorname{Aut}_M N$ satisfies $\sigma(\xi) = \xi$, it follows that θ is an injection. Hence, $\operatorname{Aut}_M N$ is also solvable and $|\operatorname{Aut}_M N| \leq |\operatorname{Aut}_K E|$.

There are 2 cases to consider.

Case A: Suppose that $\theta[\operatorname{Aut}_M N]$ is a proper subgroup of $\operatorname{Aut}_K E$. Then $[N : M] = |\operatorname{Aut}_M N| < |\operatorname{Aut}_K E| = n$. Hence, by induction hypothesis, there exists a radical extension F of M containing N.

Case B: Otherwise, $\theta : \operatorname{Aut}_M N \to \operatorname{Aut}_K E = G$ is an isomorphism. Let $J = \theta^{-1}(H)$. Then J is a normal subgroup of $\operatorname{Aut}_M N$ of index p, and clearly J is also solvable. Let $L = N^J$ and consider the following diagram:



Thus, L is a Galois extension of M and $\operatorname{Aut}_M L \simeq \operatorname{Aut}_M N / \operatorname{Aut}_L N = \operatorname{Aut}_M N / J$. Thus $|\operatorname{Aut}_M L| = p$ and so L is a cyclic extension of M. Since M contains a primitive p^{th} root of unity, there exists $u \in L$ such that $L = M(u)$ and u is a root of some polynomial $x^p - a \in M[x]$.

In particular, L is a radical extension of M. Also notice that $[N : L] = |J| < [N : M] = [E : K] = n$ and that $\operatorname{Aut}_L N = J$ is solvable. Hence by inductin hypothesis, there exists a radical extension F of L which contains N. $\square$

Finally, a couple of loose ends...

Example: Let $f(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$.

1. The equation $f(x) = 0$ is solvable by radicals

2. The splitting field E of $f(x)$ over $\mathbb{Q}[x]$ isn't a radical extension.

Proof. By Hungerford p272, the Galois group of $f(x)$ is $G = A_3 \simeq C_3$. Hence $[E : \mathbb{Q}] = 3$. Suppose that E is a radical extension of $\mathbb{Q}$. Then there exists $\alpha \in E$ such that $E = \mathbb{Q}(\alpha)$ and α is the root of an irreducible polynomial $x^3 - a \in \mathbb{Q}[x]$. Since E is normal, E must contain all roots of $x^3 - a$, ie, $\alpha, \xi\alpha, \xi^2\alpha$ where ξ is a primitive 3^{rd} root of unity. In particular, $\xi \in E$, which is impossible since $[\mathbb{Q}(\xi) : \mathbb{Q}] = 2$. □

Another loose end, what are the finite subgroups of $\mathrm{Aut}_{\mathbb{Q}} \mathbb{C}$?

Theorem 5.50 (Artin)**.** *Suppose K is an algebraically closed field of characteristic 0 and $1 \neq G$ is a finite subgroup. Let $F = K^G$. Then $[K : F] = |G| = 2$ and $K = F(i)$ where $i^2 = -1$.*

Proof. By Artin, $[K : F] = |G|$ and K is a Galois extension of F. Let $E = F(i)$ where $i^2 = -1$. Then K is also a Galois extension of E. Let $H = \mathrm{Aut}_E K$. Then it is enough to show that $H = 1$ so that $E = K$.

Suppose not and let p be a prime such that $p||H|$. Let $C \leq H$ be cyclic of order p and let $L = K^C$. Then, $[K : L] = p$ and K is a cyclic extension of L. If ξ is a primitive p^{th} root fo unity, then $\mathrm{Irr}(\xi, L, x)$ has degree $\leq p-1$. Thus, $\xi \in L$. Hence, K is the splitting field of some irreducible polynomial $x^p - a \in L[x]$. Let $\alpha = \alpha_1, \ldots, \alpha_p \in K$ be the roots of $x^p - a$. Since K is algebraically closed, there exists some $\beta \in K$ such that $\beta^p = \alpha$.

Computing with $N = N_L^K$, we find $-a = (-1)^p \alpha_1 \ldots \alpha_p = (-1)^p N(\alpha) = (-1)^p N(\beta^p) = (-1)^p N(\beta)^p$. Thus, $N(\beta) \in L$ satisfies $N(\beta)^p = (-1)^{p-1} a$. Since L doesn't contain a root of $x^p - a = 0$, it follows that $p = 2$. Thus $N(\beta)^2 = -a$. But since $i \in L$, we have that $a = (-1)(-a) = (iN(\beta))^2$, which is a contradiction. □

6 Linear Algebra

Let k be a field. Recall from linear algebra that an endomorphism of a vector space (free module over a division ring) can be represented by a matrix in one way for each basis.

Definition 6.1 (Change of Basis)**.** *Let $\{e_i\}$ and $\{f_i\}$ be two bases of a vector space V. Let C be the matrix define by $e_j = \sum_{i=1}^n c_{ij} f_i$. C is called the change of basis matrix, and CAC^{-1} represents the linear operator A in the basis $\{f_i\}$.*

Definition 6.2 (Similar Matrices)**.** *We say that the matrices A and B are similar if $\exists C$ such that $CAC^{-1} = B$*

Similar matrices are representations of the same linear operator in different bases.

Theorem 6.1 (Rational Canonical Form)**.** *Every matrix is similar to a block diagonal matrix with blocks of the form* $\begin{bmatrix} 0 & 0 & \dots & -a_1 \\ 1 & 0 & \dots & -a_2 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 1 & -a_m \end{bmatrix}$

Proof. Recall, V is a k-module. We fix $\varphi : V \to V$. Give V the structure of a $k[x]$-module by setting $x \cdot v = \varphi(v)$.

We notice that if $v = \sum b_i e_i$ then $x \cdot v = \varphi(v) = A \cdot v$

Remark: If you change basis, then $v = \sum b_j e_j = \sum_j b_j \sum_i c_{ij} f_i = \sum_i (\sum_j c_{ij} b_j) f_i$

As $k[x]$ is a PID, we have $V \simeq \oplus_\ell k[x]/f_\ell(x) \oplus k[x]^r$ where $f_1 | f_2 | \dots f_k$.

But $k[x]$ has ∞ dimension over k, as $x, x^2, x^3, \dots$ are linearly independent over k, so $r = 0$

Thus, $V \simeq \oplus_\ell k[x]/f_\ell$. Lets write $f_\ell = \sum_{i=1}^{m_\ell} d_{\ell_i} x^i$ and lets assume as k is a field that all the f_ℓ's are monic. That is, $d_\ell = 1$.

Let $m_\ell = \deg f_\ell$. So $1, x, x^2, \dots, x^{m_\ell - 1}$ generate $V_\ell \simeq k[x]/f_\ell$.

Now: how does x act on V_ℓ? It acts on this basis $\{1, x, \dots, x^{m_\ell - 1}\}$ by shifting, so $x \cdot x^k = x^{k+1}$, thus $x \cdot x^{m_\ell - 1} = x^{m_\ell} = \sum_{i=0}^{m_\ell - 1} (-d_{\ell_i}) x^i$, so $x : V_\ell \to V_\ell$ has matrix $\begin{bmatrix} 0 & 0 & \dots & -d_{\ell_0} \\ 1 & 0 & \dots & -d_{\ell_1} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 1 & -d_{\ell_{m_\ell - 1}} \end{bmatrix}$. □

Definition 6.3 (Algebraically Closed)**.** *A field K is algebraically closed if every polynomial in k has a root.*

Theorem 6.2 (Jordan Canonical Form)**.** *If k is algebraically closed, then every matrix is similar to a block diagonal matrix with blocks of the form* $\begin{bmatrix} \lambda & 1 & \dots & 0 \\ 0 & \lambda & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda \end{bmatrix}$

Proof. Assume that k is algebraically closed. We know that $V \simeq \oplus_{\ell=1}^{m} k[x]/p_\ell^{n_\ell}(x)$ where $p_\ell(x)$ is prime.

The primes in $k[x]$ with k algebraically closed are of the form $x - a$ for $a \in k$.

Suppose $p_\ell(x) = x - \lambda_\ell$, with $\lambda_\ell \in k$. Then $p_\ell^{n_\ell}(x) = (x - \lambda_\ell)^{n_\ell}$

We'll show that V_ℓ has a basis such that $\varphi_\ell : V_\ell \to V_\ell$, where $\varphi_\ell = \varphi|_{V_\ell}$ has a matrix as above.

We will show that the companion matrix of $p_\ell^{n_\ell}$ is similar to a Jordan block.

We define $B = A - \lambda I$ for λ the root of p_ℓ. We have a $k[y]$-module structure by $y \cdot v = Bv$. We check that V is a cyclic $k[y]$-module.

Then $y^n v = B^n v = (A - \lambda I)^n v = f(A)v = 0$ but $y^{n-1} v \neq 0$. So $V \simeq k[y]/y^n$ as a $k[y]$-module. The the rational canonical form of B has $a_i = 0$ unless $i = n - 1$, and $a_{n-1} = 1$.

$CAC^{-1} = CBC^{-1} + C\lambda IC^{-1} = CBC^{-1} + \lambda I$

So, in this basis, A is the transpose of a Jordan block. We reverse the order of the basis and obtain the Jordan Form. □

How can we compute the JCF?

Definition 6.4 (Eigenvalues and Eigenvectors)**.** *$\lambda \in k$ is an eigenvalue of A if $\exists x \neq 0$ such that $Ax = \lambda x$.*
$x \in V$ is an eigenvector of A if $\exists \lambda \in k$ such that $Ax = \lambda x$.

Thus, the λ's in the JCF are all eigenvalues.
If V has a basis of eigenvectors of A, then A is similar to a diagonal matrix.

Theorem 6.3. *The Following Are Equivalent:*

1. *λ is an eigenvalue.*
2. *$\exists x \neq 0$ such that $Ax = \lambda x$*
3. *$(A - \lambda I)x = 0$*
4. *$A - \lambda I$ is not invertible*
5. *$\det(A - \lambda I) = 0$.*

Definition 6.5 (Generalized Eigenspace)**.** *Let $E_\lambda^m = \{v \in V : (A-\lambda I)^m v = 0\}$. E_λ^m is called the generalized eigenspace and $v \in E_\lambda^m$ is called a generalized eigenvector.*

Note: E_λ^m is a subspace, if $v \in E_\lambda^m$ then $(A-\lambda I)v \in E_\lambda^{m-1}$, $(A-\lambda I)E_\lambda^{m+1} \subseteq E_\lambda^m \subseteq E_\lambda^{m+1}$, and $\exists N$ such that $E_\lambda^N = E_\lambda^m$ for all $m \geq N$.
If $\lambda \neq \mu$ then $E_\lambda^{\max} \cap E_\mu^{\max} = \{0\}$, and $\{E_\lambda^{\max} : \lambda \text{ eigenvalue } \}$ span V and are disjoin, so $V \simeq \oplus_\lambda E_\lambda^{\max}$. Thus, $\dim V = \sum \dim E_\lambda^{\max} = n$.
So the Jordan Canonical Form gives a lower bound on $\dim E_\lambda^{\max}$ since the bounds must add to n, we have that the number of λ in the Jordan Canonical Form is equal to $\dim E_\lambda^{\max}$.

Corollary 6.4. *All eigenvalues show up in the JCF.*

An algorithm for computing the JCF:

1. Compute the eigenvalues λ of A
2. For each λ, compute $E_\lambda^1, \ldots, E_\lambda^{\max}$.
3. If $E_\lambda^{\max} = E_\lambda^n \neq E_\lambda^{n-1}$ choose a basis for $E_\lambda^n / E_\lambda^{n-1}$. Claim: $\{(A-\lambda I)^m v_i : 1 \leq i \leq k, 0 \leq m \leq n-1\}$ is linearly independent. Look at $\{(A-\lambda I)v_i\} \subseteq E_\lambda^{n-1}$ is linearly independent. Complete this to a basis for $E_\lambda^n / E_\lambda^{n-1}$.
   Continue in this fashion until you obtain $B = \{v_1, \ldots, v_k\}$ a basis for V where each $v_i \in E_\lambda^m$ for some m and $v_i \in B$ implies $(A - \lambda I)v_i \in B$ if nonzero. This gives the desired basis.

Definition 6.6 (Minimal Polynomial)**.** *Let $I = \{f \in k[x]\}$ such that $f(A)v = 0$ for all $v \in V$. Pick a basis $v_1, \ldots, v_n$ for V. $I = \cap_{i=1}^n \Theta_{v_i}$, $\Theta_{v_i} = \{f \in k[x] : f \cdot v_i = 0\}$ with this being the $k[x]$-module structure for V with φ a linear operator.*

Since each Θ_{v_i} is nonzero and $k[x]$ is an integral domain, $I = \cap\Theta_{v_i}$ is nonzero, and I is an ideal in $k[x]$. As $k[x]$ is a PID, $I = \langle f \rangle$ for some $f \in I$.

We call f the minimal polynomial.

Lemma 6.5. *The minimal polynomial of the companion matrix of f is itself.*

Proof. Recall, if A is a block of the rational canonical form, then $e_1, \ldots, e_n$ is a basis for V. If $g(x) = \sum_{i=0}^k c_i x^i$ such that $g(A) = 0$, then $g(A)e_1 = \sum c_i A^i e_i = \sum c_i e_{i+1}$ so if $k + 1 \leq n$ then $g = 0$. So degree of minimal polynomial of A is $\geq n$. note that, by definition, $A^n e_1 = \sum_{i=0}^n a_i e_{i+1}$, $0 = -\sum a_i A^i e_i - A^n e_1 = (A^n + \sum a_i A^i)e_1 = 0$ so $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$ satisfies $f(A)v = 0$ for all $v \in V$, so $f(A) = 0$.

Thus, the minimal polynomial divides f, but has at least the same degree, so it equals f up to multiplication by a constant. □

Corollary 6.6. *If A is in rational canonical form, then A_i is the companion matrix of f_i, $f_1 | \ldots | f_\ell$ then f_ℓ is the minimal polynomial.*

Definition 6.7 (Characteristic Polynomial)**.** *The characteristic polynomial of A is* $\det(A - xI)$.

$\det(CAC^{-1} - xI) = \det(C(A - xI)C^{-1}) = \det(A - xI)$. So to compute the characteristic polynomial, we may take A to be in JCF.

Theorem 6.7 (Cayley-Hamilton)**.** *The minimal polynomial of A divides the characteristic polynomial of A.*

7 Commutative Algebra

1. Rings of Quotients and localizations

Definition 7.1 (Multiplicative Set)**.** *A subset S of a ring R is multiplicative iff $1 \in S$ and $a, b \in S$ implies that $ab \in S$.*

Definition 7.2 (Ring of Fractions)**.** *Let S be a multiplicative subset of the ring R. Then we define the equivalence relation $\sim$ on $R \times S$ by $(r, s) \sim (r', s')$ iff there exists $t \in S$ such that $t(rs' - r's) = 0$.*

For each $(r, s) \in R \times S$ the corresponding $\sim$ class is denoted by $\frac{r}{s}$. Let $S^{-1}R = \{r/s : (r, s) \in R \times S\}$. It is easily checked that $S^{-1}R$ is a ring with operations $r/s + r'/s' = (rs' + r's)/ss'$ and $r/s * r'/s' = rr'/ss'$, zero is $0/1$ and identity is $1/1$.

Furthermore, there exists a canonical homomorphism $\phi_S : R \to S^{-1}R : r \mapsto r/1$ and every element of $\phi_S[S]$ is a unit in $S^{-1}R$.

Remarks:

1. If 0 in S then $S^{-1}R$ is the trivial ring.

2. If $0 \notin S$ and S doesn't contain any zero divisors, then $\sim$ reduces to the expected relation.

3. Consider $R = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ and $S = \{0, 2, 4\}$. Consider the relation $\equiv$ on $R \times S$ given by $(r, s) \equiv (r', s')$ iff $rs' - r's = 0$. Then $(0, 1) \equiv (0, 2)$ and $(0, 2) \equiv (3, 1)$, but $(0, 1) \not\equiv (3, 1)$. It is easily checked that $S^{-1}R \simeq \mathbb{Z}_3$ so ϕ_S isn't injective.

Theorem 7.1. *Let S be a multiplicative subset of the ring R. Suppose that $0 \notin S$ and S doesn't contain any zero divisors. Then $\phi_S : R \to S^{-1}R$ is injective.*

Proof. Suppose that $\phi_S(r) = r/1 = 0/1$. Then there exists $s \in S$ such that $s(r1 - 0) = 0$. That is, $sr = 1$. Since s isn't a zero divisor, $r = 0$. □

Examples

1. If R is an integral domain and $S = R \setminus \{0\}$, then $S^{-1}R$ is a field, called the quotient field of R.

2. Suppose $R = \mathbb{Z}$, and $S = \{3^n : n \geq 0\}$. Then $\mathbb{Z}[1/3] = \{z/3^n : z \in \mathbb{Z}, n \geq 0\}$.

Convention: if R is an integral domain and $S \subseteq R \setminus \{0\}$ is multiplicative, then we identify R with its canonical copy in $S^{-1}R$.

Definition 7.3 (Extension and Retraction)**.** *Let S be a multiplicative subset of the ring R.*

1. *If $I \subseteq R$ is an ideal, then the extension of I in $S^{-1}R$ is $S^{-1}I = \{a/s : a \in I, s \in S\}$.*

2. *If $J \subseteq S^{-1}R$ is an ideal, then the contraction of J in R is $\phi_S^{-1}(J)$.*

Remarks: Clearly, $S^{-1}I$, $\phi_S^{-1}(J)$ are ideals.

Lemma 7.2. *With the above hypotheses, $S^{-1}I = S^{-1}R$ iff $S \cap I \neq \emptyset$.*

Proof. If $s \in S \cap I$, then $\frac{1}{1} = \frac{1}{s}\frac{s}{1} \in S^{-1}I$.

Conversely suppose that $S^{-1}I = S^{-1}R$. Then there exist $a \in I$ and $s \in S$ such that $\frac{a}{s} = \frac{1}{1}$. Hence, there exists $t \in S$ such that $ts - ta = t(s - a) = 0$. So $ts = ta \in S \cap I$. □

Lemma 7.3. *With the above hypotheses,*

1. *$I \subseteq \phi_S^{-1}(S^{-1}I)$*

2. *If $I = \phi_S^{-1}(J)$ for some ideal $J \subseteq S^{-1}R$, then $S^{-1}I = J$. Hence every ideal of $S^{-1}R$ has the form $S^{-1}I$ for some ideal $I \subseteq R$.*

3. *If $P \subseteq R$ is a prime ideal and $S \cap P = \emptyset$, then $S^{-1}P$ is a prime ideal of $S^{-1}R$ and $\phi_S^{-1}(S^{-1}P) = P$.*

Proof. 1 is obvious.

2: suppose that $I = \phi_S^{-1}(J)$. To see that $S^{-1}I \subseteq J$, let $x \in S^{-1}I$. Then there exists r with $\phi_S(r) \in J$ and $s \in S$ such that $x = r/s$. Hence $x = \frac{1}{s}\frac{r}{1} = \frac{1}{s}\phi_S(r) \in J$. Conversely suppose that $\frac{r}{s} \in J$. Then $\phi_S(r) = r/1 = \frac{s}{1}\frac{r}{s} \in J$ hence $r \in I$ and $/s \in S^{-1}I$.

3: By Lemma 1, $S^{-1}P$ is an ideal such that $S^{-1}P \neq S^{-1}R$. Suppose that $\frac{r}{s}\frac{r'}{s'} \in S^{-1}P$. Then there exists $a \in P$ and $t \in S$ such that $\frac{rr'}{ss'} = \frac{a}{t}$. Hence, there exists $t' \in S$ such that $t'trr' - t'ss'a = 0$. Thus, $tt'rr' = t'ss'a \in P$, since $tt' \in S$ and $S \cap P = \emptyset$, we have $rr' \in P$. Finally, by part 1, $P \subset \phi_S^{-1}(S^{-1}P)$. Conversely, suppose that $r \in \phi_S^{-1}(S^{-1}P)$. Then $\phi_S(r) \in S^{-1}P$ and so there exists $a \in P$ and $s \in S$ such that $\frac{r}{1} = \frac{a}{s}$. Hence, there exists $t \in S$ such that $tsr = ta \in P$. Since $ts \notin P$, $r \in P$. □

Theorem 7.4. *With the above hypotheses, we can define a bijection* $\{P \subseteq R : P \text{ prime ideal}, P \cap S = \emptyset\} \to \{Q \subseteq S^{-1}R : Q \text{ prime}\}$ *by* $P \mapsto S^{-1}P$.

Proof. By the third part of Lemma 2, the map $P \mapsto S^{-1}P$ is an injection between these sets. To see it is a surjection, let J be a prime ideal of $S^{-1}R$. Then $S^{-1}(\phi_S^{-1}(J)) = J$, so it is enough to show that $\phi_S^{-1}(J)$ is a prime ideal.

Suppose that $ab \in \phi_S^{-1}(J)$. Then $\phi_S(a)\phi_S(b) \in J$ and so $\phi_S(a) \in J$ or $\phi_S(b) \in J$. Thus, $a \in \phi_S^{-1}(J)$ or $b \in \phi_S^{-1}(J)$. □

Definition 7.4 (Localization at P)**.** *Suppose that P is a prime ideal of R. Then $R \setminus P$ is a multiplicative subset of R. The localization of R at P is defined to be $R_P = (R \setminus P)^{-1}R$.*

If $I \subseteq R$ is an ideal, then we write $I_P = (R \setminus P)^{-1}I$.

Example: Let $R = \mathbb{Z}$ and $P = (3)$, then $\mathbb{Z}_P = \{z/n : z \in \mathbb{Z}, (n, 3) = 1\}$.

Theorem 7.5. *Suppose that P is a prime ideal of the ring R.*

1. *There exists a bijection between $\{Q \subseteq R : Q \text{ prime and } Q \subseteq P\} \to \{J \subseteq R_P : J \text{ prime}\}$ given by $Q \mapsto Q_P$.*
2. *P_P is the unique maximal ideal of R_P.*

Proof. 1 is just a special case of the previous theorem.

For 2, we let $J \subseteq R_P$ be any maximal ideal. Then J is prime. Hence, there exists a prime ideal $Q \subseteq P$ such that $Q_P = J$. But then $J = Q_P \subseteq P_P$ so $J = P_P$. □

Definition 7.5 (Local Ring)**.** *A ring R is local if R has a unique maximal ideal.*

Theorem 7.6. *If R is a ring, then TFAE*

1. *R is a local ring*

2. *The nonunits of R form an ideal.*

Proof. $1 \Rightarrow 2$: Let M be the unique maximal ideal of R. Clearly each element of M is a nonunit. Conversely, suppose that $r \in R$ is a nonunit. Then $I = (r)$ is a proper ideal. Hence, $I \subseteq M$. So $r \in M$. Thus, M consists of the nonunits of R.

$2 \Rightarrow 1$: Pretty trivial. □

Theorem 7.7 (Nakayama's Lemma)**.** *Let R be a local ring and let $\mathfrak{m}$ be the maximal ideal of R. Suppose that E is a finitely generated R-module. If $\mathfrak{m}E = E$ then $E = 0$.*

Proof. Suppose that E is a counterexample with a minimal number of generators, say, $x_1, \ldots, x_n$. Since $\mathfrak{m}E = E$, there exist $m_1, \ldots, m_n \in \mathfrak{m}$ such that $x_n = m_1x_1 + \ldots + m_nx_n$, so then $(1 - m_n)x_n = m_1x_1 + \ldots + m_{n-1}x_{n-1}$.

Since $1 - m_n \notin \mathfrak{m}$, it follows that $1 - m_n$ is a unit. But then, $x_1, \ldots, x_{n-1}$ generates E, contradicting minimality of n. □

2. Integral Ring Extensions

Definition 7.6 (Integral over R)**.** *Let S be a ring extension of the ring R and let $\alpha \in S$. Then α is integral over R iff there exists a monic polynomial $f(x) \in R[x]$ such that $f(\alpha) = 0$.*

Example: Let $R = \mathbb{Z}$ and $S = \mathbb{Q}^{\text{alg}}$. Then $\alpha = \frac{-\sqrt{-3}}{2} \in S$ is integral over $\mathbb{Z}$ since $\alpha^2 + \alpha + 1 = 0$.

Definition 7.7 (Annihilator)**.** *Let R be a ring and let M be an R-module. Then, the annihilator of M,* $\text{Ann}(M) = \{r \in R : rm = 0, \forall m \in M\}$.

The module is faithful iff $\text{Ann}(M) = 0$.

Theorem 7.8. *If S is an extension ring of R and $\alpha \in S$, then TFAE*

1. *α is integral over S.*
2. *The ring $R[\alpha]$ is finitely generated as an R-module*
3. *There exists a faithful $R[\alpha]$-module M which is finitely generated as an R-module.*

We shall make use of the following lemma:

Lemma 7.9. *Let S be a ring and let $A = (a_{ij})$ be an $n \times n$ matrix over S. Suppose that M is an S-module and that $b_1, \ldots, b_n \in M$ satisfy $A \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = 0$. Then $(\det A)b_i = 0$ for $1 \leq i \leq n$.*

Proof. We will sketch a proof. Consider the case when $n = 3$. We just check that $\det Ab_2 = 0$. Consider the matrix $B_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & b_2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Then $\det(AB_2) = \det(A)\det(B_2) = \det Ab_2$. Also, $AB_2 = \begin{bmatrix} a_{11} & a_{12}b_2 & a_{13} \\ a_{21} & a_{22}b_2 & a_{23} \\ a_{31} & a_{32}b_2 & a_{33} \end{bmatrix}$ hence $\det(AB_2) = \begin{bmatrix} a_{11} & a_{11}b_1 + a_{12}b_2 + a_{13}b_3 & a_{13} \\ a_{21} & a_{21}b_1 + a_{22}b_2 + a_{23}b_3 & a_{23} \\ a_{31} & a_{31}b_1 + a_{32}b_2 + a_{33}b_3 & a_{33} \end{bmatrix} = 0$ □

Now we will prove the theorem.

Proof. $1 \Rightarrow 2$: Let $g(x) \in R[x]$ be a monic polynomial such that $g(\alpha) = 0$. Say that $\deg g = n$. If $\beta \in R[\alpha]$, there exists $f(x) \in R[x]$ such that $\beta = f(\alpha)$. Singe $g(x)$ is monic, there exists $q(x), r(x) \in R[x]$ with degree $< n$ such that $f(x) = q(x)g(x) + r(x)$. Thus $\beta = f(\alpha) = r(\alpha)$. Hence $1, \alpha, \ldots, \alpha^{n-1}$ generates $R[\alpha]$ as an R-module.

$2 \Rightarrow 3$: Just take $M = R[\alpha]$.

$3 \Rightarrow 1$: Let M be a faithful $R[\alpha]$-module which is finitely generated as an R-module, say by $b_1, \ldots, b_n$. Since $\alpha M \subseteq M$, there exist $a_{ij} \in R$ such that $\alpha b_i = a_{ij}b_j$. Hence, by the previous lemma, if $d = \begin{vmatrix} \alpha - a_{11} & -a_{12} & \ldots & -a_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha - a_{n1} & -a_{n2} & \ldots & -a_{nn} \end{vmatrix}$

then $db_i = 0$ for $1 \leq i \leq n$. Since M is a faithful $R[\alpha]$-module, it follows that $d = 0$. Thus, α is a root of the polynomial $\det(xI - A) \in R[x]$. And so α is integral over R. □

Definition 7.8 (Integral Extension)**.** *Let S be a ring extension of R. Then S is integral over R iff every $\alpha \in S$ is integral over R.*

Corollary 7.10. *If S is a ring extension of R and S is finitely generated as an R-module, then S is an integral extension of R.*

Proof. Let $\alpha \in S$. Then S is a faithful $R[\alpha]$-module which is finitely generated as an R-module. Hence, α is integral over R. □

Corollary 7.11. *If S is a ring extension of R and $s_1, \ldots, s_n \in S$ are integral over R, then $R[s_1, \ldots, s_n]$ is a finitely generated R-module and hence is an integral extension of R.*

Proof. We argue by induction that $R[s_1, \ldots, s_i]$ is a finitely generated R-module.

For the induction step, note that $R[s_1, \ldots, s_{i+1}] = R[s_1, \ldots, s_i][s_{i+1}]$.

Since s_{i+1} is integral over $R[s_1, \ldots, s_i]$, then $R[s_1, \ldots, s_{i+1}]$ is finitely generated as an $R[s_1, \ldots, s_i]$-module. Since $R[s_1, \ldots, s_i]$ is finitely generates as an R-module, it follows that $R[s_1, \ldots, s_{i+1}]$ is finitely generates as an R-module. □

Corollary 7.12. *Let S be a ring extension of R and and let $\hat{R} = \{\alpha \in S : \alpha$ is integral over $R\}$. Then $\hat{R}$ is a subring of S called the integral closure of R in S.*

Proof. Let $\alpha, \beta \in \hat{R}$. Then $R[\alpha, \beta]$ is an integral extension of R. Hence $\alpha - \beta, \alpha\beta \in \hat{R}$. □

Definition 7.9 (Integrally Closed)**.**
1. *With the above hypotheses, R is integrally closed in S iff $\hat{R} = R$.*
2. *An integral domain R is integrally closed iff R is integrally closed in its quotient field K.*

Proposition 7.13. *If R is a UFD, then R is integrally closed.*

Proof. Suppose that a/b is integral over R, where $a, b \in R$ and there exists a prime p such that $p|b$ and $p \not| a$. There exist $a_0, \ldots, a_{n-1} \in R$ such that $(a/b)^n + a_{n-1}(a/b)^{n-1} + \ldots + a_0 = 0$, hence $a^n + a_n b a^{n-1} + \ldots + b^n a_0 = 0$. Since $p|b$, it follows that $p|a^n$ and so $p|a$, contradiction. □

Example: $\mathbb{Z}[i]$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$.

Proof. Clearly $\mathbb{Z}[i] \subseteq \hat{\mathbb{Z}}$ since i is integral over $\mathbb{Z}$. Since $\mathbb{Z}[i]$ is a UFD, it is integrally closed in $\mathbb{Q}(i)$. The result follows. □

Definition 7.10 (Number Field)**.** *A number field L is a finite extension of $\mathbb{Q}$. If L is a number field, then the ring of algebraic integers of L is the integral closure of $\mathbb{Z}$ in L.*

Example: Let $\omega = \frac{-1+\sqrt{-3}}{2}$. Then $\mathbb{Z}[\omega]$ is the algebraic closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-3})$.

Proof. Just like before, using the fact that $\mathbb{Z}[\omega]$ is a UFD. □

Definition 7.11 (Lies Above)**.** *Let S be an extension ring of R and let I be an ideal of R. Then the ideal J of S lies above I iff $J \cap R = I$.*

Nonexample: Clearly no ideal of $\mathbb{Q}$ lies above the ideal (2) of $\mathbb{Z}$.

Theorem 7.14 (Lying Over Theorem)**.** *Let S be an integral extension of R and let P be a prime ideal of R. Then there exists a prime ideal Q of S which lies over P.*

Proof Delayed
$\mathbb{Z} \subset \mathbb{Z}[i]$, then (2) has $(1+i)$ and $(1-i)$ lying over it.
$\mathbb{Z} \subset \mathbb{Z}[\omega]$, then $(2) \subset \mathbb{Z}[\omega](2)$.

Proposition 7.15. *Let S be an integeral extension of R and let $\sigma : S \to A$ be a ring homomorphism. Then $\sigma[S]$ is an integral extension of $\sigma[R]$.*

Proof. Let $\alpha \in S$. Then there exists $a_{n-1}, \ldots, a_0 \in R$ such that $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$. Applying σ we obtain $\sigma(\alpha)^n + \sigma(a_{n-1})\sigma\alpha^{n-1} + \ldots + \sigma(a_0) = 0$, thus, $\sigma(\alpha)$ is integral over $\sigma[R]$. □

Application: Let R be an integral domain of char 0 with quotient field K and let E be a finite algebraic extension of K. If $\alpha \in E$ in integral over R, then $N_K^E(\alpha), \mathrm{tr}_K^E(\alpha)$ are also integral over R. In particular, if R is integrally closed, then $N_K^E(\alpha), \mathrm{tr}_K^E(\alpha) \in R$.

Proof. If $\sigma \in e_K(E, K^{\mathrm{alg}})$, then $\sigma(\alpha)$ is integral over R. Hence, so are $N_K^E(\alpha) = \prod_{\sigma \in e_K(E,K^{\mathrm{alg}})} \sigma(\alpha)$ and $\mathrm{tr}_K^E(\alpha) = \sum_{\sigma \in e_K(E,K^{\mathrm{alg}})} \sigma(\alpha)$ □

Definition 7.12 (Integral Homomorphism)**.** *A ring homomorphism $f : R \to S$ is integral iff S is an integral extension of $f[R]$.*

Definition 7.13. *Suppose that $f : R \to S$ is a ring homomorphism and T is a multiplicative subset of R. Then, slightly abusing notation by writing $T^{-1}S$ instead of $f[T]^{-1}S$, we can define a ring homomorphism $T^{-1}f : T^{-1}R \to T^{-1}S : r/t \mapsto f(r)/f(t)$.*

Furthermore, the following diagram commutes:

$$\begin{array}{ccc} S & \longrightarrow & T^{-1}S \\ \uparrow f & & \uparrow T^{-1}f \\ R & \longrightarrow & T^{-1}R \end{array}$$

Proposition 7.16. *Let $f : R \to S$ be integral and let T be a multiplicative subset of R. Then $T^{-1}f : T^{-1}R \to T^{-1}S$ is also integral.*

Proof. To simplify notation, we just consider the case where f and $T^{-1}f$ are inclusions.

Let $s/t \in T^{-1}S$. Then there exist $a_0, \ldots, a_{n-1} \in R$ such that $s^n + a_{n-1}s^{n-1} + \ldots + a_0 = 0$. Gence $(s/t)^n + a_{n-1}/t(s/t)^{n-1} + \ldots, a_0/t^n = 0$, hence s/t is integral over $T^{-1}R$. □

Proposition 7.17. *Suppose that T is an integrally closed integral domain and that T is a multiplicative subset of R such that $0 \notin T$. Then $T^{-1}R$ is also integrally closed.*

Proof. Let K be the quotient field of R and hence also of $T^{-1}R$. Suppose that $\alpha \in K$ is integral over $T^{-1}R$. Then there exists $a_0, \ldots, a_{n-1} \in R$ and $t_0, \ldots, t_{n-1} \in T$ such that $\alpha^n + a_{n-1}/t_{n-1}\alpha^{n-1} + \ldots + a_0/t_0 = 0$. Let $t = t_0 \ldots t_{n-1} \in T$. Then it is clear that $t\alpha$ is integral over R and so $t\alpha \in R$. But this means that $\alpha \in T^{-1}R$. □

We will now prove the Lying Over Theorem:

Proof. Let S be an integral extension of R and let P be a prime ideal of R. Let $T = R \setminus P$ ad consider teh ring of quotients $T^{-1}R$ and $T^{-1}S$. To simplify notation, we shall suppose that each of the following maps is an influsion.

$$\begin{array}{ccc} S & \longrightarrow & T^{-1}S \\ \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle T^{-1}f} \\ R & \longrightarrow & T^{-1}R = R_P \end{array}$$

(If collapsing occurs, it is easily checked that the following arguments remain valud using the canonical homomorphisms)

By Proposition 3, $T^{-1}S$ is an integral extension of $T^{-1}R$, and by Theorem 3, $T^{-1}R$ is a local ring with maximal ideal $\mathfrak{m}_P = T^{-1}P$. Also, by Lemma 2.3, $\mathfrak{m}_P$ lies over P.

Claim: $\mathfrak{m}_P T^{-1}S \neq T^{-1}S$.

Suppose that $\mathfrak{m}_P T^{-1}S = T^{-1}S$. Then there exist $m_i \in \mathfrak{m}_P$ and $b_i^{-1} \in T^{-1}S$ such that $1 = m_1 b_1 + \ldots + m_n b_n$. Let $B = R_P[b_1, \ldots, b_n]$. Since $T^{-1}S$ is an integral extension of R_P, it follows that B is a finitely generated R_P-module. By the equation, for each $1 \leq i \leq n$, we have $\mathfrak{m}_P B = B$. By Nakayama's Lemma, $B = 0$, which is a contradiction.

It follows that $\mathfrak{m}_P T^{-1}S$ is contained in a maximal ideal $\mathfrak{n}$ of $T^{-1}S$. Since $\mathfrak{m}_P \subseteq \mathfrak{n} \cap T^{-1}R$, and $\mathfrak{m}_P$ is a maximal ideal of $T^{-1}R$, it follows that $\mathfrak{m}_P = \mathfrak{n} \cap T^{-1}R$.

Thus:

$$\begin{array}{ccccc} S & \longrightarrow & T^{-1}S & & N \\ \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle T^{-1}f} & & \uparrow \\ R & \longrightarrow & T^{-1}R & & \uparrow \\ & & & & \uparrow \\ & & & & \uparrow \\ P & & \longrightarrow & & M_P \end{array}$$

Let $Q = \mathfrak{n} \cap S$. Clearly Q is a prime ideal of S. Finally note that $P = \mathfrak{m}_P \cap R = (\mathfrak{n} \cap T^{-1}R) \cap R = (\mathfrak{n} \cap S) \cap R = Q \cap R$. Thus, Q lies above P. □

Proposition 7.18. *Let S be an integral extension of R and let P be a prime ideal of R. Suppose that that Q is a prime ideal of S which lies above P. Then Q is a maximal ideal iff P is a maximal ideal.*

Proof. Suppose that P is a maximal ideal. Then R/P is a field and S/Q is an integral domain, which is integral over R/P by Prop 2. Since $R/S \subseteq S/Q \subseteq (R/P)^{\text{alg}}$, it follows that S/Q is a field. Thus, Q is a maximal ideal. Next suppose that Q is a maximal ideal. Then S/Q is a field which is integral over the integral domain R/P. Suppose that R/P isn't a field. Then R/P has a maximal ideal $\mathfrak{m}$ such that $0 \neq \mathfrak{m} \neq R/P$. By the Lying Over Theorem, there exists a prime ideal of S/Q which lies above $\mathfrak{m}$, which is impossible. □

3. Integral Galois Extensions

Standing Hypotheses: Let R be an integral domain of characteristic 0 which is integrally closed in its quotient field K. Let E be a finite Galois extension of K and S be the integral closure of R in E. Let $G = \mathrm{Aut}_K E$ be the corresponding Galois Group.

Remark: Clearly, if $\sigma \in G$, then $\sigma[S] = S$.

Proposition 7.19. *Suppose that P is a maximal ideal of R and that $\mathscr{P}$ and $\mathscr{R}$ are prime ideals of S that lie above P. Then there exists $\sigma \in G$ such that $\sigma[\mathscr{P}] = \mathscr{R}$.*

Proof. Suppose that $\sigma[\mathscr{P}] \neq \mathscr{R}$ for all $\sigma \in G$. Then $\sigma[\mathscr{P}] \neq \tau[\mathscr{R}]$ for all $\sigma, \tau \in G$. By Proposition 5, each $\sigma[\mathscr{P}]$ and $\tau[\mathscr{R}]$ is a maximal ideal of S. Hence, by the Chinese Remainder Theorem, there exists $x \in S$ such that $x \equiv 0 \mod \sigma[\mathscr{P}]$ for all $\sigma \in G$ and $\equiv 1 \mod \tau[\mathscr{R}]$ for all $\tau \in G$.

Since R is integrally closed in K, it follows that $N_K^E(x) = \prod_{\sigma \in G} \sigma(x) \in S \cap K = R$ and so $N_K^E(x) \in \mathscr{P} \cap R = P$.

However, since $x \notin \tau[\mathscr{R}]$ for all $\tau \in G$, it follows that $\tau(x) \notin \mathscr{R}$ for all $\tau \in G$. Since $\mathscr{R}$ is a prime ideal, it follows that $N_K^E(x) = \prod_{\tau \in G} \tau(x) \notin \mathscr{R}$ and so $N_K^E(x) \notin P$, contradiction. □

Definition 7.14 (Decomposition Group)**.** *Fix a maximal ideal P of R and let $\mathscr{P}$ be a maximal ideal of S which lies above P, we define the decomposition group of $\mathscr{P}$ to be $G_{\mathscr{P}} = \{\sigma \in G : \sigma[\mathscr{P}] = \mathscr{P}\}$*

Then, regarding R/P as a subfield of $S/\mathscr{P}$, each $\sigma \in G_{\mathscr{P}}$ induces an automorphism $\overline{\sigma}$ of $S/\mathscr{P}$ which fixes R/P pointwise. Thus we obtain a homomorphism $G \to \mathrm{Aut}_{R/P}(S/\mathscr{P}) : \sigma \mapsto \overline{\sigma}$.

Definition 7.15 (Decomposition Field)**.** *The decomposition field of $\mathscr{P}$ is $E^{dec} = E^{G_{\mathscr{P}}}$, the fixed field of $G_{\mathscr{P}}$.*

Let S^{dec} be the integral closure of R in E^{dec}. Let $\mathscr{D} = \mathscr{P} \cap S^{dec}$. Then $\mathscr{D}$ is a prime ideal of S^{dec} which lies above P. Hence $\mathscr{D}$ is a maximal ideal of S^{dec}.

Furthermore, by the previous proposition, $\mathscr{P}$ is the unique prime ideal of S which lies above $\mathscr{D}$.

Proposition 7.20. *E^{dec} is the smallest subfield F of E such that $K \subseteq F \subseteq E$ and $\mathscr{P}$ is the unique prime ideal of S which lies above the prime ideal $\cap$ of $S \cap F$.*

Proof. We've just seen that E^{dec} is such a subfield. To see that is it hte smallest such subfield, let F be any such subfield and let $H = \mathrm{Aut}_F E$. Let $Q = \mathscr{P} \cap F$.

Since $\mathscr{P}$ is the unique prime ideal of S which lies above Q, it follows that $H \leq G_{\mathscr{P}}$. Hence $F = E^H \supseteq E^{dec} = E^{G_{\mathscr{P}}}$. □

Example: Suppose $R = \mathbb{Z}$, $E = \mathbb{Q}(i)$. Let $P = (2)$.

GThen $(1+i)$, $(1-i)$ are the ideals of $S = \mathbb{Z}[i]$ which lie above P. Let $\mathscr{P} = (1+i)$. Then $G_{\mathscr{P}} = 1$ and so $E^{dec} = E^1 = \mathbb{Q}(i)$.

Let $R = \mathbb{Z}$ and $E = \mathbb{Q}(\omega)$, where $\omega^2 + \omega + 1 = 0$. Again, let $\mathbb{Z} = (2)$. Then $\mathscr{P} = 2\mathbb{Z}[\omega]$ is the unique prime ideal of $S = \mathbb{Z}[\omega]$ which lies above P. Then $G_{\mathscr{P}} = G$ and $E^{dec} = E^G = \mathbb{Q}$.

Proposition 7.21. *Under the canonical injection, $R/P \hookrightarrow S^{dec}/\mathscr{D}$, we have $R/P = S^{dec}/\mathscr{D}$.*

Proof. Let $\sigma \in G \setminus G_{\mathcal{P}}$. Then clearly $\sigma^{-1}\mathcal{P} \neq \mathcal{P}$.

Define $\mathcal{D}_\sigma = \sigma^{-1}\mathcal{P} \cap S^{dec}$.

Since $\mathcal{P}$ is the unique prime ideal of S lying above $\mathcal{D}$, it follwos that $\mathcal{D}_\sigma \neq \mathcal{D}$.

Clearly $\mathcal{D}_\sigma$ is a prime ideal of S^{dec}. Since $\mathcal{D}_\sigma$ lies above the maximal ideal P of R, then by Proposition 5, we know that $\mathcal{D}_\sigma$ is a maximal ideal of S^{dec}.

Now fix some $x \in S^{dec}$. We seek an element $\alpha \in R$ such that $x \equiv \alpha \mod \mathcal{D}$.

By the Chinese Remainder Theorem, there exists $y \in S^{dec}$ such that $y \equiv x \mod \mathcal{D}$, $y \equiv 1 \mod \mathcal{D}_\sigma$ for all $\sigma \in G \setminus G_{\mathcal{P}}$.

In particular, we have that $y \equiv 1 \mod \sigma^{-1}\mathcal{P}$ for all $\sigma \in G \setminus G_{\mathcal{P}}$ and hence, $\sigma(y) \equiv 1 \mod \mathcal{P}$ for all $\sigma \in G \setminus G_{\mathcal{P}}$.

In summary, we have that $y \equiv x \mod \mathcal{P}$ and $\sigma(y) \equiv 1 \mod \mathcal{P}$ for all $\sigma \in G \setminus G$.

✓

Now consider $\alpha = N_K^{E^{dec}}(y) \in R$, since R is integrally closed in K. Let $e_K(E^{dec}, K^{\text{alg}}) = \{\tau_1, \ldots, \tau_m\}$ so that $N_K^{E^{dec}}(y) = \tau_1(y) \ldots \tau_m(y)$.

Then for each $1 \leq i \leq m$, there exists $\sigma_i \in G$ such that $\tau_i = \sigma_i|_{E^{dec}}$. Notice that if $\sigma \in G_{\mathcal{P}}$, then $\sigma|_{E^{dec}} = \text{id}$.

Hence, we can suppose that $\sigma_1 = 1$ and $\sigma_i \in G \setminus G_{\mathcal{P}}$ for $2 \leq i \leq m$.

It follows that $\alpha = N_K^{E^{dec}}(y) \equiv x \mod \mathcal{P}$. Since $\alpha, x \in S^{dec}$, it follows that $\alpha \equiv x \mod \mathcal{D}$, as required. □

Let $\overline{S} = S/\mathcal{P}$ and $\overline{R} = R/P$. For each $\alpha \in S$, let $\overline{\alpha} \in \overline{S}$ be the corresponding element. Then, for each $\sigma \in G_{\mathcal{P}}$, the corresponding $\overline{\sigma} \in \text{Aut}_{\overline{R}}\,\overline{S}$ satisfies $\overline{\sigma}(\overline{\alpha}) = \overline{\sigma(\alpha)}$.

Finally, for each $f \in S[x]$, let $\overline{f} \in \overline{S}[x]$ be the corresponding polynomial.

More Hypotheses: From now on, we also suppose that $\overline{R}$ is a finite field. (This isn't really essential, but it allows us to ignore separability issues.)

Theorem 7.22. *1. $\overline{S}$ is a finite Galois extension of $\overline{R}$ with $[\overline{S} : \overline{R}] \leq [E : K]$*

2. The homomorphism $G_{\mathcal{P}} \to \text{Aut}_{\overline{R}}\,\overline{S} : \sigma \mapsto \overline{\sigma}$ is surjective.

Proof. 1. It is enough to show that $[\overline{S} : \overline{R}] \leq [E : K]$. Let $\overline{\alpha} \in \overline{S}$ and consider a corresponding $\alpha \in S$. Let $f(x) = \text{Irr}(\alpha, K, x)$. Then $\deg f \leq [E : K]$. Since the roots of f are integral over R, it follows that the coefficients of f are also integral over R.

Since R is integrally closed in K, it follows that $f(X) \in R[x]$. Clearly $\overline{f}(\overline{\alpha}) = 0$, thus $\overline{f} \in \overline{R}[x]$ is a polynomial of degree $\leq [E : K]$ such that $\overline{f}(\overline{\alpha}) = 0$. Hence $[\overline{S} : \overline{R}] \leq [E : K]$.

2. Since $G_{\mathcal{P}} = \mathrm{Aut}_{E^{dec}} E$ and $S^{dec}/\mathcal{D} = R/P$, we can suppose that $K = E^{dec}$ and $G = G_{\mathcal{P}}$. Let $\overline{\alpha} \in \overline{S}$ satisfy $\overline{S} = \overline{R}(\overline{\alpha})$. Let $f(x) = \mathrm{Irr}(\alpha, K, x)$. Then we have already seen that $f(x) \in R[x]$ so we can form $\overline{f}(x) \in \overline{R}[x]$. Now notice that any $\tau \in \mathrm{Aut}_{\overline{R}} \overline{S}$ is uniquely determined by its effect on $\overline{\alpha}$ and that $\overline{\alpha}$ must also be a root of $\overline{f}(x)$. Let $\beta = \tau(\overline{\alpha})$.

   Since the roots of $f(x)$ are integral over R, we see that $f(x) = \prod_{i=1}^{m}(x - \alpha_i)$, $\alpha_1 = \alpha$, splits into linear factos in $S[x]$. Applying the canonical homomorphism, we obtain that $\overline{f}(x) = \prod_{i=1}^{m}(x - \overline{\alpha_i})$ has a corresponding splitting in $\overline{S}[x]$. In particular, there exists $1 \leq i \leq m$ such that $\overline{\alpha}_i = \beta$. Let $\sigma \in G = G_{\mathcal{P}}$ satisfy $\sigma(\alpha) = \alpha_i$. Then $\overline{\sigma}(\overline{\alpha}) = \overline{\alpha}_i = \beta$ and so $\overline{\sigma} = \tau$.

□

Theorem 7.23. *With the above hypotheses, suppose further that there exists a monic irreducible $f(x) \in R[x]$ such that E is the splitting field of f over K and $\overline{f}(x)$ has no multiple roots in $\overline{R}^{\mathrm{alg}}$. Then:*

1. *The homomorphism $G_{\mathcal{P}} \to \mathrm{Aut}_{\overline{R}} \overline{S}$ is an isomorphism.*
2. *$\overline{S}$ is the splitting field of $\overline{f}$ over $\overline{R}$.*

Proof. 1. Let $\{\alpha_1, \ldots, \alpha_n\} \subseteq S$ be the roots of $f(x)$ and let $\{\overline{\alpha}_1, \ldots, \overline{\alpha}_n\} \subseteq \overline{S}$ be their reductions mod $\mathcal{P}$. For any $\sigma \in G_{\mathcal{P}}$, we have $\overline{\sigma}(\overline{\alpha}_I) = \overline{\sigma(\alpha_i)}$ $1 \leq i \leq n$. hence, if $\overline{\sigma} = 1$, then $\sigma = 1$.

2. Clearly $\overline{S}$ contains the splitting field $\overline{E} = \overline{R}[\overline{\alpha}_1, \ldots, \overline{\alpha}_n]$ of $\overline{f}$ over $\overline{R}$. Because $G_{\mathcal{P}} \to \mathrm{Aut}_{\overline{R}} \overline{S}$ surjectively, we see that $\mathrm{Aut}_{\overline{E}} \overline{S} = 1$, and so $\overline{E} = \overline{S}$.

□

Warning: Consider the irreducible monic $f(x) = x^2 + 3 \in \mathbb{Z}[x]$. Reducing mod 2, we have that $\overline{f}(x) = x^2 + 1 = (x+1)^2 \in \mathbb{F}_2[x]$, so the splitting field of $\overline{f}$ over $\mathbb{F}_2$ is $\mathbb{F}_2$. Let $P = (2)$ and let S be the integral closure of $\mathbb{Z}$ in the splitting field $E = \mathbb{Q}(\sqrt{-3})$. Recall that $S = \mathbb{Z}[\omega]$ where $\omega = \frac{-1+\sqrt{-3}}{2}$. Also, $\mathcal{P} = 2S$ is the unique prime ideal of S lying above P, thus $\overline{S} = S/\mathcal{P} = \mathbb{F}_4$.

Extended Example

Consider the irreducible polynomial $f(x) = x^4 + 5x^2 + 10x - 15 \in \mathbb{Z}[x]$. Let E be the splitting field and G e the Galois group. It is easily checked that $f(x)$ has exactly two real roots. It follows that $G \not\leq A_4$.

Reducing modulo 3, we obtain the following decomposition into irreducibles $x^4 + 2x^2 + x = x(x^3 + 3x + 1) \in \mathbb{F}_3[x]$. Thus, G contains a 3 cycle. Since G is a transitive subgroup of S_4, it contains every 3 cycle, and so $A_4 \leq G$, so $G = S_4$.

Let S be the ring of algebraic integers in E. Consider the ideal $P = (3)$ of $\mathbb{Z}$ and let $\mathcal{P}$ be a maximal ideal of S which lies above P. Since $\overline{S} = S/\mathcal{P} \simeq \mathbb{F}_{3^3}$.

We have that $G_{\mathcal{P}} \simeq C_3$. Hence $[G : G_{\mathcal{P}}] = 8$. Thus, there are exactly 8 maximal ideals of S which lie over P and $[E^{dec} : \mathbb{Q}] = 8$.

Question: How many maximal ideals of S^{dec} lie above P?

Answer: Suppose that $\mathcal{D}'$ is any maximal ideal of S^{dec} which lies above P. By the Lying Over Theorem, there exists a maximal ideal $\mathcal{R}$ of S which lies over $\mathcal{D}'$, and clearly $\mathcal{R}$ lies over P.

Thus, we must compute the size of $\{S^{dec} \cap \mathcal{R} : \mathcal{R}$ is a maximal idela of S lying over $P\}$.

Let $\mathcal{R}$ be any such ideal of S. Then either $G_{\mathcal{R}} = G_{\mathcal{P}}$ or $G_{\mathcal{R}} \cap G_{\mathcal{P}} = 1$.

Let $\mathcal{R} = \sigma\mathcal{P}$ for some $\sigma \in G$. Then $G_{\mathcal{R}} = G_{\mathcal{P}}$ iff $\sigma \in N_G(G_{\mathcal{P}})$. Hence the number of such ideals $\mathcal{R}$ is $[N_G(G_{\mathcal{P}}), G_{\mathcal{P}}] = [S_3 : A_3] = 2$, so there are two such ideals, $\mathcal{P}$ and $\mathcal{P}'$.

Then $\mathcal{D} = \mathcal{P} \cap S^{dec} \neq \mathcal{P}' \cap S^{dec} = \mathcal{D}'$, since $\mathcal{P}$ is the unique maximal ideal of S which lies above $\mathcal{D} = \mathcal{P} \cap S^{dec}$.

Now suppose that $\mathcal{R}$ satisfies $G_{\mathcal{R}} \cap G_{\mathcal{P}} = 1$, then $\{\sigma\mathcal{R} : \sigma \in G_{\mathcal{P}}\}$ consists of three ideals, each lying over $\mathcal{R} \cap S^{dec}$. Hence the number of maximal ideals of S^{dec} lying above P is $2 + (8-2)/3 = 4$.

If we reduce modulo 2 instead, we obtain $x^4 + x^2 + 1 = (x^2 + x + 1)^2 \in \mathbb{F}_2[x]$, so it is unclear what is $S/\mathcal{P}$ where $\mathcal{P}$ lies above (2). We also don't know what $G_{\mathcal{P}}$ is.

4. Nötherian Rings and Modules

Definition 7.16 (Nötherian Module)**.** *Let R be a ring and let M be an R-module. Then M is Noetherian iff M satisfies the ascending chain condition (ACC) on submodules. IE, if $M_1 \subseteq M_2 \subseteq \ldots$ is an increasing chain of submodules, then there is an n such that $M_\ell = M_n$ for all $\ell \geq n$.*

Definition 7.17 (Nötherian Ring)**.** *The ring R is Nötherian iff R is a Nötherian R-module.*

Theorem 7.24. *If R is a ring and M is an R-module, then the following are equivalent:*

1. *M is Nötherian.*
2. *M satisfies the maximum condition for submodules: ie, whenever $\mathcal{S}$ is a nonempty set of submodules of M, then $\mathcal{S}$ contains a maximal element under inclusion.*
3. *Every submodule of M is finitely generated.*

Proof. (1) $\Rightarrow$ (2): Let $\mathcal{S}$ be a nonempty collection of submodules of M. Suppose $\mathcal{S}$ doesn't contain a maximal element. Then we can inductively choose $M_n \in \mathcal{S}$ such that $M_0 \subsetneq M_1 \subsetneq \ldots$, contradiction.

(2) $\Rightarrow$ (3): Let N be a submodule of M. Let $\mathcal{S} = \{A : A$ is a finitely generated submodule of $N\}$. Then $\mathcal{S}$ has a maximal element A. We claim that $A = N$. Otherwise, there exists $b \in N \setminus A$ and so $A \subsetneq A + Rb \in \mathcal{S}$, contradiction.

(3) $\Rightarrow$ (1) suppose that $M_0 \subseteq M_1 \subseteq \ldots$ is a chain of submodules of M. Then $N = \cup_n M_n$ is a submodule of M and so is finitely generated. Then N is finitely generated by, say, $a_1, \ldots, a_t$. There exists n such that $a_1, \ldots, a_t \in M_n$. Clearly $M_\ell = M_n$ for all $\ell \geq n$. $\square$

Corollary 7.25. *A ring R is Nötherian iff every ideal is finitely generated.*

Example: In particular, every PID is Noetherian.

Question: Suppose that E is a field such that $[E : \mathbb{Q}] < \infty$. Let R be the ring of algebraic integers in E. Is R Nötherian?

Proposition 7.26. *1. If M is a Nötherian R-mdoule, then every submodule of M and every quotient of M is also Noetherian.*

2. Suppose that M is an R-module and N is a submodule. If N and M/N are Nötherian, then M is also Nötherian.

Proof. 1. Obvious.

2. Claim: Suppose that $E \subseteq F$ are submodules of M. If $E \cap N = F \cap N$ and $(E + N)/N = (F + N)/N$ then $E = F$.

To prove the claim, we suppose that $x \in F$. Then there exists $y \in E$ and $u, v \in N$ such that $x + u = y + v$. Hence $x - y = v - u \in F \cap N = E \cap N$. Thus $x = (x - y) + y \in E$.

Now, we let $M_0 \subseteq M_1 \subseteq \ldots$ be an increasing chain of submodules of M. Consider teh associated chains $M_0 \cap N \subseteq \ldots$ and $(M_0 + N)/N \subseteq \ldots$ of submodules of $N, M/N$ respectively. Since N and M/N are Nötherian, there exists n such that for all $\ell \geq n$, $M_\ell \cap N = M_n \cap N$ and $(M_\ell + N)/N = (M_n + N)/N$. Hence $M_\ell = M_n$ for all $\ell \geq n$. □

Corollary 7.27. *If $M_1, \ldots, M_n$ are Nötherian R-modules, then $M_1 \oplus \ldots \oplus M_n$ is also Nötherian.*

Suppose that M is an R-module, and $M_1, \ldots, M_n$ are R-modules such that $M = M_1 + \ldots + M_n$. If $M_1, \ldots, M_n$ are Nötherian, then M is Nötherian.

Proof. Arguing by induction, we can suppose that $n = 2$. Then M_1 and $(M_1 \oplus M_2)/M_1 \simeq M_2$ are Nötherian, and hence $M_1 \oplus M_2$ is.

We can define a surjective homomorphism from $M_1 \oplus \ldots \oplus M_n$ to $M_1 + \ldots + M_n = M$ by $(m_1, \ldots, m_n) \mapsto m_1 + \ldots + m_n$. The result follows. □

Proposition 7.28. *If R is a Nötherian ring and M is a finitely generated R-module, then M is Nötherian,*

Proof. Let $x_1, \ldots, x_n$ generate M. Then define a surjective homomorphism $R \oplus \ldots \oplus R \to M$ by $(r_1, \ldots, r_n) \mapsto r_1 x_1 + \ldots + r_n x_n$. Since $R \oplus \ldots \oplus R$ is Nötherian, the result follows. □

Theorem 7.29. *Let K be a field such that $[K : \mathbb{Q}] < \infty$ and let R be the ring of algebraic integers in K. Then R is Nötherian.*

Proof. Note that it is enough to show that R is finitely generated as a $\mathbb{Z}$-module. For then, by Prop 10, R is a Nötherian $\mathbb{Z}$-module and hence is also a Nötherian R-module.

Choose $\gamma \in K$ such that $K = \mathbb{Q}(\gamma)$. Let $\mathrm{Irr}(\gamma, \mathbb{Q}, x) = x^n + q_{n-1}x^{n-1} + \ldots + q_0$, the $q_i \in \mathbb{Q}$. Clearing denominators, $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ such that $t\gamma^n + a_{n-1}\gamma^{n-1} + \ldots + a_0 = 0$. Thus, $\alpha = t\gamma \in R$ and $K = \mathbb{Q}(\alpha)$.

Warning: It doesn't follwo that $R = \mathbb{Z}[\alpha]$. For example, let $K = \mathbb{Q}(\sqrt{-3})$. Then $\mathbb{Z}[\sqrt{-3}] \subsetneq R$.

Note that $[K : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. Let $\alpha = \alpha_1 \ldots, \alpha_n$ be the distinct conjugates of α in the normal closure E of K. Let $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)$. Then $d = \Delta^2 \in \mathbb{Z}$.

Claim: $R \subset d^{-1}\mathbb{Z}[\alpha]$.

Before proving the claim, we complete the proof of ht ethorem. Note that $\mathbb{Z}[\alpha]$ is a finitely generated free $\mathbb{Z}$-module, and hence, so is $d^{-1}\mathbb{Z}[\alpha]$. Since R is a $\mathbb{Z}$-submodule, it follows that R is also a finitely generated free $\mathbb{Z}$-module.

We will now prove the claim: Let $\beta \in R$. Then there exist $b_0, \ldots, b_{n-1} \in \mathbb{Q}$ such that $\beta = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$. It follows that the (not necessarily distinct) conjugates of β in E are $\beta_j = b_0 + b_1\alpha_j + \ldots + b_{n-1}\alpha_j^{n-1}$ for $1 \leq j \leq n$.

Note that $\begin{vmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ \vdots & & & \\ 1 & \alpha_n & \ldots & \alpha_n^{n-1} \end{vmatrix} = \prod_{i<j}(\alpha_i - \alpha_j) \neq 0$, hence we can use Cramer's Rule to solve the matrix equation $\begin{pmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ \vdots & & & \\ 1 & \alpha_n & \ldots & \alpha_n^{n-1} \end{pmatrix} \begin{pmatrix} b_0 \\ \vdots \\ b_{n-1} \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$.

We obtain $b_i = \frac{1}{\Delta}(\gamma_{i1}\beta_1 + \ldots \gamma_{in}\gamma_n)$ $0 \leq i \leq n-1$ where each γ_{ij} is a polynomial with integer coefficients in $\{\alpha_r^s : 1 \leq r \leq n, 0 \leq s \leq n-1\}$. In particular, γ_{ij} is an algebraic integer of E. Since each β_j is an algebraic integer, we decude that $db_i = \Delta(\gamma_{i1}\beta_1 + \ldots + \gamma_{in}\beta_n)$ is also an algebraic integer. Since $db_i \in \mathbb{Q}$, if follows that $db_i \in \mathbb{Z}$. Thus $\beta = b_0 + \ldots + b_{n-1}\alpha^{n-1} \in d^{-1}\mathbb{Z}[\alpha]$. □

Theorem 7.30 (Hilbert Basis Theorem)**.** *If R is a Nötherian ring, then the polynomial ring $R[x]$ is also Nötherian.*

Corollary 7.31. *If R is Nötherian, then $R[x_1, \ldots, x_n]$ is Nötherian.*

Corollary 7.32. *Let R be a Nötherian ring and let $S = R[a_1, \ldots, a_n]$ be an extension ring which is finitely generated as a ring over R. Then S is also Nötherian.*

Proof. We can define a surjective homomorphism $f : R[x_1, \ldots, x_n] \to R[a_1, \ldots, a_n]$. By the homework, the result follows. □

We will now prove the Hilbert Basis Theorem:

Proof. Let I be an ideal of $R[x]$. For each $n \geq 0$, let J_n be the set of all leading coefficients a_n of polynomails of degree n such that

(*) $a_n x^n + \ldots + a_0 \in I$.

Clearly, J_n is an ideal of R. Furthermore, if $(*)$ holds, then $a_n x^{n+1} + \ldots + a_0 x = x(a_n x^n + \ldots + a_0) \in I$, and so $J_0 \subseteq J_1 \subseteq \ldots$. As R is Nötherian, then

there exists t such that $J_\ell = J_t$ for all $\ell \geq t$. For each $0 \leq \ell \leq t$, let $a_{\ell 1}, \ldots, a_{\ell s_\ell}$ be generators of J_ℓ and let $f_{\ell_i} \in I$ be a polynomial of degree ℓ with leading coefficients $a_{\ell i}$. We claim that $X = \{f_{\ell_i} : 0 \leq \ell \leq t, 1 \leq i \leq s_\ell\}$ generates I. We shall prove by induction of $d = \deg f$ that if $f \in I$ then $f \in (X)$. First, suppose that $d = 0$ and that $f = r \in I \cap R = J_0$.

Then clearly, $r \in (a_{01}, \ldots, a_{0s_0}) \subseteq (X)$.

Now suppose that $d > 0$ and that the result holds for all $0 \leq k < d$. Let $f \in I$ be a polynomial of degree d with leading coefficient r.

First suppose that $d \leq gt$. Then $r \in J_d$ and so $r = r_1 a_{d_1} + \ldots r_{s_d} a_{d_{s_d}}$ for some $r_i \in R$. Thus the polynomial $r_1 f_{d_1} + \ldots r_{s_d} f_{d_{s_d}} \in (X) \subseteq$ is a polynomial of degree d with leading coefficient r. Hence $f - \sum_{i=1}^{s_d} r_i f_{d_i} \in I$ has degree at most $d-1$ and so by induction hypothesis lies in (X). It fllows that $f = (f - \sum_{i=1}^{s_d} r_i f_{d_i}) + \sum_{i=1}^{s_d} r_i f_{d_i} \in (X)$.

Finally, suppose that $d > t$. Then $r \in J_d = J_t$ and so $r = r_1 a_{t1} + \ldots + r_{s_t} a_{ts_t}$ sor some $r_i \in R$. Thus the polynomial $r_1 x^{d-t} f_{t_1} + \ldots + r_{s_t} f_{ts_t} \in (X) \subseteq I$ has leading coefficient r and degree d. Arguing as in the previous case, we see inductively that $f \in (X)$. □

An application...

Definition 7.18 (Affine n-space)**.** *Let k be any field and $n \geq 1$. k^n is called affine n-space over K.*

Let $k[\vec{x}] = k[x_1, \ldots, x_n]$.

Definition 7.19 (Algebraic Set)**.** *A subset $V \subset k^n$ is algebraic iff there is a subset $S = \{p_i(\vec{x}) : i \in I\} \subseteq k[\vec{x}]$ such that $V = V(S) = \{\vec{a} \in k^n : p_i(\vec{a}) = 0$ for all $i \in I\}$.*

Example: We can regard $SL_2(k)$ as an algebraic subset of k^4 defined by identifying it with $\{(a, b, c, d) : ad - bc = 1\}$, which is defined by the single polynomial $p(\vec{x}) = x_1 x_4 - x_2 x_3 - 1$.

Suppose that $V = V(S)$ is an algebraic set and that I is the ideal of $k[\vec{x}]$ generated by S. Clearly, if $f(\vec{x}) \in I$ then $f(\vec{a}) = 0$ for all $\vec{a} \in V = V(S)$, and so $V(S) \subseteq V(I)$. Also since $I \supseteq S$, it is clear that $V(I) \subseteq V(S)$. Thus $V(S) = V(I)$.

Thus we have a "natural" surjective map from ideals of $k[\vec{x}]$ to algebraic subsets of k^n taking I to $V(I)$. The map is NOT injective, however, as $V(x)$ and $V(x^2)$ are both $\{0\}$.

We can also define a "natural" map from the algebraic subsets of k^n to ideals of $k[\vec{x}]$ by $V \mapsto J(V)$ where $J(V)$ is the ideal of all polynomials vanishing on V.

Definition 7.20 (Radical of an Ideal)**.** *If I is an ideal of the ring R, then the radical of I is the ideal* $\operatorname{Rad} I = \{r \in R : r^n \in I$ *for some $n \geq 1$}.

The ideal I is a radical ideal iff $I = \operatorname{Rad} I$.

Example: If $V \subset k^n$ is an algebraic set, then $J(V)$ is a radical ideal.

Hence, we actually "natural" map from algebraic subsets of k^n to radical ideals of $k[\vec{x}]$ by $V \mapsto J(V)$.

This map must be injective, because $V = V(J(V))$. By definition, $V \subseteq V(J(V))$. Let I be an ideal such that $V = V(I)$. Then $I \subseteq J(V)$ and so $V = V(I) \supseteq V(J(V))$, hence $V = V(J(V))$.

Remark: If k is an arbitrary field, then the map need not be surjective. $(x^2+1) \subset \mathbb{R}[x]$. Howeer, the correspondence is a bijection when k is algebraically closed.

This is the content of Hilbert's Nullstellensatz.

Theorem 7.33. *Let k be any field and $n \geq 1$.*

1. *If $V \subseteq k^n$ is an algebraic set, then there exists a finite subset of polynomials $S \subset k[x_1, \ldots, x_n]$ such that $V = V(S)$.*

2. *If $V_1 \supseteq V_2 \supseteq \ldots \supseteq V_n \supseteq \ldots$ is a descending sequence of algebraic subsets of k^n, then there exists t such that $V_\ell = V_t$ for all $\ell \geq t$.*

Proof. 1. Let I be an ideal such that $V = V(I)$ since $k[x_1, \ldots, x_n]$ is Nötherian, I is finitely generated, say, by S. Clearly $V = V(S)$.

2. Consider $J(V_1) \subseteq \ldots$. Then there is a t such that $J(V_t) = J(V_\ell)$ for all $\ell \geq t$. Hence $V_t = V(J(V_t)) = V(J(V_\ell)) = V_\ell$ for all $\ell \geq t$.

□

Remark: The following variant of the first part of the theorem is often useful: If S is a subset of $k[x_1, \ldots, x_n]$, then there exists a finite subset S_0 such that $V(S) = V(S_0)$.

Definition 7.21 (Variety of Representations)**.** *Let G be a finitely generated group with fixed generating set $T = \{t_1, \ldots, t_r\}$.*

Let $\mathscr{R} = \{W(y_1, \ldots, y_r) : W$ is a word such that $W(t_1, \ldots, t_r) = 1\}$ be the corresponding set of relations.

Then, the corresponding variety of representations of (G, T) in $SL_2(\mathbb{C})$ is the algebraic subset of $\mathbb{C}^{4r}$ defined by $V_{G,T} = \{(M_1, \ldots, M_r) \in SL_2(\mathbb{C})^r : W(M_1, \ldots, M_r) = 1$ for all $W \in \mathscr{R}\}$

Remark: To see that this is an algebraic set, we must check that the condition $W(M_1, \ldots, M_r) = 1$ corresponds to a set of polynomial equations.

Let $Rep(G, SL_2(\mathbb{C}))$ be the set of all group homomorphisms $\pi : G \to SL_2(\mathbb{C})$. Then we can define a bijection $Rep(G, SL_2(\mathbb{C})) \to V_{G,T}$ by $\pi \mapsto (\pi(t_1), \ldots, \pi(t_r))$.

Of course $\mathscr{R}$ is infinite, and since most groups are not finitely presented, we apparently need infintiely many words to define $V_{G,T}$, except...by the Hilbert Basis Theorem

Theorem 7.34. *With the above hypotheses, there exists a finite $\mathscr{R}_0 \subseteq \mathscr{R}$ such that $V_{G,T} = \{(M_1, \ldots, M_r) \in SL_2(\mathbb{C})^r : W(M_1, \ldots, M_r) = 1$ for $w \in \mathscr{R}_0\}$.*

This is not a contradiction, though the least it can tell us is that most finitely generated groups do not have faithful linear representations.

Definition 7.22 (Residually Free)**.** *A group G is residually free iff for all $1 \neq g \in G$, there exists a homomorphism $\pi : G \to F$ into a free group F such that $\pi(g) \neq 1$.*

Some examples/remarks:

Clearly, every residually free group is torsion-free, and every free group is residually free. If $G_1, \ldots, G_n$ are residually free, then $G_1 \oplus G_2 \oplus \ldots \oplus G_n$ is residually free.

Proof. Let $1 \neq g = (g_1, \ldots, g_n) \in G_1 \times \ldots \times G_n$, then there exists i such that $g_i \neq 1$, hence there is a homomorphism $G_1 \times \ldots \times G_n \to G_i \to F$ such that $(\pi \circ p_i)(g) = \pi(g_i) \neq 1$. □

Theorem 7.35. *Suppose that $G_1 \overset{\phi_1}{\to} G_2 \overset{\phi_2}{\to} \ldots \to G_n \to \ldots$ is a seqeunce of surjective homomorphisms between finitely generated residually free groups, then there exists t such that $\phi_e \ll$ is an isomorphism for all $\ell \geq t$.*

Basis Facts about Free Groups:

1. The matrices $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ free generate a free group on two generators.
2. The commutator subgroup of the free group F_2 on 2 generators is a free group on infinitely many generators. Hence, if G is a finitely generated residually free group and $1 \neq g \in G$, then there exists $\pi : G \to F_2$ such that $\pi(g) \neq 1$.

$$\pi : G \to F_2 = \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle \leq SL_2(\mathbb{C}).$$

Remark: There exists a finitely generated residually free group which isn't finitely presented.

Proof. Recall that $F_2 \times F_2$ is residually free. Hence if $G \leq F_2 \times F_2$, then G is also residually free.

By Google, there exists a finitely generated subgrtoup $G \leq F_2 \times F_2$ which is not finitely presented. □

We will now prove Theorem 15.

Proof. Let $T_1 = \{t_1, \ldots, t_r\}$ be a generating set for G_1; and for $n \geq 1$, let $T_n = \{t_1^{(n)}, \ldots, t_r^{(n)}\}$ be the image of T_1 under the surjective homomorphism $G_1 \to \ldots \to G_n$. Then T_n is a set of generators for G_n. For each $n \geq 1$, let $V_n = V_{G_n, T_n} \subseteq (SL_2(\mathbb{C})^r) \subseteq \mathbb{C}^{4r}$.

Since $\phi_n[T_n] = T_{n+1}$, for each word w if $w(t_1^{(n)}, \ldots, t_r^{(n)}) = 1$, then $w(t_1^{(n+1)}, \ldots, t_r^{(n+1)}) = 1$.

Thus, the corresponding sets of relations satisfy $\mathscr{R}_n \subseteq \mathscr{R}_{n+1}$; and so the algebraic sets satisfy $V_n \supseteq V_{n+1}$. Hence $V_1 \supseteq \ldots V_n \supseteq \ldots$. By Theorem 13,

there exists n such that $V_\ell = V_n$ for all $\ell \geq n$. hence it is enough to prove the following:

If $\phi_k : G_k \to G_{k+1}$ isn't an ismorphism, then $V_k \supsetneq V_{k+1}$.

Since $\phi_k : G \to G_{k+1}$ is not an ismorphism, there exists a word such that $g = w(t_1^{(k)}, \ldots, t_r^{(k)}) \neq 1$ but $\phi_k(g) = w(t_1^{(k+1)}, \ldots, t_r^{(k+1)}) = 1$. In particular, $w \in \mathscr{R}_{k+1}$. Since G_k is residually free, there exists a homomrophism $\pi : G_k \to F_2$ such that $\pi(g) \neq 1$. We can suppose that $F_2 \leq SL_2(\mathbb{Z}) \leq SL_2(\mathbb{C})$. Thus $(\pi(t_1^{(k)}), \ldots, \pi(t_r^{(k)})) \in V_k$. However, since $w(\pi(t_1^{(k)}), \ldots, \pi(t_r^{(k)})) = \pi(w(t_1^{(k)}, \ldots, t_r^{(k)})) = \pi(g) \neq 1$ and $w \in \mathscr{R}_{k+1}$, we see that $(\pi(t_1^{(k)}), \ldots, \pi(t_r^{(k)})) \notin V_{k+1}$. And so the claim is proved. □

5. Transcendence Bases

Definition 7.23 (Algebraically Dependent)**.** *Let F be an extension field of K and let $S \subseteq F$. Then S is algebraically dependent over k iff there exist distinct $s_1, \ldots, s_n \in S$ and $0 \neq p(\vec{x}) \in k[x_1, \ldots, x_n]$ such that $p(s_1, \ldots, s_n) = 0$.*

Otherwise, S is algebraically independent.

Examples:

1. $\{\sqrt{2}\}$ is algebraically dependent over $\mathbb{Q}$.
2. $\{\pi\}$ is algebraically independent over $\mathbb{Q}$.
3. $\{\pi, \sqrt{\pi}\}$ are algebraically dependent over $\mathbb{Q}$. To see this, let $p(x_1, x_2) = x_1 - x_2^2 \in \mathbb{Q}[x_1, x_2]$. Then $p(\pi, \sqrt{\pi}) = 0$.
4. Let $F = k(y_1, \ldots, y_n)$ be the field of rational functions in the variables $\{y_1, \ldots, y_n\}$. Then $\{y_1, \ldots, y_n\}$ is algebraically independent over k.

Definition 7.24 (Transcendence Basis)**.** *A subset $S \subseteq F$ is a transcendence basis of F over K iff S is a maximal independent subset.*

Remark: Transcendence Bases always exist. Why? Because if $\{S_i : i \in I\}$ is an increasing chain of independent sets, then $\cup_i S_i$ is also independent, because of the finitary nature of dependence. Now apply Zorn's Lemma.

Example: Let $F = k(y_1, \ldots, y_n)$ be a field of rational functions. Then $\{y_1, \ldots, y_n\}$ is a transcendence basis.

Theorem 7.36. *Let F be an extension of K and $S \subseteq F$ be algebraically independent over K. Then if $u \in F \setminus K(S)$, then the following are equivalent:*

1. *$S \cup \{u\}$ is algebraically independent.*
2. *u is transcendental over $K(S)$.*

Proof. 2 ⇒ 1: Assume u is transcendental over $K(S)$. SUppose there exist distinct $s_1, \ldots, s_{n-1} \in S$ and $f(\vec{x}) \in k[x_1, \ldots, x_n]$ such that $f(s_1, \ldots, s_{n-1}, u) = 0$. Then u is a root of the polynomial $f(s_1, \ldots, s_{n-1}, x_n) \in K(S)[x_n]$.

Express $f = h_r x_n^r + h_{r-1} x_n^{r-1} + \ldots + h_0$ where $h_i \in k[x_1, \ldots, x_{n-1}]$. Since u is transcendental over $K(S)$, we have that $h_i(s_1, \ldots, s_{n-1}) = 0$ for $0 \leq i \leq r$. Since S is algebraically independent over K, it follows that $h_i = 0$ for $0 \leq i \leq r$. Thus $f = 0$. hence $S \cup \{u\}$ is algebraically independent over K.

$1 \Rightarrow 2$: Assume that $S \cup \{u\}$ is algebraically independent over K. Suppose $f(x) = \sum_{i=0}^n a_i x^i \in k(S)[x]$ is such that $f(u) = 0$. Then there exists a finite subset $\{s_1, \ldots, s_r\} \subseteq S$ such that $a_i \in K(s_1, \ldots, s_r)$ for $0 \leq i \leq n$. Let $f_i, g_i \in k[x_1, \ldots, x_r]$ be such that $a_i = f_i(s_1, \ldots, s_r)/g_i(s_1, \ldots, s_r)$.

Define $g = g_0 g_1 \ldots g_n$ and for $0 \leq i \leq n$, let $\overline{f}_i = g f_i / g_i = f_i g_0 \ldots g_{i-1} g_{i+1} \ldots g_n \in k[x_1, \ldots, x_r]$. Notice that for $0 \leq i \leq n$, $a_i = \overline{f}_i(s_1, \ldots, s_r)/g(s_1, \ldots, s_r)$, and so $f(x) = g(s_1, \ldots, s_r)^{-1} \sum_{i=0}^n \overline{f}_i(s_1, \ldots, s_r) x^i$.

Let $h(x_1, \ldots, x_r, x) = \sum_{i=1}^n \overline{f}_(x_1, \ldots, x_r) x^i$. Since $f(u) = 0$ and $g(s_1, \ldots, s_r) \neq 0$, it follows that $h(s_1, \ldots, s_r, u) = 0$. Since $S \cup \{u\}$ is algebraically independent over K, it follows that $h = 0$. And so, $\overline{f}_i = 0$ for $0 \leq i \leq n$. Hence, $a_i = 0$ for $0 \leq i \leq n$, and so $f = 0$.

Hence, u is transcendental over $K(S)$. □

Corollary 7.37. *Let F be an extension of K and $S \subseteq F$ be algebraically independent over K. Then TFAE:*

1. *S is a transcendence basis for F over K.*
2. *F is algebraic over $K(S)$.*

An analogy?
Vector Spaces over K

1. k-linear span $\langle S \rangle$ of S.
2. Basis = Independent Generating Set

Field extension F over K

1. K-algebraic closure of S, ie, $K(S)^{\text{alg}} \cap F$
2. Transcendence Basis = Independent Generating Set

Question: Suppose $S, T \subseteq F$ are transcendence bases over K. Does $|S| = |T|$?

Notation: From now on, we fix some extension F of K and write $\text{alg}_K(S) = K(S)^{\text{alg}} \cap F$.

Theorem 7.38. *The closure operator $\text{alg}_K(S)$ satisfies the following properties:*

1. *If $S \subseteq F$, then $S \subseteq \text{alg}_K(S)$.*
2. *$S, T \subseteq F$ and $S \subseteq T$ then $\text{alg}_K(S) \subseteq \text{alg}_K(T)$.*
3. *If $S \subseteq F$ then $\text{alg}_K(\text{alg}_K(S)) = \text{alg}_K(S)$*

4. *If* $S \subseteq F$ *and* $a, b \in F$ *satisfy* $b \in \mathrm{alg}_K(S \cup \{a\}) \setminus \mathrm{alg}_K(S)$*, then* $a \in \mathrm{alg}_K(S \cup \{b\}) \setminus \mathrm{alg}_K(S)$.

Proof. Homework □

The above result says that (F, alg_K) is a matroid.

Remark: The most important axiom is clearly 4, which is called the exchange property. The other axioms 1,2,3 are satisfied by every natural closure operator.

e.g., let G be a group, and for each $S \subseteq G$, let $cl(S)$ be the subgroup generated by S.

Definition 7.25. *Let* (X, cl) *be a matroid.*

1. *The subset* $I \subset X$ *is dependent iff there exists* $x \in I$ *such that* $x \in cl(I \setminus \{x\})$*. Otherwise,* I *is independent.*
2. *The subset* $B \subseteq X$ *is a basis iff* B *is an independent subset of* X *such that* $cl(B) = X$.

Question: Does every matroid have a basis?

Definition 7.26 (Dependent Sets and Bases)**.** *Let* (X, cl) *be a matroid.*

1. *The subset* $I \subseteq X$ *is dependent iff there is* $x \in I$ *such that* $x \in \mathrm{cl}(I \setminus \{x\})$*. Otherwise independent.*
2. *A basis is an independent set* I *such that* $cl(I) = X$.

Warning: There exist matroids without bases.

e.g. consider the closure operation cl on $\mathbb{N}$ defined by $\mathrm{cl}(S) = S$ if $|S| < \infty$, $\mathrm{cl}(S) = \mathbb{N}$ if $|S| = \infty$.

Remark: Of course, in the matroid (F, alg_K), matroid independence is exactly the same as algebraic independence.

Lemma 7.39 (5.7)**.** *Suppose that* $I \subseteq X$ *is independent and* $x \in X \setminus I$*. Then TFAE:*

1. $I \cup \{x\}$ *is independent.*
2. $x \notin \mathrm{cl}(I)$.

Proof. (1) $\Rightarrow$ (2): By definition.

(2) $\Rightarrow$ (1): Suppose that $I \cup \{x\}$ is not independent. We claim that $x \in \mathrm{cl}(I)$. If not, there exists $y \in I$ such that $y \in \mathrm{cl}(I \setminus \{y\} \cup u)$. Since I is independent, $y \notin \mathrm{cl}(I \setminus \{y\})$. Thus $y \in \mathrm{cl}((I \setminus \{y\}) \cup \{x\}) \setminus \mathrm{cl}(I \setminus \{y\})$. Hence $x \in \mathrm{cl}((Y \setminus \{y\}) \cup \{y\}) = \mathrm{cl}(I)$ as required. □

As an immediate consequence, we obtain:

Lemma 7.40. *If* $I \subseteq X$ *is independent then TFAE:*

1. *I is a basis*

2. $\mathrm{cl}(I) = X$.

Theorem 7.41. *If B is a fintie basis of X, then every basis C satisfies $|C| = |B|$.*

Proof. The result is clear if $B = \emptyset$. Hence, we can suppose that $B = \{b_1, \ldots, b_n\}$. Let C be any basis of X.

Claim: There exists $c_1 \in C$ such that $\{c_1, b_2, \ldots, b_n\}$ is a basis of X. Since $\mathrm{cl}(\{b_2, \ldots, b_n\}) \neq X = \mathrm{cl}(C)$.

Thus there exists $c_1 \in C$ such that $c_1 \notin \mathrm{cl}(\{b_2, \ldots, b_n\})$. In particular, $\{c_1, b_2, \ldots, b_n\}$ is independent. Also, $c_1 \in \mathrm{cl}(\{b_1, \ldots, b_n\}) \setminus \mathrm{cl}(\{b_2, \ldots, b_n\})$ and so $b_1 \in \mathrm{cl}(\{c_1, b_2, \ldots, b_n\})$. It follows that $\mathrm{cl}(\{c_1, b_2, \ldots, b_n\}) = X$.

Similarly, there exists $c_2 \in C$ such that $\{c_1, c_2, b_3, \ldots, b_n\}$ is a basis. Continuing in this fashion, we eventually obtain $\{c_1, \ldots, c_n\} \subseteq C$ which is a basis. Thus, $C = \{c_1, \ldots, c_n\}$. □

Definition 7.27 (Finitary)**.** *The matroid (X, cl) is finitary iff whenever $x \in \mathrm{cl}(S)$, there exists a finite $S_0 \subseteq S$ such that $x \in \mathrm{cl}(S_0)$.*

Example: (F, alg_K) is a finitary matroid.

Lemma 7.42. *If (X, cl) is a finitary matroid, then X has a basis.*

Lemma 7.43 (5.11)**.** *If (X, d) is a finitary matroid, then X has a basis.*

Proof. We can apply Zorn to the poset of independent subsets of X. □

Theorem 7.44. *If (X, cl) is a finitary matroid, then any two bases have the same cardinality.*

Proof. Let B, C be bases of X. We can suppose B is infinite. It follows that C is also infinite. For each $b \in B$, there exists a finite subset $C_b \subseteq C$ such that $b \in \mathrm{cl}(C_b)$.

Hence, $\mathrm{cl}(\cup_{b \in B} C_b) = X$ and so $C = \cup_{b \in B} C_b$. Hence $|C| \leq |B| \aleph_0 = |B|$. Similarly, $|B| \leq |C|$ and so $|B| = |C|$. □

Definition 7.28 (Transcendence Degree)**.** *If F is an extension field of K then the transcendence degree is $\mathrm{tr\,dim}\, F/K = |S|$ where S is any transcendence basis of F over K. If K is the prime subfield of F, we write $\mathrm{tr\,dim}\, F$.*

Theorem 7.45. *Suppose F, E are algebraically closed fields. Then TFAE:*

1. *$F \simeq E$*

2. *$\mathrm{char}\, F = \mathrm{char}\, E$ and $\mathrm{tr\,dim}\, E = \mathrm{tr\,dim}\, F$.*

Proof. (1) $\Rightarrow$ (2): Obvious.

(2) $\Rightarrow$ (1): We can suppose that E and F are both extensions of the same prime field K. Let $\operatorname{tr}\dim E = \operatorname{tr}\dim F = \lambda$, and let $X = \{x_\alpha : \alpha < \lambda\}$ and $Y = \{y_\alpha : \alpha < \lambda\}$ be transcendence bases of E, F. Then we can define an isomorphism $\varphi : k(X) \to k(Y) : x_\alpha \mapsto y_\alpha$.

This extens to an isomorphism $\overline{\varphi} : F = K(X)^{\text{alg}} \to K(Y)^{\text{alg}} = E$. □

Corollary 7.46. *Fix some characteristic $p \geq 0$.*

1. *There are exactly $\aleph_0$ countable algebraically closed fields of* $\operatorname{char} p$ *up to isomorphism.*

2. *If κ is any uncountable cardinal, there exists a unique algebraically closed field of* $\operatorname{char} p$ *and cardinality κ up to isomorphism.*

Proof. 1. For each $0 \leq n \leq \aleph_0$, there exists a unique algebraically closed field of characteristic p and transcendence degree n up to isomorphism.

2. It is easily checked if F is any uncountable field, then $\operatorname{tr}\dim F = |F|$. The result follows.

□

6. The Hilbert Nullstellensatz

Let K be a field and let F be a field extension. If I is an ideal of $K[x_1, \ldots, x_n]$, then $V_F(I) = \{\vec{a} \in F^n : p(a) = 0 \text{ for all } p \in I\}$.

In this section, we prove the following:

Theorem 7.47 (Hilbert Nullstellensatz)**.** *Suppose F is an algebraically closed extension of K. If I is a proper ideal of $K[x_1, \ldots, x_n]$, then $V_F(I) \neq \emptyset$.*

As we will see, the above theorem is equivalent to:

Theorem 7.48. *Let K be a field and let $K[a_1, \ldots, a_n]$ be a finitely generated ring extension. If $K[a_1, \ldots, a_n]$ is a field, then $K[a_1, \ldots, a_n]$ is algebraic over K.*

We will prove the equivalence:

Proof. Proof that the above implies Nullstellensatz: Let I be a proper ideal of $K[x_1, \ldots, x_n]$. Then there exists a maximal M such that $M \supseteq I$. Consider the field $k[x_1, \ldots, x_n]/M = k[a_1, \ldots, a_n]$ where $a_i = x_i + M$.

By assumption, $k[\vec{a}]$ is algebraic over K. Since F is algebraically closed, there exists an embedding $\varphi : k[\vec{a}] \to F$ over F. Then clearly $(\varphi(a_1), \ldots, \varphi(a_n))$ is a zero of I in F^n. Thus $V_F(I) \neq \emptyset$.

The other implication: Let $k[a_1, \ldots, a_n]$ be a field which is finitely generatoed over K as a ring extension. Consider the ring homomorphism $\varphi : k[x_1, \ldots, x_n] \to k[a_1, \ldots, a_n]$ by $x_i \mapsto a_i$.

Then $\ker \varphi = M$ is a maximal ideal of $K[x_1, \ldots, x_n]$. By the Nullstellensatz, M has a zero $(\xi_1, \ldots, \xi_n) \in (K^{\text{alg}})^n$. Consider teh homomorphism

$\psi : K[x_1, \ldots, x_n] \to K^{\text{alg}}$, $x_i \mapsto \xi_i$. Then $M \subseteq \ker \psi$, and so $\ker \psi = M$. Thus $K[a_1, \ldots, a_n] \simeq K[\xi_1, \ldots, \xi_n]$. Since each $\xi_i \in K^{\text{alg}}$, it follows that $K[\vec{a}]$ is an algebraic extension of K. □

We will next prove theorem 22.

Lemma 7.49. *Let $R \subseteq S \subseteq T$ be rings such that R is Nötherian and $T = R[t_1, \ldots, t_n]$ is finitely generated as a ring over R. If T is finitely generated as an S module, then S is also finitely generated as a ring over R.*

Proof. :et $\{w_1, \ldots, w_m\}$ be a finite system of generators of the S-module T, which includes $t_1, \ldots, t_n\}$. Then for each $1 \leq i, j \leq m$ there exist $a_\ell^{ij} \in S$ for $1 \leq \ell \leq m$ such that $w_i w_k = \sum_{\ell=1}^m a_\ell^{ik} w_\ell$.

Consider the ring $S' = R[\{a_\ell^{ik} : 1 \leq i, k, \ell \leq m\}]$. Then $T = S'w_1 + \ldots + S'w_m$.

Since every product of powers of $\{t_1, \ldots, t_n\}$ lies in the right hand side. Since S' is a finitely generated ring extension of a Nötherian ring, it follows that S' is also Nötherian. Since T is a finitely generated S'-module, it follows that T is a Nötherian S'-module. Since $S' \subseteq S \subseteq T$, it follows that S is a finitely generated S'-module. Since S' is finitely generated as a ring extension of R, it follows that S is also finitely generated as a ring extension of R. □

Lemma 7.50. *Let $E = K(z_1, \ldots, z_t)$ be the field of rational functions in the variables $z_1, \ldots, z_t$ where $t \geq 1$. Then E is NOT finitely generated as a ring over K.*

Proof. Suppose that $X = \{f_1/g_1, \ldots, f_s/g_s\}$ satisfies $E = K[X]$, where $f_i, g_i \in k[z_1, \ldots, z_n]$. Let p be any irreducible polynomial which doesn't divide any of teh g_i. Then clearly $\frac{1}{p} \notin K[X]$, contradiction. □

We will now prove Theorem 22.

Proof. Let $K[a_1, \ldots, a_n]$ be a field which is finitely generated over K as a ring. Suppose that $k[\vec{a}]$ isn't algebraic over K. Let $\{z_1, \ldots, z_t\}$ be a transcendence basis of $K[\vec{a}]$ over K where $t \geq 1$, and let $S = K(z_1, \ldots, z_t)$. Then $K[\vec{a}]$ is a finitely generated algebraic extension of S.

And so, $K[\vec{a}]$ is finitely generated as an S-module. Hence, applying Lemma 8, we see that S is finitely generated as a ring over K. This contradicts Lemma 9. □

(The above method of proof of the Nullstellensatz is due to Zariski and Artin)

Theorem 7.51. *Let F be an algebraically closed extension of K and let I be an ideal of $K[x_1, \ldots, x_n]$. If $f \in K[x_1, \ldots, x_n]$, then TFAE:*

1. *$f(\vec{a}) = 0$ for all $\vec{a} \in V_F(I)$.*
2. *$f \in \operatorname{Rad} I$*

Proof. $2 \Rightarrow 1$: Obvious.

$1 \Rightarrow 2$: [Rabinowitz's Trick] We can suppose that $f \neq 0$. Consider the ideal J of $K[x_1, \ldots, x_n, y]$ generated by $I \cup \{1 - yf\}$. Then clearly $V_F(J) = \emptyset$, and so $J = K[x_1, \ldots, x_n, y]$, hence, there exist polynomials $g_i \in k[x_1, \ldots, x_n, y]$ and $h_i \in I$ such that $g_0(1 - yf) + \sum_i g_i h_i = 1$. Substituting $\frac{1}{f}$ for y in this equation, we have $a_1/f^{n_1}h_1 + \ldots + a_r/f^{n_r}h_r$ where $a_i \in K[x_1, \ldots, x_n]$ and $n_i \geq 0$. Clearing the denominators, we obtain $f^m = b_1h_1 + \ldots + b_rh_r$ for some $m \geq 0$, $b_i \in k[x_1, \ldots, x_n]$. Thus, if $m \geq 1$, then $f \in \operatorname{Rad} I$. If $m = 0$, then $1 \in I$, and so $I = K[\vec{x}]$, and the result is trivial. □

In particular, suppose that k is algebraically closed and reconsider the injective map from algebraic subsets of k^n to radical ideals of $k[x_1, \ldots, x_n]$ by $V \mapsto J(V)$. We have seen that this is injective.

Claim: The above map is also surjective.

Proof. If J is a radical ideal of $k[\vec{x}]$, then $V(J) \mapsto J$. □

8 Category Theory

Definition 8.1 (Category)**.** *A category is a class $\mathscr{C}$ of objects together with*

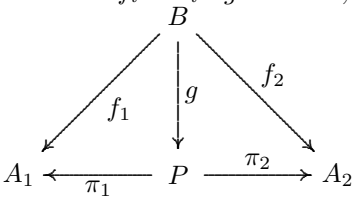
1. *A class of disjoin sets,* $\hom(A, B)$*, one for each pair of objects $A, B \in \mathscr{C}$*
2. *For each triple, $A, B, C \in \mathscr{C}$ we have a function from* $\hom(B, C) \times \hom(A, B)$ *to* $\hom(A, C)$*, called composition of morphisms, which is*
   (a) *Associative, that is, given $f : A \to B, g : B \to C, h : C \to D$, we have $(h \circ g) \circ f = h \circ (g \circ f)$*
   (b) *For each object $B \in \mathscr{C}$, there is a morphism called $1_B : B \to B$ such that for all $f : A \to B$ and $g : B \to C$, $1_B \circ f = f$ and $g \circ 1_B = g$.*

Definition 8.2 (Equivalence)**.** *In a category $\mathscr{C}$, a morphism $f : A \to B$ is an equivalence if there exists a morphism $g : B \to A$ such that $f \circ g = 1_B$, $g \circ f = 1_A$.*

If there is an equivalence from A to B, we say that A and B are equivalent.

Definition 8.3 (Products)**.** *Let $\mathscr{C}$ e a category and $\{A_i : i \in I\}$ a family of objects of $\mathscr{C}$.*

A product for the family is an object P of $\mathscr{C}$ together with maps $\pi_i : P \to A_i$ such that if $B \in \mathscr{C}$ has maps $f_i : B \to A_i$, then there is a unique map $g : B \to P$ such that $f_i = \pi_i \circ g$. That is, f_i factors through π_i.



Lemma 8.1. *If $(P, \{\pi_i\})$ and $(Q, \{\psi_i\})$ are both products of the family $\{A_i : i \in I\}$ then P and Q are equivalent.*

Proof. Since P is a product, $\exists! g : Q \to P$ such that $\psi_i = \pi_i \circ g$ and since Q is a product, $\exists! f : P \to Q$ such that $\pi_i = \psi_i \circ f$.

Then $\pi_i = \pi_i \circ g \circ f$ for all $i \in I$.

So $g \circ f : P \to P$ must be the unique option making this commute, so $g \circ f = 1_P$. Similarly, $f \circ g = 1_Q$. □

Products are defined using a universal property.

Definition 8.4 (Universal Object)**.** *An object I in $\mathscr{C}$ is universal (or initial) if $\forall C \in \mathscr{C}$ there is a unique morphism $f : I \to C$.*

Definition 8.5 (Couniversal Object)**.** *An object T in $\mathscr{C}$ is couniversal (or terminal) if $\forall C \in \mathscr{C}$ there is a unique morphism $g : C \to T$.*

Lemma 8.2. *If I and I' are universal for $\mathscr{C}$ then I and I' are equivalent. Similarly, two couniversal objects must be equivalent.*

Proof. Since I is universal, there is a unique morphism $f : I \to I'$.

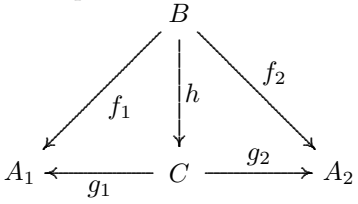
Since I' is universal, there is a unique morphism $g : I' \to I$.

As I is universal, $g \circ f = h = 1_I$, as we know that the identity morphism exists.

Similarly, $f \circ g = 1_{I'}$. □

Products are a special case. Given $\{A_i : i \in I\}$ objects of some category $\mathscr{C}$, define the category $\mathscr{C}_A$ whose objects are the objects B of $\mathscr{C}$ with maps $f_i : B \to A_i$ for each i.

A morphism $(B, \{f_i\}) \to (C, \{g_i\})$ in $\mathscr{C}_A$ is a morphism $h : B \to C$ of $\mathscr{C}$ such that $f_i = g_i \circ h$ for all i. That is, it satisfies



The product is then the couniversal object in $\mathscr{C}_A$.

Definition 8.6 (Covariant Functor)**.** *Let $\mathscr{C}$ and $\mathscr{D}$ be two categories.*

A covariant functor $T : \mathscr{C} \to \mathscr{D}$ is two functions, $T : \mathrm{ob}\,\mathscr{C} \to \mathrm{ob}\,\mathscr{D}$ and $T : \mathrm{mor}\,\mathscr{C} \to \mathrm{mor}\,\mathscr{D} : \hom(C, C') \mapsto \hom(T(C), T(C'))$ such that $T(1_C) = 1_{T(C)}$ for all $C \in \mathscr{C}$ and $T(f \circ g) = T(f) \circ T(g)$

Example: Let $\mathscr{G}$ be the category of groups. Fix $g \in \mathscr{G}$.

Then $\hom(G, -) : \mathscr{G} \to Sets : H \mapsto \hom(G, H)$ is a covariant functor. If $H \to H'$ is a homomorphism, then $\tilde{h} : \hom(G, H) \to \hom(G, H') : \varphi \mapsto h \circ \varphi$

Definition 8.7 (Contravariant Functor)**.** *Let $\mathscr{C}$ and $\mathscr{D}$ be two categories.*

A covariant functor $T : \mathscr{C} \to \mathscr{D}$ is two functions, $T : \operatorname{ob}\mathscr{C} \to \operatorname{ob}\mathscr{D}$ and $T : \operatorname{mor}\mathscr{C} \to \operatorname{mor}\mathscr{D} : \hom(C, C') \mapsto \hom(T(C'), T(C))$ such that $T(1_C) = 1_{T(C)}$ for all $C \in \mathscr{C}$ and $T(f \circ g) = T(g) \circ T(f)$

Definition 8.8 (Opposite Category)**.** *Let $\mathscr{C}$ be a category. The opposite category has objects $\operatorname{ob}\mathscr{C}$ and morphisms $\hom(A^{op}, B^{op}) = \hom(B, A)$*

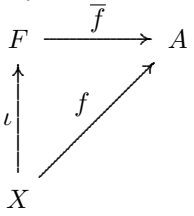
There is a contravariant functor from $\mathscr{C} \to \mathscr{C}^{op}$. And given a contravariant functor $\mathscr{C} \to \mathscr{D}$, we can define a covariant functor $\mathscr{C}^{op} \to \mathscr{D}$.

Definition 8.9 (Natural Transformation)**.** *Let $\mathscr{C}, \mathscr{D}$ be categories and let $S, T : \mathscr{C} \to \mathscr{D}$ be covariant functors.*

A natural transformation $\alpha : S \to T$ is a function that assigns to each object of $\mathscr{C}$ a morphism $\alpha_C : S(C) \to T(C)$ of $\mathscr{D}$ such that $\forall f : C \to C'$ of $\mathscr{C}$ the following diagram commutes.

$$\begin{array}{ccc} S(C) & \xrightarrow{\alpha_C} & T(C) \\ \Big\downarrow{\scriptstyle S(f)} & & \Big\downarrow{\scriptstyle T(f)} \\ S(C') & \xrightarrow{\alpha_{C'}} & T(C') \end{array}$$

Definition 8.10 (Free Object)**.** *If $\mathscr{C}$ is a category whose objects are all sets and every morphism is function, then an object $F \in \mathscr{C}$ is free on a set X if $\exists! \iota : X \to F$ a set inclusion such that $\forall f : X \to A$ of sets, for $A \in \operatorname{ob}\mathscr{C}$, $\exists! \overline{f} : F \to A$ such that the following diagram commutes.*



9 Representation Theory

Recall that if G is a finite group with $|G| = p^n$ for some prime p, then $Z(G) \neq 1$. Hence, there exists some $t \geq 1$ such that $Z_t(G) = G$.

Theorem 9.1. *If G is a finite p-group, then G is nilpotent.*

In this section, we will prove:

Theorem 9.2 (Burnside)**.** *If G is a finite group and $|G| = p^a q^b$ for some primes p, q, then G is solvable.*

Example: Consider the dihedral group D_5. Then $|D_5| = 10$ and $Z(D_5) = 1$. Thus, D_5 is not nilpotent.

Example: Consider $A_5 = 2^2 * 3 * 5$.

Basic Strategy: Show that G isn't simple, assuming G isn't cyclic of order p. Then the result follows by induction.

Definition 9.1 (k-Representation)**.** *Let G be a finite group and let k be a field. Then a k-representation of G is a homomorphism $\pi : G \to GL(V) : g \mapsto \pi_g$ where $0 \neq V$ is a finite dimensional vector space over k.*

The degree of π is $\deg \pi = \dim_k V$.

Remark: We usually just write representation.

Examples:

1. A representation of degree 1 is just a homomorphism $\pi : G \to k^*$.
2. Suppose that G acts on the finite set X. Let $kX = \oplus_{x \in X} k e_x$. Then the corrsponding permutation representation is the homomorphism $\pi : G \to GL(kX)$ defined by $\pi_g(e_x) = e_{g \cdot x}$.

Definition 9.2 (G-invariant Subspace)**.** *Let $\pi : G \to GL(V)$ be a representation. Then the subspace $W \leq V$ is G-invariant iff $\pi_g[W] = W$ for all $g \in G$.*

Examples: $0, V$ are G-invariant subspaces - the trivial invariant subspaces.

Definition 9.3 (Subrepresentation)**.** *If W is a nonzero G-invariant subspace, then the associated subrepresentation is the homomorphism $\pi|_W : G \to GL(W)$ by $g \mapsto \pi_g|_W$.*

Definition 9.4 (Irreducible)**.** *The representation $\pi : G \to GL(V)$ is irreducible iff there are no nontrivial G invariant subspaces.*

Example: If $\deg \pi = 1$, then π is irreducible.

Question: Is every representation a direct sum of irreducible representations?

Theorem 9.3 (Maschke)**.** *Suppose that $p = \operatorname{char} k \not| |G|$.*

If $\pi : G \to GL(V)$ is a k-representation, and $W \leq V$ is a nontrivial G-invariant subspace, then there exists a G-invariant subspace $U < V$ such that $V = W \oplus U$.

Proof. Let $S < V$ be any subspace such that $V = W \oplus S$ and let $\theta : V = W \oplus S \to W$, that is, $w + s \mapsto w$, be the associated projection.

Then $\theta(w) = w$ for all $w \in W$ and $\theta[V] \subseteq W$. Furthermore, if $\psi \in \hom_k(V, V)$ satisfies these two conditions, then there exists a corrsponding decomposition $V = W \oplus (1 - \psi)[V]$ where $(1 - \psi)[V] = \{v - \psi(v) : v \in V\}$.

Claim: Suppose that $\pi_g(\psi(v)) = \psi(\pi_g(v))$ for all $g \in G$ and $v \in V$. Then $(1 - \psi)[V]$ is G-invariant.

Proof of Claim: For all $g \in G$ and $v \in V$, we ave $\pi_g(v - \psi(v)) = \pi_g(v) - \pi_g(\psi(v)) = \pi_g(v) - \psi(\pi_g(v)) = (1 - \psi)[V]$. As π_g is an invertible linear transformation, we must have that $\pi_g((1 - \psi)[V]) = (1 - \psi)[V]$, and so the claim holds.

Thus, it is enough to find a G-invariant projection.

Let $\theta : V \to W$ be our original projection. Define $\psi : V \to V$ by $\psi(v) = \frac{1}{|G|}\sum_{g\in G} \pi_g\theta\pi_g^{-1}(v)$. This is the only point where we use the fact that $p = \operatorname{char} k \not| |G|$.

If $h \in G$, then $\pi_h\psi\pi_h^{-1} = \frac{1}{|G|}\sum_{g\in G} \pi_h\pi_g\theta\pi_g^{-1}\pi_h^{-1} = \frac{1}{|G|}\sum_{g\in G} \pi_{hg}\theta\pi_{hg}^{-1} = \frac{1}{|G|}\sum_{a\in G} \pi_a\theta\pi_a^{-1} = \psi$ and so $\pi_h\psi = \psi\pi_h$. Thus, it is enough to check that ψ satisfies conditions (i) and (ii).

(i): If $w \in W$ and $g \in G$ then $\pi_g(\theta(\pi_g^{-1}(w))) = \pi_g(\pi_g^{-1}(w)) = w$ since $\pi_g^{-1}[W] = W$.

Hence $\psi(w) = \frac{1}{|G|}\sum_{g\in G} \pi_g\theta\pi_g^{-1}(w) = w$

(ii): Finally, if $v \in V$ is arbitrary and $g \in G$, then $\pi_G(\theta(\pi_g^{-1}(v))) \in W$, since $\theta[V] \subseteq W$. Thus $\psi(v) \in W$. □

Corollary 9.4. *If* $\operatorname{char} k \not| |G|$ *then every* k*-representation of* G *decomposes into a direct sum of irreducible representations.*

Here if $\pi^i : G \to GL(V_i)$, $1 \le i \le d$, are representations then their direct sum is the representation $\phi = \pi^1 \oplus \ldots \oplus \pi^d = G \to GL(V_1 \oplus \ldots \oplus V_d)$, $\phi_g(v_1 + \ldots + v_d) = \pi_g^1(v_1) + \ldots + \pi_g^d(v_d)$ where $v_i \in V_i$ and $g \in G$.

Even more explicitly...if we choose a basis $\mathcal{B}_i$ of V_i, then each ϕ_g has the form of a block diagonal matrix, with respect to $\mathcal{B} = \cup_i \mathcal{B}_i$.

Convention: From now on, we shall only consider representations over $\mathbb{C}$. In particular, every representation will be a direct sum of irreducible representations.

A reminder of some linear algebra.

Let $M_n(\mathbb{C})$ be the ring of $n \times n$ matrices over $\mathbb{C}$. For each $A \in M_n(\mathbb{C})$, the characteristic polynomial is $\det(Ix - A) = |Ix - A|$. The roots of the characteristic polynomial are called characteristic roots or eigenvalues. The trace is the sum of the diagonal entries which is the sum of the eigenvalues counted with multiplicities.

Some basic results:

1. Suppose that $A \in M_n(\mathbb{C})$ and $B \in M_n(\mathbb{C})$ is invertible, then $|Ix - BAB^{-1}| = |B(Ix - A)B^{-1}| = |Ix - A|$. If particular, it makes sense to speak of the characteristic polynomial and trace of a linear transformation $f : V \to V$.

2. (Cayley-Hamilton) If $A \in M_n(\mathbb{C})$ and $p(x) = |Ix - A|$, then $p(A) = 0$. In particular, the minimal polynomial divides the characteristic polynomial.

Theorem 9.5. *1. Suppose that* $A, B \in M_n(\mathbb{C})$ *satisfy* $AB = BA$ *and let* $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ *be the characteristic roots of* A, B*. Then, after renumbering the* β_i *if necessary, the characteristic roots of* AB *are* $\alpha_1\beta_1, \ldots, \alpha_n\beta_n$*.*

2. If $p(x) \in \mathbb{C}[x]$ *, then the characteristic roots of* $p(A)$ *are* $p(\alpha_1), \ldots, p(\alpha_n)$

3. If A *is invertible, then the characteristic roots of* A^{-1} *are* $\alpha_1^{-1}, \ldots, \alpha_n^{-1}$*.*

Definition 9.5 (Character)**.** *If $\pi : G \to GL(V)$ is a representation, then the corresponding character is the function $\chi_\pi : G \to \mathbb{C}$ by $\chi_\pi(g) = \operatorname{tr}(\pi_g)$.*

The character χ_π is irreducible iff π is irreducible.

Lemma 9.6. *If $\pi : G \to GL(V)$ is a representation, then*

1. *$\chi_\pi(1) = \dim_{\mathbb{C}} V = \deg \pi$*
2. *$\chi_\pi(g) = \chi_\pi(hgh^{-1})$ for all $g, h \in G$.*

Proof. 1. Obvious.

2. Fix some basis $\mathcal{B}$ of V and let M_g be the corresponding matrix of π_g. Then
$$\chi_\pi(hgh^{-1}) = \operatorname{tr}(M_h M_g M_h^{-1}) = \operatorname{tr}(M_g) = \chi_\pi(g).$$

□

In particular, each character is a class function, ie, it is constant on every conjugacy class of G.

Definition 9.6 ($\mathrm{C}\ell(G)$)**.** $\mathrm{C}\ell(G) = \{f \in {}^G\mathbb{C}$ *is a class function* $\}$.

Lemma 9.7. *[(a)]*

1. *$\mathrm{C}\ell(G)$ is a vector space over $\mathbb{C}$.*
2. *$\dim_{\mathbb{C}} \mathrm{C}\ell(G) =$the number of conjugacy classes.*

Proof. (a) is trivial.

Clearly, the characteristic functions on the conjugacy classes of G form a basis. □

Remark, eventually we will show that the distinct irreducible characters form a basis of $\mathrm{C}\ell(G)$.

Lemma 9.8. *Let $\pi : G \to GL(V)$ be a representation.*

1. *If $g \in G$ then $\chi_\pi(g)$ is a sum of roots of unity. In particular, $\chi_\pi(g)$ is an algebraic integer.*
2. *If $g \in G$ then $\chi_\pi(g) = \overline{\chi_\pi(g)}$*
3. *If $g \in G$, then $|\chi_\pi(g)| \leq \deg \pi$. Furthermore $|\chi_\pi(g)| = \deg \pi$ iff $\pi_g = \lambda \operatorname{id}_V$ for some $\lambda \in \mathbb{C}$.*

Proof. Fix some basis $\mathcal{B}$ of V and let M_g be the matrix of π_g. Let $d = \dim_{\mathbb{C}} V = \deg \pi$.

1. Let $g \in G$ have order n. Then $M_g^n = I$. Hence, by Theorem 4, every characteristic root of M_g is an n^{th} root of unity. The result follows.

2. Let $\lambda_1, \ldots, \lambda_d$ be the characteristic roots of M_g. Then the characteristic roots of M_g^{-1} are $\lambda_1^{-1}, \ldots, \lambda_d^{-1}$. Since the $\lambda + i$ are roots of unity, $\lambda_i^{-1} = \overline{\lambda}_i$. The result follows.

3. Again, let $\lambda_1, \ldots, \lambda_d$ be the characteristic roots of M_g. Since each λ_i is a root of unity, we have $|\lambda_i| = 1$. HEnce $|\chi_\pi(g)| = |\lambda_1 + \ldots + \lambda_n| \leq |\lambda_1| + \ldots + |\lambda_d| = \deg \pi$.

   Furthermore, if $\xi, \eta \in \mathbb{C}^*$, then $|\xi + \eta| \leq |\xi| + |\eta|$, and $|\xi + \eta| = |\xi| + |\eta|$ iff $\eta = r\xi$ for some $r \in \mathbb{R}^+$.

   Thus, $|\chi_\pi(g)| = \deg \pi$ iff $\lambda_1 = \ldots = \lambda_d = \lambda \in \mathbb{C}$. Thus M_g satisfies two polynomial equations, $x^n - 1 = 0$ and $(x - \lambda)^d = 0$

   Hence, M_g satisfies the gcd of these polynomials, which must be $x - \lambda$, since $x^n - 1$ has no repeated roots.

□

Definition 9.7 (Intertwines)**.** *Suppose that $\pi : G \to GL(V)$ and $\rho : G \to GL(W)$ are representations, then the linear map $f : V \to W$ intertwines π and ρ iff for every $g \in G$, the following diagram commutes:*

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle \pi_g}\uparrow & & \uparrow{\scriptstyle \rho_g} \\ V & \xrightarrow{f} & W \end{array}$$

ie, f is a homomorphism between two G-actions. Let $\hom_G(\pi, \rho)$ be the vector space of intertwiners between π and ρ.

Examples: Suppose $\pi : G \to GL(V)$ is a representation and that $W \leq V$ is a G-invariant subspace. Let $f : V \to W$ be a G-invariant projection. Then $f \in \hom_G(\pi, \pi|_W)$.

We always have $0 \in \hom_G(\pi, \rho)$.

We always have that $\lambda \operatorname{id}_V \in \hom_G(\pi, \pi)$ for every $\lambda \in \mathbb{C}$.

Definition 9.8 (Equivalence)**.** *The represenations π and ρ are equivalent or isomorphic if there exists an invertible intertwiner between π and ρ.*

Theorem 9.9 (Schur's Lemma)**.** *Suppose that $\pi : G \to GL(V)$ and $\rho : G \to GL(W)$ are irreducible representations.*

1. *if π and ρ aren't equivalent, then $\hom_{\mathbb{C}}(\pi, \rho) = 0$. That is, the zero map $f \equiv 0$ is the only intertwiner between π and ρ.*

2. *If π and ρ are equivalent, then $\dim \hom_{\mathbb{C}}(\pi, \rho) = 1$, ie, if wlog $\pi = \rho$, then the only interetwiners are $\lambda \operatorname{id}_V$ for $\lambda \in \mathbb{C}$.*

Proof. [(a)]

Suppose $\dim_{\mathbb{C}} \hom_G(\pi, \rho) \neq 0$ and let $f : V \to W$ be a nonzero intertwiner. Clearly $\ker f$ is a G-invariant subspace of V. Since $\ker f \neq V$ and π is irreducible, $\ker f = 0$, and so f is injective.

Similarly, $\operatorname{Im} f$ is a G-invariant subspace of W. Since $\operatorname{Im} f \neq 0$ and ρ is irreduicble, it follows that $\operatorname{Im} f = W$. Thus, f is invertible and ρ, π are equivalent.

2. Since π, ρ are equivalent, we can suppose that $\pi = \rho$. It is now enough to show that if $f \in \hom_G(\pi, \pi)$, then $f = \lambda \operatorname{id}_V$ for some $\lambda \in \mathbb{C}$. Let λ be an eigenvalue of f. Then the corresponding eigenspace $U \neq 0$ and is clearly G-invariant. Since π is irreducible, it follows that $U = V$ and the result follows.

□

Corollary 9.10. *Suppose that $\pi : G \to GL(V)$ and $\rho : G \to GL(W)$ are irreducible representations and let $h : V \to W$ be any linear map. We define $\tilde{h} = \frac{1}{|G|} \sum_{g \in G} \rho_g^{-1} h \pi_g$. Then*

1. *If π and ρ are inequivalent, then $\tilde{h} = 0$.*
2. *if π and ρ are equal, then $\tilde{h} = \frac{\operatorname{tr}(h)}{\dim_{\mathbb{C}} V} \operatorname{id}_V$.*

Proof. First note that $\tilde{h}$ intertwines π and ρ. If π, ρ are inequivalent, then $\tilde{h} \equiv 0$.

Now suppose that π, ρ are equal. Then $\tilde{h} = \lambda \operatorname{id}_V$ for some $\lambda \in \mathbb{C}$. To evaluation λ, notice that $\lambda \dim_{\mathbb{C}} V = \operatorname{tr}(\tilde{h}) = \operatorname{tr}(h)$, and so $\lambda = \frac{\operatorname{tr}(g)}{\dim_{\mathbb{C}}(V)}$. □

Definition 9.9. *We define a scalar product on ${}^G\mathbb{C}$ by $\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\psi(g)}$.*

Theorem 9.11. *[(i)]*

1. *If χ_π is an irreducble character, then $\langle \chi_\pi | \chi_\pi \rangle = 1$*
2. *If χ_π, χ_ρ are irreducible characters and π, ρ aren't equivalent, then $\langle \chi_\pi | \chi_\rho \rangle = 0$.*

Proof Delayed.

Remark: Thus the distinct irreducible characters form a orthonormal set in $C\ell(G)$. WE shall soon see that they actually form an orthonormal basis. Already we see that there are only finitely many non-isomorphic irreducible representations, and this number is bounded above by the number of conjugacy classes.

Definition 9.10. *We defined a scalar product on ${}^G\mathbb{C}$ by $\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \phi(g) \overline{\psi(g)}$.*

Theorem 9.12. *If π and ρ are irreducible representations, then $\langle \chi_\pi, \chi_\rho \rangle = 1$ if π, ρ are equivalent and otherwise 0.*

Proof Postponed.

Corollary 9.13. *Let $\pi : G \to GL(V)$ be a representation and $V = W_1 \oplus \ldots \oplus W_k$ be a decomposition into irreducible representations.*

If $\rho : G \to GL(W)$ is an irreducible representation, then the rumber of $\pi|_{W_i}$ which are isomorphic to ρ is given by $\langle \chi_\pi, \chi_\rho \rangle$.

Proof. Let $\pi_i = \pi|_{W_i}$. Then $\chi_\pi = \chi_{\pi_1} + \ldots + \chi_{\pi_k}$.

Hence $\langle \chi_\pi, \chi_\rho \rangle = \langle \chi_{\pi_1} + \ldots + \chi_{\pi_k}, \chi_\rho \rangle = \langle \chi_{\pi_1}, \chi_\rho \rangle + \ldots + \langle \chi_{\pi_k}, \chi_\rho \rangle =$ the number of i such that π_i is isomorphic to ρ. □

Corollary 9.14. *Suppose that $\pi : G \to GL(V)$ and $\rho : G \to GL(W)$ are representations.*

1. *π and ρ are isomorphic iff $\chi_\pi = \chi_\rho$.*
2. *π is irreducible iff $\langle \chi_\pi, \chi_\pi \rangle = 1$.*

Proof. a) Immediate from previous corollary.

b) If $\pi = \ell_1 \pi_1 + \ldots + \ell_s \pi_s$ is a decomposition into irreducible representations, then $\langle \chi_\pi, \chi_\pi \rangle = \ell_1^2 + \ldots + \ell_s^2$. □

From now on, let $\pi_1, \ldots, \pi_h$ be the distinct irreducible representations of G, and let $n_i = \deg \pi_i$.

Definition 9.11. *Consider the action of G on itself by left multiplication and let $\rho : G \to GL(\mathbb{C}G)$ be the corresponding permutation representation, known as the regular representation. Thus $\mathbb{C}G = \oplus_{g \in G} \mathbb{C} e_g$, and for each $g \in g$ we have $\rho_g(e_t) = e_{gt}$.*

Lemma 9.15. *If ρ is the regular representatation of G, then $\chi_\rho(g) = |G|$ if $g = 1$ and 0 if $g \neq 1$.*

Proof. If $g = 1$, then $\chi_\rho(1) = \dim_{\mathbb{C}} \mathbb{C}G = |G|$.

If $g \neq 1$, then $\rho_g(e_t) = e_{gt} \neq e_t$, and so all the diagonal elements of the corresponding permutation matrix are zero. □

Corollary 9.16. *Every irreducible representation π_i is conmtained in the regular representation ρ with multiplicity $n_i = \deg \pi_i$.*

Proof. The multiplicity of π_i in ρ is given by

$$\begin{aligned}\langle \chi_\rho, \chi_{\pi_i} \rangle &= \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \overline{\chi_{\pi_i}(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \chi_{\pi_i}(g^{-1}) \\ &= \frac{1}{|G|} \chi_\rho(1) \chi_{\pi_i}(1) \\ &= \frac{1}{|G|} |G| \deg \pi_i \\ &= n\end{aligned}$$

□

Corollary 9.17. $|G| = n_1^2 + \ldots + n_h^2$.

Proof. $|G| = \dim_{\mathbb{C}} \mathbb{C}G = \sum_{i=1}^h n_i \deg \pi_i = n_1^2 + \ldots + n_h^2$. □

Next we will reluctantly turn to the proof of theorem 7.15

Proof. Let $\pi : G \to GL(V)$ and $\rho : G \to GL(W)$ be (not necessarily distinct) irreducible representations. Fixing bases of V and W, let $A_g = (a_{ij}(g))$ and $B_g = (b_{k\ell}(g))$ be the corresponding matrices of π_g, ρ_g. (If $\pi = \rho$, we choose $A_g = B_g$).

Consider any linear map $h : V \to W$ and let $C = (c_{\ell i})$ be the corresponding $m \times n$ matrix, where $\dim_{\mathbb{C}} V = n$ and $\dim_{\mathbb{C}} W = m$. Let $D = (d_{jk})$ be the matrix corrsponding to $\tilde{h} = \frac{1}{|G|} \sum_{g \in G} \rho_g^{-1} h \pi_g$.

Then $d_{jk} = \frac{1}{|G|} \sum_{\substack{i\ell \\ g \in G}} b_{k\ell}(g^{-1}) c_{\ell i} a_{ij}(g)$.

First suppose that π, ρ are not equivalent. Then $\tilde{h}$ is the zero map, and so each $d_{kj} = 0$. Regard the RHS of the above as a linear form in the variables $c_{\ell i}$.

Since the form vanishes identically, each coefficient is 0. Hence, Claim 1: If $\pi \neq \rho$, then for all k, ℓ, i, j, we have $\frac{1}{|G|} \sum_{g \in G} b_{k\ell}(g^{-1}) a_{ij}(g) = 0$.

It follows that $\langle \chi_\pi, \chi_\rho \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\pi(g) \chi_\rho(g^{-1}) = \frac{1}{|G|} \sum_{g \in G} \left(\sum_i a_{ii}(g) \right) \left(\sum_k b_{kk}(g) \right) = \sum_{i,k} \frac{1}{|G|} \sum a_{ii}(g) b_{kk}(g) = 0$.

ext suppose that $\pi = \rho$. Then we have that $\tilde{h} = \mathrm{tr}(g)/\dim_{\mathbb{C}} V \,\mathrm{id}$. Arguing as in the previous case, we see that if $k \neq j$, then $d_{kj} = 0$, and so for all ℓ, i, we have $\frac{1}{|G|} \sum_{g \in G} a_{k\ell}(g^{-1}) a_{ij}(g) = 0$.

In particular, Claim 2: If $k \neq j$, then $\frac{1}{|G|} \sum_{g \in G} a_{kk}(g^{-1}) a_{jj}(g) = 0$.

Now suppose that $k = j$ and choose h such that $c_{\ell i} = 1$ if $\ell = i = k$ and 0 otherwise.

Then $\mathrm{tr}(h) = 1$. Hence the above formulae give Claim 3: for each $1 \leq k \leq n = \dim_{\mathbb{C}} V$, $\frac{1}{|G|} \sum a_{kk}(g^{-1}) a_{kk}(g) = \frac{1}{n}$. Applying Claim 2 and Claim

3, we get $\langle \chi_\pi, \chi_\pi \rangle = \frac{1}{|G|} \sum \chi_\pi(g)\chi_\pi(g^{-1}) = \sum_{i,j} \frac{1}{|G|} \sum_{g \in G} a_{ii}(g) a_{kk}(g^{-1}) = \sum_k \frac{1}{|G|} \sum_{g \in G} a_{kk}(g) a_{kk}(g^{-1}) = n \frac{1}{n} = 1$.

This concludes the proof. □

Theorem 9.18. *The characters $\chi_{\pi_1}, \ldots, \chi_{\pi_h}$ are an orthonormal basis for $C\ell(G)$.*

Corollary 9.19. *h = the number of conjugacy classes of G.*

Proof. The characteristic functions of the conjugacy classes of G form a basis of $C\ell(G)$. □

Corollary 9.20. *If G is abelian, then every irreducible representation of G has degree 1.*

Proof. Since G is abelian, $h = |G|$. As $G = n_1^2 + \ldots + n_{|G|}^2$, $n_i = 1$ for all i. □

Notation: Irreducible representations $\pi_1, \ldots, \pi_h$, irreducible characters $\chi_1, \ldots, \chi_h$, conjugacy classes $C_1, \ldots, C_h$, and Fixed representative $g_i \in C_i$.

For each group we have the character table of G.

	C_1	$\ldots$	C_j	$\ldots C_h$	
χ_1			$\vdots$		
$\vdots$			$\vdots$		
χ_i	$\ldots$	$\ldots$	$\chi_i(g_j)$	$\ldots$	$\ldots$
$\vdots$			$\vdots$		
χ_h			$\vdots$		

For A_4, we get

	1	(12)(34)	(123)	(132)
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4	3	-1	0	0

The first three are the representations of C_3, a homomorphic image of A_4, but now we must determine π_4.

Consider the action of A_4 on $X = \{1, 2, 3, 4\}$ and let $\varphi : A_4 \to GL(\mathbb{C}X)$ be the corresponding permutation representation. Then $\chi_\varphi(g) = \text{fix}(g)$, the number of fixed points of g, which is $\chi_1 + \chi_4$. Note the following A_4-invariant decomposition.

So $\mathbb{C}X = \mathbb{C}v_x \oplus V_0$ where $v_x = e_1 + e_2 + e_3 + e_4$ and $V_0 = \sum_i a_i e_i | a_1 + a_2 + a_3 + a_4 = 0\}$. Thus χ_4 is the character of $\varphi|_{V_0}$.

Remark: Suppose that G acts 2-transitively on X and $\pi : G \to GL(\mathbb{C}X)$ is the corresponding permutation representation. Then $\chi_\pi - 1$ is an irreducible character.

Proof. As above, we have a G-invariant decomposition $\mathbb{C}X = \mathbb{C}v_x \oplus V_0$, so $\chi_\pi - 1$ is the character of $\pi|_{V_0}$. Hence, it's enough to show that $\langle \chi_\pi, \chi_\pi \rangle = 2$.

Claim: $\sum_{g\in G} \mathrm{fix}(g)^2 = 2|G|$.

Assuming the claim, $\langle \chi_\pi, \chi_\pi \rangle = \frac{1}{|G|} \sum_{g\in G} \chi_\pi(g)\overline{\chi_\pi(g)} = \frac{1}{|G|} \sum_{g\in G} \mathrm{fix}(g)^2 = 2$.

To prove the claim, we count the number of elements of $\Omega = \{\langle a, b, g\rangle \in X \times X \times G | g(a) = a, g(b) = b\}$ in two ways.

(1) For each $g \in G$, the number of elements $\langle a, b, g\rangle \in \Omega$ is $\mathrm{fix}(g)^2$, thus $|\Omega| = \sum_{g\in G} \mathrm{fix}(g)^2$.

(2) For each $a \in X$, the numebr of elmeents $\langle a, b, g\rangle \in \Omega$ is given by $\sum_{b\in X} |G_{a,b}| = |G_a| + \sum_{b\in X\setminus\{a\}} |G_{a,b}| = |G_a| + [G_a : G_{a,b}]|G_{a,b}|$ by 2-transitivity, and this is $|G_a| + |G_a| = 2|G_a|$. Thus, $|\Omega| = \sum_{a\in X} 2|G_a| = 2[G : G_a]|G_a| = 2|G|$. □

To explain why the columns of a character table are orthogonal, recall that $\frac{1}{|G|} \sum_{g\in G} \chi_i(g)\overline{\chi_j(g)} = \delta_{ij}$.

Thus $\frac{1}{|G|} \sum_{k=1}^{h} |C_k|\chi_i(g_k)\overline{\chi_j(g_k)} = \delta_{ij}$. Or $\sum_{k=1}^{h} \sqrt{\frac{|C_k|}{|G|}}\chi_i(g_k)\overline{\sqrt{\frac{|C_k|}{|G|}}\chi_j(g_k)} = \delta_{ij}$

In other words, the rows of the matrix with ij term $\sqrt{\frac{|C_k|}{|G|}}\chi_i(g_l)$ form an orthonormal basis of $\mathbb{C}^h$. In other words, the matrix is unitary. If follows that the columns are also orthonomal, thus $\sum_{i=1}^{h} \sqrt{\frac{|C_k|}{|G|}}\chi_i(g_k)\overline{\sqrt{\frac{|C_\ell|}{|G|}}\chi_i(g_\ell)} = \delta_{k\ell}$.

And so, $\frac{\sqrt{|C_k||C_\ell|}}{|G|} \sum_{i=1}^{h} \chi_i(g_k)\overline{\chi_i(g_\ell)} = \delta_{k\ell}$.

Hence $\sum_{i=1}^{h} \chi_i(g_k)\overline{\chi_i(g_\ell)} = \frac{|G|}{|C_k|}\delta_{kl}$.

In summary we have proved:

Theorem 9.21 (The Orthogonality Relations)**.** *[(a)]*

1. $\frac{1}{|G|} \sum_{g\in G} \chi_i(g)\chi_j(g^{-1}) = \delta_{ij}$.
2. $\sum_{i=1}^{h} \chi_i(g_k)\chi_i(g_\ell^{-1}) = \frac{|G|}{|C_k|}\delta_{k\ell}$.

In order to prove Burnside's Theorem, we only require:

Theorem 9.22 (Folklore)**.** *For each $1 \le i, k \le h$, the number $\frac{|C_k|}{\deg \pi_i}\chi_i(g_k)$ is an algebraic integer.*

Proof Postponed.

Before proving Burnside, we prove

Theorem 9.23. *For each $1 \le\le h$, the degree $\deg \pi_i$ divides $|G|$.*

Proof. By the first orthogonality relation, we have $\sum_{i=1}^{h} |C_k|\chi_i(g_k)\chi_i(g_k^{-1}) = |G|$. And so, $\sum_{i=1}^{h} \frac{|C_k|}{\deg \pi_i}\chi_i(g_k)\chi_i(g_k^{-1}) = \frac{|G|}{\deg \pi_i}$, which is a sum of products of algebraic integers, and so is an algebraic integer. Hence, $\frac{|G|}{\deg \pi_i}$ is a rational algebraic integer. □

Burnside's Theorem is an "easy" consequence of the following slightly technical result which explains most of the zeros in our above character tables.

Theorem 9.24. *If* $(|C_k|, \deg \pi_i) = 1$*, then either*

1. $\chi_i(g_k) = 0$*, or*
2. $\chi_i(g) = \deg \pi_i \omega$ *for some root of unity* ω*, in which case* $\pi_i(g) = \omega I$ *is a scalar matrix.*

Proof Postponed.

Now we can prove Burnside.

Proof. Suppose that G is a counterexample of minimal order.

Then G must be a simple nonabelian group of order $|G| = p^a q^b$ for some primes $p \neq q$ and $a, b \geq 1$.

Let Q be a Sylow q-subgroup of G and let $1 \neq g \in Z(Q)$. Since $Q \leq C_G(g)$ and $|g^G| = [G : C_G(c)]$, it follows that $|g^G| = p^c$ for some $c \geq 1$. Let $g \in C_k$.

Let $\pi_1 = 1, \pi_2, \ldots, \pi_h$ be the irreducible representations of G. Consider some $2 \leq \ell \leq h$. If $p | \deg \pi_\ell$, then we can write $\deg \pi_\ell = pd_\ell$. On the other hand, if $p \not| \deg \pi_\ell$, then $(|C_k|, \deg \pi_\ell) = 1$. Since G is simple and nonabelian, we must havde that $\chi_\ell(g) = 0$ for each such ℓ.

Appealing to the second orthogonality condition, we see that $0 = \sum_{\ell=1}^{h} \chi_\ell(g)\chi_\ell(1) = 1 + \sigma \sum_{p | \deg \pi_\ell}^{\ell \geq 2} \chi_\ell(g) \deg \pi_\ell = 1 + p \sum d_\ell \chi_\ell(g)$

Thus, $-1/p = \sum d_\ell \chi_\ell(g)$ is an algebraic integer. □

We still have three things to prove that we have delayed.

First we prove Theorem 12.

Proof. Suppose $\pi_i(g_k)$ isn't a scalar matrix. Then, let $c_k = |C_k|$ and $n_i = \deg \pi_i$. By Theorem 10, $\frac{|C_k|}{\deg \pi_i} \chi_i(g_k)$ is an algebraic integer. Let $\alpha = \chi_i(g_k)/\deg \pi_i$.

Claim: α is an algebraic integer.

Proof of claim: Since $(C_k, n_i) = 1$, there exist $a, b \in \mathbb{Z}$ such that $ac_k + bn_i = 1$. Hence $\alpha = ac_k\alpha + bn_i\alpha = a\frac{|C_k|}{\deg \pi_i}\chi_i(g_k) + b\chi_i(g_k)$ is an algebraic integer.

Recall that $\chi_i(g_k) = \omega^{m_1} + \ldots + \omega^{m_{n_i}}$ for a suitably chosent root ω of unity. Also, since $\pi_i(g_k)$ isn't a scalar matrix, Lemma 3c implies that $|\chi_i(g_k)| < \deg \pi_i$ and so $|\alpha| < 1$. Let $\alpha = \alpha_1, \ldots, \alpha_r$ be the distinct conjugates of α over $\mathbb{Q}$. Then $\alpha_s = \omega_s^{m_1} + \ldots + \omega_s^{m_{n_i}}$ for some root of unity ω_s. It follows that each $|\alpha_s| < 1$.

Let $E = \mathbb{Q}(\alpha)$ and consider $N_{\mathbb{Q}}^E(\alpha) = \alpha_1 \ldots \alpha_r$. Since α is an algebraic integer, it follows that $N_{\mathbb{Q}}^E(\alpha) \in \mathbb{Z}$. Since $|N_{\mathbb{Q}}^E(\alpha)| < 1$, it follows that $N_{\mathbb{Q}}^E(\alpha) = 0$. And hence, $\alpha = \chi_i(g_k)/\deg \pi_i = 0$. □

Next, we will prove Theorem 8.

We will make use of the following east observation:

Lemma 9.25. *If* χ *is an irreducible character of* G*, then so is* $\overline{\chi}$*.*

Proof. Let $g \mapsto M_g$ be the matrix representation corresponding to χ.

Then $\overline{\chi}$ corresponds to $g \mapsto (M_g^{-1})^t$. Since $\langle \chi, \chi \rangle = \langle \overline{\chi}, \overline{\chi} \rangle = 1$, it follows that $\overline{\chi}$ is an irreducible character. □

And now the proof of the theorem.

Proof. We suppose that $f \in \mathrm{C}\ell(G)$ satisfies $\langle \chi_i, f \rangle = 0$ for $1 \leq i \leq h$. We must show that $f = 0$. Let $\rho : G \to GL(\mathbb{C}G)$ be the regular representation and consider the map $\rho_f = \sum_{g \in G} f(g)\rho_g$.

Notice that $\rho_f(e_1) = \sum_{g \in G} f(g)\rho_g(e_1) = \sum_{g \in G} f(g)e_g$. Hence, it is enough to show that $\rho_f = 0$.

As $\rho = \oplus_\pi \deg \pi_i \pi_i$ summed over the irreducible representations, we know that $\rho_f = \oplus_\pi \deg \pi \sum_{g \in G} f(g)\pi_g = \oplus_\pi \deg \pi \pi_f$ and so it is enough to show that $\pi_f = \sum_{g \in G} f(g)\pi_g = 0$.

To see this, first note that if $t \in G$, then $\pi_t \pi_f \pi_t^{-1} = \sum_g \in G f(g)\pi_t \pi_g \pi_t^{-1} = \sum_{g \in G} f(tft^{-1})\pi_{tgt^{-1}} = \pi_f$. Hence, by Schur's Lemma, it follows that $\pi_f = \lambda I$ for some $\lambda \in \mathbb{C}$. Finally, we note that

$$\deg \pi \lambda = \sum_{g \in G} f(g)\chi_\pi(g) = |G| \langle f, \overline{\chi}_\pi \rangle = 0$$

Thus, $\lambda = 0$. □

And finally, we will now prove Theorem 10.

Proof. Identifying each basis vector $e_g \in \mathbb{C}G$ with the corresponding element $g \in G$, we obtain a natural noncommutative ring structure on $\mathbb{C}G$. Furthermore, each representation $\theta : G \to GL(V)$ extends linearly to a ring homomrophism $\theta : \mathbb{C}G \to \mathrm{End}(V)$. For each conjugacy class C_k opf G, define $\underline{c}_i = \sum_{g \in C_i} g \in \mathbb{C}G$.

Then it is easily checked that $\underline{c}_1, \ldots, \underline{c}_h$ is a basis of $Z(\mathbb{C}G)$ (the center). Here there exist $\ell_k^{ij} \in \mathbb{C}$ such that $\underline{c}_i \underline{c}_j = \sum_{k=1}^h \ell_k^{ij} \underline{c}_k$.

Since $\underline{c}_i \underline{c}_j = \sum a \sum b = \sum ab$ where $a \in C_i, b \in C_j$. We see that each $\ell_k^{ij} \in \mathbb{Z}$.

Now let $\pi : G \to GL(V)$ be an irreducible representation. Then apply π to the definition of multiplication, adn get

$$\pi(\underline{c}_i)\pi(\underline{c}_j) = \sum_{k=1}^h \ell_k^{ij} \pi(\underline{c}_k)$$

By Schur's Lemma, since each $\underline{c}_i$ is in the center of the group ring, it follows that $\pi(\underline{c}_i) = \lambda_i I$ for some $\lambda_i \in \mathbb{C}$. Taking traces, we see that $\deg \pi \lambda_i = \sum_{g \in C_i} \chi_\pi(g) = |C_i| \chi_\pi(g_i)$. Hence, $\lambda_i = \frac{|C_i|}{\deg \pi} \chi_\pi(g_i)$.

Hency, by substituting into the above formula, we obtain

$$\frac{|C_i|}{\deg \pi} \chi_\pi(g_i) \frac{|C_j|}{\deg \pi} \chi_\pi(g_j) = \sum_{k=1}^h \ell_k^{ij} \frac{|C_k|}{\deg \pi} \chi_\pi(g_k)$$

Hence, the ring $R = \mathbb{Z}[\{\frac{|C_i|}{\deg \pi}\chi_\pi(g_i)|1 \leq i \leq h\}]$ is finitely generated as a $\mathbb{Z}$-module, and hence is an integral extension of $\mathbb{Z}$. In particular, each $\frac{|C_i|}{\deg \pi}\chi_\pi(g_i)$ is an algebraic integer. $\square$