Introduction to Galois Theory

Alex Rutar*
University of St Andrews

Winter 2019†

*alex@rutar.org
†Last updated: May 21, 2022

Contents

Preface

This collection of notes is based on the PMath 348 course "Introduction to Galois Theory", taught at the University of Waterloo in Winter 2019 by Blake Madill. These notes are currently in draft form and will likely remain so for a long time. If you find errors (typographical or logical), you can contact me at alex@rutar.org.

I. Structure of Finite Groups

1 Group Quotients

1.1 Universal Property of Quotients

Let $H \trianglelefteq G$ be a normal subgroup of G, and let $\pi : G \to G/H$ be the natural projection map. This map has the following universal property:

1.1 Theorem (Universal Property of Quotients). *Let $\phi : G \to G'$ be a homomorphism. If $H \subset \ker(\phi)$, there is a unique homomorphism $\overline{\phi} : G/H \to G'$ so that $\phi = \overline{\phi} \circ \pi$.*
In particular, $\ker(\overline{\phi}) = \ker(\phi)/H$ and $\operatorname{im}(\overline{\phi}) = \operatorname{im}(\phi)$.

One can rephrase this universal property as follows. Suppose $\phi : G \to G'$ is a homomorphism of groups and $H \trianglelefteq G$ is a normal subgroup. If $H \leq \ker(\phi)$, then ϕ induces a homomorphism $\overline{\phi} : G/H \to G'$ given by $xH \mapsto \phi(x)$ such that $\ker(\overline{\phi}) = \ker(\phi)/H$, $\operatorname{im}(\overline{\phi}) = \operatorname{im}(\phi)$.

Proof. Define $\overline{\phi}(xH) = \phi(x)$. Then $\overline{\phi} \circ \pi(g) = \overline{\phi}(gH) = \phi(g)$, so $\overline{\phi} \circ \pi = \phi$. This map is well-defined: suppose $xH = yH$. Then $y^{-1}x \in H$, so $\phi(y^{-1}x) = 0$ since $H \leq \ker(\phi)$. Thus

$$\overline{\phi}(xH) = \phi(x) = \phi(yy^{-1}x) = \phi(y)\phi(y^{-1}x) = \phi(y) = \overline{\phi}(yH)$$

so $\overline{\phi}$ is well-defined.

To see that $\overline{\phi}$ is unique, let ψ satisfy the universal property as well, so $\psi \circ \pi = \phi$. In particular, $\phi(h) = \psi \circ \pi(g) = \psi(gN)$, so $\psi(gN) = \overline{\phi}(gN)$ so $\overline{\phi}$ is unique.

$\overline{\phi}$ is a homomorphism since ϕ is:

$$\overline{\phi}((aH)(bH)) = \overline{\phi}((ab)H) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(aH)\overline{\phi}(bH)$$

Finally,

$$xH \in \ker(\overline{\phi}) \iff \overline{\phi}(xH) = 0 \iff \phi(x) = 0 \iff x \in \ker(\phi) \qquad \square$$

1.2 Corollary (First Isomorphism). *Suppose $\phi : G \to H$ is a surjective homomorphism. Then $G/\ker(\phi) \cong H$.*

Proof. Take $H = \ker(\phi)$, so $\overline{\phi} : G/\ker(\phi) \to H$ is surjective since $\operatorname{im}(\overline{\phi}) = \operatorname{im}(\phi) = H$ and injective since $\ker(\overline{\phi}) = \ker(\phi)/\ker(\phi) = \{1\}$. $\square$

1.2 Correspondence Theorem

1.3 Theorem. *Let $\phi : G \to G'$ be a homomorphism of groups. ϕ induces two maps on the set of subgroups Γ and Γ' of G and G' respectively:*

$$\phi_* : \Gamma \to \Gamma' \text{ given by } \phi_*(H) = \phi(H)$$
$$\phi^* : \Gamma' \to \Gamma \text{ given by } \phi^*(H') = \phi^{-1}(H')$$

Then $\phi_* \circ \phi^*(H') = H' \cap \operatorname{im}(\phi)$ and $\phi^* \circ \phi_*(H) = \langle H, \ker(\phi) \rangle$.

Recall that $H' \cap \mathrm{im}(\phi)$ is the largest subgroup of H' contained in $\mathrm{im}(\phi)$, and $\langle H, \ker(\phi)\rangle$ is the smallest group containing H and $\ker(\phi)$.

1.4 Corollary. *Let G be a group and $N \trianglelefteq G$. Then the quotient map $\pi : G \to G/N$ is a bijection from the set of subgroups of G containing N to the set of subgroups of G/N.*

Proof. Recall that π is a group homomorphism, and $\ker(\phi) = N$ and $\mathrm{im}(\phi) = G/N$. Then $\pi_* \circ \pi^*(H') = H' \cap \mathrm{im}(\pi) = H'$ and $\pi^* \circ \pi_*(H) = \langle H, \ker(\pi)\rangle = H$ so π is a bijection.□

2 GROUP ACTIONS

Definition. We say that a group G *acts on a set* X if there is a map $G \times X \to X$ satisfying $g(hx) = (gh)x$ and $1x = x$.

Equivalently, an action of G on X is a map $g \mapsto \pi_g$, which assigns to each $g \in G$ a permutation $\pi_G \in S_X$ which respects the operation of G; that is to say, if $g, h \in G$, then $\pi_{gh} = \pi_g \circ \pi_h$. In other words, an action of G on X is a homomorphism $\pi : G \to S_X$.

The action is often written in multiplicative form: we say $\pi_g(a) = b$ and can write $g \cdot a = b$, with $a, b \in X$ and $g \in G$.

Example. The most classic example of a group action is the action of G on itself by conjugation. For each $g \in G$, define the map $\phi_g : G \to G$ given by $\phi_g(x) = gxg^{-1}$. Since ϕ_g is an automorphism, it is certainly a permutation, and for any $g, h \in G$,

$$\phi_{gh}(x) = (gh)x(gh)^{-1} = g(hgh^{-1})g^{-1} = \phi_g \circ \phi_h(x)$$

Definition. Let π be an action of G on X.

1. The *kernel* of the action is the kernel of π as a homomorphism $G \to S_X$; in other words, the set $\{g \in G : g \cdot a = a \text{ for all } a \in X\}$.
2. The action is *faithful* if the kernel is $\{1\}$ (equivalently, if π is injective).
3. Given $a \in X$, the *orbit* of a is the set $G \cdot a = \{g \cdot a : g \in G\}$

If G acts faithfully on X, then G is isomorphic to a subgroup of S_X with isomorphism given by π.

2.1 Proposition. *Let G act on X. The orbits of the action partition X.*

Proof. The orbits clearly cover X since $a \in G \cdot x$ for any $a \in X$. Suppose $G \cdot a$ and $G \cdot b$ are orbits. Either they or disjoint, or $x \in G \cdot a \cap G \cdot b$. Thus get g, h so that $x = g \cdot a = h \cdot b$. But

$$(g^{-1}h) \cdot b = g^{-1} \cdot (h \cdot b) = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = 1 \cdot 1 = a$$

so $a \in G \cdot b$. Thus $G \cdot a \subseteq G \cdot b$; the reverse inclusion follows identically, so $G \cdot a = G \cdot b$.□

Definition. An action of G on X is *transitive* if it has only one orbit, X.

Definition. Let π be an action of G on X. Given $a \in X$, the *stabilizer* of a is the set $G_a = \{g \in G : g \cdot a = a\}$.

2.2 Proposition (Orbit-Stabilizer). *Suppose G acts on X. For every $a \in X$,*

(i) $G_a \leq G$
(ii) $|G \cdot a| = [G : G_a]$

Hence if G is finite, then every orbit has size dividing G.

Proof. 1. It suffices to show that G_a is closed under multiplication and inverses. Let $g, h \in G_a$. Then $(gh) \cdot a = g \cdot (h \cdot a) = g \cdot a = a$, so $gh \in G_a$. Similarly, $g^{-1} \cdot a = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = 1 \cdot a = 1$.

2. Let g, h be arbitrary. Then

$$\begin{aligned} g \cdot a = h \cdot a &\iff h^{-1} \cdot (g \cdot a) = h^{-1} \cdot (h \cdot a) \\ &\iff (h^{-1}g) \cdot a = a \\ &\iff h^{-1}g \in G_a \\ &\iff hG_a = gG_a \end{aligned}$$

so that $g \cdot a$ depends only on gG_a. Thus the number of distinct values of $g \cdot a$ equals the number of left cosets of G_a. □

2.1 CONJUGATION AND THE CLASS EQUATION

Recall the action of G on itself by conjugation: the maps ϕ_g are given by $\phi_g(x) = gxg^{-1}$.

Definition. The *conjugacy class* of an element $a \in A$ is the set $G \cdot a = \{gag^{-1} : g \in G\} := \mathrm{Conj}(a)$.

By general properties of group actions, G is partitioned by its conjugacy classes, and $|\mathrm{Conj}(g)| = [G : G_a]$. In particular, when G is finite, $|\mathrm{Conj}(a)| \div |G|$ for any $g \in G$. Furthermore, the stabilizer G_a satisfies

$$G_a = \{g \in G : g \cdot a = a\} = \{g \in G : gag^{-1} = g\} = \{g \in G : ga = ag\} = C_G(a)$$

which is the centralizer of a in G. We thus have that $|\mathrm{Conj}(g)| = [G : C_G(g)]$.

What happens when $\mathrm{Conj}(g) = \{g\}$? In this case, we say that g is *central* (and otherwise call the conjugacy classes *non-central*). In this special case,

$$\begin{aligned} |\mathrm{Conj}(g)| = 1 &\iff [G : C_G(g)] = 1 \\ &\iff G = C_G(g) \\ &\iff ga = ag \forall a \in G \\ &\iff g \in Z(G) \end{aligned}$$

Thus G is the disjoint union of $Z(G)$ and its non-central conjugacy classes. In particular, if $a_1, \ldots, a_m$ are representatives of the non-central conjugacy classes, we have

$$|G| = |Z(G)| + \sum_{i=1}^{m} |\mathrm{Conj}(a_i)| = |Z(G) + \sum_{i=1}^{m} [G : C_G(a_i)]$$

2.2 CONJUGATION ACTION ON SUBGROUPS

Let G be a group, $P, Q \leq G$ be subgroups. Let $\mathcal{K}$ denote the set of conjugates of P in G.

2.3 *Proposition.* *For any $A \in \mathcal{K}$, $A \leq G$. If $A, B \in \mathcal{K}$, then $|A| = |B|$.*

In other words, $\mathcal{K}$ is composed of subgroups of G conjugate to P, all of which have the same size as P.

Proof. If $a, b \in hPh^{-1}$, then $a = hp_1h^{-1}$, $b = hp_2h^{-1}$ so $ab = h(p_1p_2)h^{-1} \in hPh^{-1}$. Similarly, $a^{-1} = (hp_1h^{-1})^{-1} = hp_1^{-1}h^{-1} \in hPh^{-1}$ as well.

To see that $|A| = |B|$, since A, B are conjugate, get x so $B = xAx^{-1}$. The map $\alpha : A \to B$ given by $a \mapsto xax^{-1}$ is a bijection. It is injective, since if $xa_1x^{-1} = xa_2x^{-1}$ then $a_1 = a_2$; and it is surjective, since if $b \in B$, get $a \in A$ so $xax^{-1} = b$. □

Given this setup, Q acts on $\mathcal{K}$ by conjugation: for $g \in Q$ and $hPh^{-1} \in \mathcal{K}$, we define $g \cdot hPh^{-1} = g(hPh^{-1})g^{-1} = (gh)P(gh)^{-1} \in \mathcal{K}$.

The orbits are equivalence classes of conjugates of P, where $h_1Ph_1^{-1} \sim h_2Ph_2^{-1}$ if they are conjugate by some element of Q.

Recall that $N_G(H) = \{g \in G : gHg^{-1} = H\}$; note that $N_G(H)$ is the largest subgroup of G containg H as a normal subgroup. Then the stabilizers are given by $Q_{P_i} = \{q \in Q : qP_iq^{-1} = P_i\} = N_G(P_i) \cap Q$.

3 STRUCTURE OF FINITELY GENERATED ABELIAN GROUPS

4 SYLOW THEOREMS

Lagrange's theorem, that says that the order of any subgroup of a group G must divide its order. From the previous section, for finite abelian G, if $m \div |G|$ is any factor, then G has a subgroup of order m. This does not necessarily hold for groups which are not abelian.

4.1 Proposition. *There exists a group G and $m \div |G|$ so there is no subgroup of G with order m.*

Proof. Take $G = A_4$, so $|G| = 12$. I claim that H has no group of order 6. For contradiction, suppose $H \leq G$ and $|H| = 6$. Let $a \in G$ such that $|a| = 3$; there are 8 such elements. Consider the cosets H, aH, a^2H. Since $[G : H] = 2$, there are 3 cases:

- $aH = H$, so $a \in H$
- $aH = a^2H$, so $H = aH$ and $a \in H$
- $a^2H = H$ so $H = aH$ and $a \in H$, since $a^3 = 1$.

Thus all 8 elements of order 3 are in H, contradiction. □

While in general these subgroups do not exist, a partial converse is given by the First Sylow Theorem.

4.1 SYLOW *p*-GROUPS

Definition. Let p be a prime. We say that a group G is a *p-group* if $|G| = p^k$, $k \in \mathbb{N}$. If $H \leq G$ is a p-group, we say that H is a *p-subgroup*. If $|H| = p^k||G|$ with k maximal, then we say that G is a *Sylow p-subgroup of G*.

Before we prove the First Sylow Theorem, let's recall Cauchy's Theorem. Some standard proofs resort to the class equation; here, I will present a different alternative approach.

4.2 Theorem (Cauchy). *Let G be a finite group and let $p \div |G|$ be prime. If r is the number of solutions to the equation $x^p = 1$, then $p|r$.*

Proof. Let $|G| = n$, $p|n$ prime, and define

$$S = \{(a_1, a_2, \dots, a_p) : a_i \in G, a_1 a_2 \cdots a_p = 1\}$$

and note that $|S| = n^{p-1}$. Define $\sim$ on S by $a \sim b$ if a and b are cyclic permutations of each other.

If all components of a $p-$tuple are equal, then its equivalence class has 1 member. Otherwise, its equivalence class has p members.

If r denotes the number of solutions to $x^p = 1$, then r is equal to the number of equivalence classes with exactly 1 member. Let s denote the number of equivalence classes with p members; then, $r + ps = n^{p-1}$ and since $p|n$, $p|r$ as well. $\square$

4.3 Corollary. *If $p \div |G|$ is prime, then there exists $H \leq G$ with $|H| = p$.*

Proof. By Cauchy's Theorem, there is at least one non-trivial solution to the equation $x^p = 1$. Let g be such an element; then $H = \langle g \rangle \leq G$ has order p. $\square$

In a sense, Cauchy's Theorem provides a partial converse to Lagrange's Theorem. However, the First Sylow Theorem is a strengthening of this claim. In particular, Cauchy's Theorem follows as an easy corollary.

4.4 Theorem (First Sylow). *Let G be a finite group and let p be a prime dividing its order. Then G contains a Sylow $p-$subgroup.*

Proof. The proof follows by induction on $|G|$. If $|G| = 2$, then G is its own Sylow 2-subgroup. If $|G| \geq 2$ is finite, let $p \div |G|$, and say $|G| = p^n m$ where $p \not\div m$.

Case 1: $p \div |Z(G)|$. By Cauchy, there exists $a \in Z(G)$ so that $o(a) = p$. Since $\langle a \rangle \subseteq Z(G)$, $\langle a \rangle \trianglelefteq G$. If $n = 1$, we are done; otherwise, by induction, $G/\langle a \rangle$ has a Sylow $p-$subgroup $\overline{H}$. By correspondence, $\overline{H} = H/\langle a \rangle$ for some $H \leq G$. Thus, $p^{n-1} = |H|/p$, so $|H| = p^n$ and H is a Sylow $p-$subgroup of G.

Case 2: $p \not\div |Z(G)|$. By the Class equation, there is some a_i so that $p \nmid [G : C_G(a_i)] = |G|/|C_G(a_i)|$. Thus $p^n \div |C_G(a_i)|$ where a_i is non-central. Since $a_i \notin Z(G)$, $|C_G(a_i)| < |G|$. By induction, $C_G(a_i)$ has a Sylow $p-$subgroup, which is also a Sylow $p-$subgroup of G. $\square$

4.2 STRUCTURE OF SYLOW p-SUBGROUPS

Let G be a group and suppose $H \leq G$.

4.5 Lemma. *Suppose $p \div |G|$, P is a Sylow $p-$subgroup of G, and Q is a $p-$subgroup of G. Then $Q \cap N_G(P) = Q \cap P$.*

Proof. Since $P \subseteq N_G(P)$, $P \cap Q \subseteq N_G(P) \cap Q$. For notation, set $N = N_G(P)$ and $H = N_G(P) \cap Q$. It remains to show $H \subseteq P \cap Q$.

Write $|P| = p^n$ and $|H| = p^m$. Since $P \trianglelefteq N$, $HP \leq N$. Thus

$$|HP| = \frac{|H| \cdot |P|}{|H \cap P|} = p^k, k \leq n$$

As well, $P \subseteq HP$ so $n \leq k$, and $P = HP$. Thus $H \subseteq HP = P$. $\square$

4.6 Lemma. *Let G, p, P, Q be as in the previous lemma, and let $\mathcal{K}$ denote the set of conjugates of P in G. Let Q act on $\mathcal{K}$ by conjugation, so the orbits have representatives $P = P_1, P_2, \ldots, P_r$. Then, $|\mathcal{K}| = \sum_{i=1}^{r}[Q : Q \cap P_i]$.*

Proof. By the Orbit-Stabilizer lemma,

$$\begin{aligned} |\mathcal{K}| = \sum_{i=1}^{r} |Q \cdot P_i| &= \sum_{i=1}^{r} [Q : Q_{P_i}] \\ &= \sum_{i=1}^{r} [Q : N_G(P_i) \cap Q] \\ &= \sum_{i=1}^{r} [Q : P_i \cap Q] \end{aligned}$$

where the last line follows from the previous lemma. □

4.7 Theorem (Second Sylow). *If P and Q are Sylow $p-$subgroups of G, then there exists $g \in G$ so that $P = gQg^{-1}$.*

Since the conjugation action preserves the order of groups, the Sylow $p-$subgroups of G are precisely the equivalence class of any Sylow $p-$subgroup of G.

Proof. Let $\mathcal{K}$ be the set of conjugates of P in G, and let P act on $\mathcal{K}$ by conjugation. Recall that for $P_i, P_j \in \mathcal{K}$, $|P_i| = |P_j|$.

Let $P = P_1, P_2, \ldots, P_r$ be orbit represntatives. Then by the Lemma above,

$$|\mathcal{K}| = \sum_{i=1}^{r} [P : P \cap P_i] = 1 + \sum_{i=2}^{r} [P : P_i \cap P] \equiv 1 \pmod{p}$$

since $p \div [P : P_i \cap P]$: this follows since $P_i \cap P \lneq P$ and $|P| = p^n$.

Now let Q act on K by conjugation. Reindexing if necessary, let the orbits have representatives $P = P_1, P_2, \ldots, P_s$. If $Q \neq P_i$ for $i = 1, 2, \ldots, s$, then by the same argument as above, $|\mathcal{K}| = \sum_{i=1}^{s}[Q : P_i \cap Q] \equiv 0 \pmod{p}$, a contradiction. Thus $Q = P_i$ and so Q is a conjugate of P. □

Now Sylow's third theorem follows easily:

4.8 Theorem (Third Sylow). *Let $p \div |G|$ be prime, $|G| = p^n m$ with $\gcd(p, m) = 1$, and n_p denote the number of Sylow $p-$subgroups of G. Then if P is any Sylow $p-$subgroup of G,*

1. $n_p \equiv 1 \pmod{p}$
2. $n_p = [G : N_G(P)]$

In particular, $n_p | m$, and $n_p = 1$ if and only if $N_G(P) = G$; in other words, that P is a normal subgroup of G.

Proof. Let P be a Sylow $p-$subgroup of G and let $\mathcal{K}$ be the set of conjugates of P in G. From the proof of Sylow's second theorem, $n_p = |\mathcal{K}| \equiv 1 \pmod{p}$.

Now let G act on K by conjugation so $\mathcal{K} = G \cdot P$. By the Orbit-Stabilizer theorem, $|G| = |G_P| \cdot |G \cdot P|$. Since $G_P = N_G(P) \cap G = N_G(P)$, $p^n m = |N_G(P)| \cdot n_p$. Thus $n_p | p^n m$, and since $n_p \not\equiv 0 \pmod{p}$, $n_p | m$. □

Remark. $\operatorname{disc} f(x)$ is not a square in F if and only if $\operatorname{Gal} f(x) \not\subseteq A_2$ iff $\operatorname{Gal} f(x) = S_2$ iff $f(x)$ is irreducible.

Example. Prove that there is no simple group of order 56.

Note that $56 = 2^3 \cdot 7$. Since $n_7 \equiv 1 \pmod 7$ and $n_7 | 8$, we have $n_7 \in \{1, 8\}$. If $n_7 = 1$, then G has a normal Sylow $7-$subgroup. By Lagrange, distinct Sylow 7-subgroups intersect trivially. Thus there are $8 \cdot 6 = 48$ elements of order 7 in G. This forces $n_2 = 1$. In either case, G is not simple.

Remark. If $p \neq q$ are prime, $p, q \div |G|$. Then if H_p, H_q are $p-$ and $q-$subgroups, then $H_p \cap H_q = \{1\}$. Similarly, if $|G| = pm$ and H, K are Sylow $p-$subgroups, then $H = K$ or $H \cap K = \{1\}$.

Example. If $|G| = pq$, where p, q prime, $p < q$, $p \not\div q - 1$. Then G is cyclic.

Since $n_p \equiv 1 \pmod p$ and $n_p \div |q$. We cannot have $n_p = q$, so G has a normal Sylow $p-$subgroup H_p. Since $p < q$, $q \not\div p - 1$, so $n_q = 1$ and G has a normal Sylow $q-$subgroup H_q, say H_q. Since $H_p \cap H_q = \{1\}$, $G \cong H_p \times H_q \cong \mathbb{Z}_{pq}$ since p, q are coprime.

Example. If $|G| = 30$, then G has a subgroup isomorphic to $\mathbb{Z}_{15}$. Since $n_5 \equiv 1 \pmod 5$ and $n_5 | 6$, $n_5 \in \{1, 6\}$. Similarly, $n_3 \equiv 1 \pmod 3$, and $n_3 | 10$, so $n_3 \in \{1, 10\}$. By counting elements, at least one must be normal. Let H_3, H_5 be Sylow subgroups. Since $3 \not\div 5 - 1$, $Z_{15} \cong H_3 H_5 \leq G$ by the previous example.

Example. If $|G| = 60$, $n_5 > 1$, then G is simple. Since $|G| = 60$, $n_5 \equiv 1 \pmod 5$ and $n_5 | 12$, we must have $n_5 = 6$ (accounting for 25 elements). Suppose $N \trianglelefteq G$.

Case 1: $5 \div |H|$. Then H contains a Sylow $5-$subgroup of G. Since H is normal, H contains all conjugate other Sylow 5-subgroups, so $|H| \geq 25$ and $|H| = 30$. By the previous example, $n_5 = 1$ since $\mathbb{Z}_{15}$ has only 1 Sylow 5-subgroup.

Case 2: $|H| \in \{2, 3, 4, 6, 12\}$. If $|H| = 12$, H has a normal Sylow 2- or 3-subgroup, which is normal in G. Call it K. If $|H| = 6$, then H has a normal Sylow 3-subgroup which is normal in G. Call it K. By replacing H with K if necessary, we may assume $|H| \in \{2, 3, 4\}$. Consider $\overline{G} = G/H$. Then $|\overline{G}| = \{15, 20, 30\}$. In any case, $\overline{G}$ has a normal Sylow 5-subgroup; call it $\overline{P}$. By correspondence, $\overline{P} = P/H$. P is a normal subgroup of G, so P is a proper, non-trivial normal subgroup of G. As well, $|P| = |\overline{P}| \cdot |H| = 5$, so $5 \div |H|$ and $5 \div |P|$. This contradicts Case 1.

Example. A_5 is simple since $|A_5| = 60$ and $\langle (12345) \rangle$, $\langle (13245) \rangle$ are distinct Sylow 5-subgroups.

II. Fields

5 Irreducible Polynomials

Definition. Let R be an integral domain. We say $f(x) \in R[x]$ is *irreducible* over R if f is a non-unit, non-irreducible, and whenever $f(x) = g(x)h(x)$, then either g is a unit or h is a unit. Otherwise, f is *reducible*.

Remark. A canonical way to construct new fields as follows. Suppose F be a field and I an ideal of $F[x]$. Since $F[x]$ is a PID ($F[x]$ has a division algorithm), then $I = \langle p(x) \rangle$, $p(x) \in F[x]$. Moreover, I is maximal if and only if $p(x)$ is irreducible. Thus $F[x]/I$ is a field if and only if $p(x)$ is irreducible.

> ***5.1 Proposition.*** *Let F be a field. If $f(x) \in F[x]$, $\deg f(x) > 1$ and $f(x)$ has a root in F, then $f(x)$ is reducible over F. In particular, if $\deg f(x) \in \{2, 3\}$, then $f(x)$ is irreducible over F if and only if f has no roots in F.*

Proof. By the division algorithm, $f(x) = (x-a)q(x) + r(x)$ where $\deg r(x) \leq 1$. Then $f(x) = 0 + r = r$, so $f(x) = (x-a)q(x) + f(a)$, so $(x-a) \div f(x)$ if and only if $f(a) = 0$. From this, the first claim follows immediately.

For the second claim, if $g(x) | f(x)$, then either $\deg g = \deg f$, $\deg g = 2$, or $\deg g = 1$. If every divisor has the same degree as f, then f is irreducible; otherwise, f has a factor of degree 1 and the claim follows by the initial observation. □

> ***5.2 Lemma (Gauss' Lemma).*** *Let R be a UFD with field of fractions F. Let $p(x) \in R[x]$. If $p(x) = A(x)B(x)$ with $A(x), B(x)$ non-constant in $F[x]$, then there exists $r \in F^\times$ such that $a(x) = rA(x), b(x) = r^{-1}B(x) \in R[x]$.*

Proof. PMATH 347. □

Remark. Gauss' Lemma states that if $p(x) \in R[x]$ is reducible over F, then $p(x)$ is reducible over R. In particular, if $p(x)$ is irreducible over $\mathbb{Z}$, then $p(x)$ is irreducible over $\mathbb{Q}$ as well.

Let R be an integral domain and I a proper ideal. If $p(x) \in R[x]$ with coefficients a_i, then $\overline{p}(x) \in (R/I)[x]$ with coefficients $a_i + I$. The map $p(x) \mapsto \overline{p}(x)$ is a ring homomorphism.

> ***5.3 Proposition.*** *Let I be a proper ideal of an integral domain R, and $p(x) \in R[x]$ non-constant and monic. If $\overline{p}(x)$ cannot be factored in $(R/I)[x]$ into polynomials of lesser degree, then $p(x)$ is irreducible in $\mathrm{Frac}(R)[x]$.*

Proof. Suppose $p(x)$ is reducible over $\mathrm{Frac}(R)$. By Gauss' Lemma, there is a non-trivial factorization $p(x) = f(x)g(x)$ over $R[x]$ with $\deg f, \deg g < \deg p$. Without loss of generality, $f(x)$ and $g(x)$ are also monic. Thus, in $(R/I)[x]$, $\overline{p}(x) = \overline{f}(x) = \overline{g}(x)$. Since $I \subsetneq R$, $1 \notin I$, so $\deg \overline{f} = \deg f$, $\deg \overline{g} = \deg g$, $\deg \overline{p} = \deg p$ and $\overline{f} = \overline{g}\overline{h}$ is a non-trivial factorization. □

5.4 Corollary. *Let $f(x) \in \mathbb{Z}[x]$, $\deg f(x) \geq 1$. Let $p \in \mathbb{Z}$ be a prime. If $\overline{f}(x) \in \mathbb{Z}_p[x]$ such that $\deg f(x) = \deg \overline{f}(x)$ and $\overline{f}(x)$ is irreducible over $\mathbb{Z}_p$, then $f(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Take $R = \mathbb{Z}$, $I = (p)$ in the previous lemma. □

5.5 Proposition (Eisenstein's Criterion). *Let R be an integral domain and P a prime ideal of R. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. If $a_i \in P$ and $a_0 \notin P^2$, then $f(x)$ is irreducible over R.*

Proof. Suppose $f(x)$ is reducible over R. Since $f(x)$ is monic, $f(x) = g(x)h(x)$, where $g(x), h(x) \in R[x]$ with $\deg g(x), \deg h(x) < \deg f(x)$. Therefore,

$$\begin{aligned}\overline{f}(x) &= \overline{g}(x)\overline{h}(x) \\ &= x^n \in (R/P)[x]\end{aligned}$$

Since P is prime, R/P is an integral domain. Thus $\overline{g}(0) = \overline{h}(0) = 0$ and $g(0), h(0) \in P$, so $a_0 = g(0)h(0) \in P^2$. □

Example.

1. $f(x,y) = x^2 + y^2 - 1 \in \mathbb{Q}[x,y]$ is irreducible. Let $g(y) = y^2 + (x^2 - 1)$, and take $P = \langle x+1 \rangle$. Since $x+1$ is irreducible, P is a prime ideal of $\mathbb{Q}[x]$. Moreover, $x^2 - 1 \in P$ but $(x+1)^2 \notin P^2$, so by Eisenstein, $f(x,y)$ is irreducible.
2. Suppose $f(x) = x^n - d$, where d is not a perfect square. Then f is irreducible over $\mathbb{Q}$ by Eisenstein.
3. $f(x) = x^3 + 2x + 16$. Consider modulo 3, $\overline{f}(x) = x^3 + 2x + 1$, which is irreducible by checking $0, 1, 2$ as roots.
4. $f(x) = x^4 + 5x^3 + 6x^2 - 1$. Then $\overline{f} = x^4 + x^3 + 1 \in \mathbb{Z}_2[x]$ is irreducible by checking roots and the unique irreducible quadriatic $x^2 + x + 1$.
5. Let p be a prime, and $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = (x^p - 1)/(x-1)$, so
$$f(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{p-1}x^{p-2} + \cdots + \binom{p}{2}x + \binom{p}{1}$$
Since $f(x)$ is irreducible if and only if $f(x+a)$ is irreducible, $f(x)$ is irreducible by Eisenstein.

6 FIELD EXTENSIONS

6.1 Proposition. *The polynomial ring $F[x]$ has a division algorithm (i.e. it is a Euclidean domain). Thus $F[x]$ is a PID.*

Proof. PMATH 347. □

Definition. Let K be a field. $F \subseteq K$ is a *subfield* of K if F is a field under the same operations. A *field extension* of F is a field K which contains an isomorphic copy of F as a subfield. In this case, we write K/F. We say $F_1/F_2/\cdots/F_n$ is a *tower of fields* if each F_i/F_{i+1} is a field extension.

Remark. Suppose $f(x) \in F[x]$ is irreducible. Then $K = F[x]/\langle f(x)\rangle$ contains F in the following natural way: define $\phi : F \to K$ by $\phi(x) = x + \langle f(x)\rangle$. It follows that ϕ is injective: if $\phi(x) = \phi(y)$, then $x - y \in \langle f(x)\rangle$. Since $x - y \in F$ but $\langle f(x)\rangle \neq F[x]$, we must have $x - y = 0$ so $x = y$.

If $\mathrm{char}(F) = p > 0$, then there is a natural injection $\mathbb{Z}_p \to F$: consider the map $\phi : \mathbb{Z} \to F$ given by $n \mapsto n \cdot 1_F$; apply the first isomorphism theorem.

Definition. Let $\alpha_1, \dots, \alpha_n \in K$. The *field extension of F generated by* $\alpha_1, \dots, \alpha_n$ is

$$F(\alpha_1, \dots, \alpha_n) = \left\{ \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} : f, g \in F[x_1, \dots, x_n], g(\alpha_1, \dots, \alpha_n) \neq 0 \right\}$$

Remark. Note that $K/F(\alpha_1, \dots, \alpha_n)/F$.

6.2 Proposition. *Suppose K/F, $\alpha \in K$. If α is a root of some non-zero $f(x) \in F[x]$, which is irreducible over F, then $F(\alpha) \cong F[x]/\langle f(x)\rangle$. Moreover, if $\deg f(x) = n$, then $F(\alpha) = \mathrm{span}_F\{1, \alpha, \dots, \alpha^{n-1}\}$.*

Proof. Let $\alpha \in K$ be a root of $f(x) \in F[x]$ with $\deg f(x) = n$. Consider the map

$$\phi : F[x] \to F(\alpha), \qquad \phi(g(x)) = g(\alpha)$$

One can verify that this is a ring homomorphism. Set $I = \ker(\phi)$: since $F[x]$ is a PID, $I = \langle g(x)\rangle$; since $f(x) \in I$, $f(x) = g(x)h(x)$ for some $h(x) \in F[x]$. Since I is a proper ideal, g is not a unit, so by irreducibility of f, h is a unit and $\langle g(x)\rangle = \langle f(x)\rangle$. Thus by the first isomorphism theorem, $F[x]/\langle f(x)\rangle \cong \phi(F[x])$ via $h(x) + \langle f(x)\rangle \mapsto h(\alpha)$.

By definition, $\phi(F[x]) \subseteq F(\alpha)$. Since $\phi(F[x])$ is a field (up to isomorphism) which contains $\alpha = \phi(x)$ and F, $F(\alpha) \subseteq \phi(F[x])$, so equality holds.

Finally, by the division algorithm,

$$F[x]/\langle f(x)\rangle = \left\{c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_0 + \langle f(x)\rangle, c_i \in F\right\}$$

Thus $F(\alpha) = \{c_{n-1}\alpha^{n-1} + \cdots + c_a\alpha + c_0 : c_i \in F\} = \mathrm{span}_F\{1, \alpha, \dots, \alpha^{n-1}\}$. $\square$

Remark. Suppose $g \in F[x]$ such that $g(\alpha) = 0$. Since $F[x]$ is an integral domain, g must have an irreducible factor f with $f(\alpha) = 0$. In particular,

1. If $h(x) \in F[x]$, $h(\alpha) = 0$ then $h(x) \in \langle f(x)\rangle$ and $f(x) \div h(x)$.
2. $\langle f(x)\rangle$ contains a unique, monic, irreducible polynomial. If $g(x) \in \langle f(x)\rangle$ is irreducible, then $g(x) = uf(x)$.

Definition. Let K/F be an extension and $\alpha \in K$ a root of a nonzero polynomial in $F[x]$. Then, there exists a unique monic irreducible $f(x) \in F[x]$ such that $f(\alpha) = 0$. We call $f(x)$ the *minimal polynomial* of α over F. If $\deg f(x) = n$, then n is the *degree of α over F*.

6.3 Proposition. *Let K/F be an extension and $\alpha \in K$ with minimal polynomial $f(x) \in F[x]$, with $\deg_F(\alpha) = n$. Then $\{1, \alpha, \dots, \alpha^{n-1}\}$ is a basis for K/F.*

Proof. That it spans follows from the previous proposition (Proposition 6.2). If the set is linearly dependent, then the coefficients in the dependence relation would give a polynomial g with $g(\alpha) = 0$ and $\deg g \leq n - 1$, a contradiction. $\square$

6.4 Corollary. *Let $\alpha, \beta \in K$ have the same minimal polynomial $f(x) \in F[x]$. Then $F(\alpha) \cong F(\beta)$.*

Proof. This is immediate since $F(\alpha) \cong F[x]/\langle f(x)\rangle \cong F(\beta)$. $\square$

6.1 FINITE EXTENSIONS

Definition. We say that K/F is a *finite extension* if K is a finite dimensional $F-$vector space. We call $\dim_F K$ the *degree* of K/F and denote this dimension by $[K : F]$.

6.5 Theorem. *If K/E and E/F are extensions, then $[K : F] = [K : E][E : F]$.*

Proof. Let $\{v_1, \ldots, v_n\}$ be a basis for K/E and $\{w_1, \ldots, w_m\}$ a basis for E/F. Let's show $\{w_i v_j : i \in [n], j \in [m]\}$ is a basis for K/F. Suppose $\sum_{i,j} c_{ij} v_i w_j = 0$. Then $\sum_i \left(\sum_j c_{ij} w_j\right) v_i = 0$; since the v_i are linearly independent, for each i, $\sum_j c_{ij} w_j = 0$ is linearly independent. It is clear that this sets spans, so it is indeed a basis. $\square$

Definition. Let K/F be an extension. We say $\alpha \in K$ is *algebraic over F* if it is the root of a non-zero polynomial. Otherwise, we say α is *transcendental over F*. We say K/F is algebraic if every $\alpha \in K$ is algebraic over F. Otherwise, we say K/F is transcendental.

Remark. If $\alpha \in K$ is algebraic over F, then α has a minimal polynomial in $F[x]$.

6.6 Theorem. *If K/F is finite, then K/F is algebraic.*

Proof. Suppose $[K : F] = n < \infty$, and let $\alpha \in K$. Consider $\alpha, \alpha^2, \ldots, \alpha^{n+1}$. If $\alpha^i = \alpha^j$ for some $i \neq j$ then α is a root of $f(x) = x^j - x^i$. Otherwise, since $\{\alpha, \alpha^2, \ldots, \alpha^{n+1}\}$ is linearly dependent over F, there is some dependence relation and α is a root of $f(x) = c_{n+1}x^{n+1} + \cdots + c_1 x \neq 0$. $\square$

Definition. We say that K is a *finitely generated* extension of F if there exists $\alpha_1, \ldots, \alpha_n \in K$ such that $K = F(\alpha_1, \ldots, \alpha_n)$.

6.7 Proposition. *If K is a finitely generated and algebraic extension of F, then K/F is finite.*

Proof. Suppose K/F is algebraic, where $K = F(\alpha_1, \ldots, \alpha_n)$, $\alpha_i \in K$. If $n = 1$, then $[F(\alpha_1) : F] = \deg_F(\alpha_1) < \infty$.

Assume the result for n and consider $K = F(\alpha_1, \ldots, \alpha_n, \alpha_{n+1})$. Then

$$[F(\alpha_1, \ldots, \alpha_n, \alpha_{n+1})] = [F(\alpha_1, \ldots, \alpha_n)(\alpha_{n+1}) : F(\alpha_1, \ldots, \alpha_n)] \cdot [F(\alpha_1, \ldots, \alpha_n) : F] < \infty$$

by the tower theorem. $\square$

6.8 Proposition. *If K/E and E/F are both algebraic, then K/F is algebraic.*

Proof. Let $\alpha \in K$. Since K/E is algebraic, α has a minimal polynomial in E:

$$p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in E[x]$$

Thus α is algebraic over $F(c_0, c_1, \ldots, c_{n-1})$. Note that

$$[F(c_{n-1}, \ldots, c_1, c_0)(\alpha) : F(c_{n-1}, \ldots, c_1, c_0)] < \infty.$$

Since $F(c_{n-1}, \ldots, c_1, c_0) \subseteq E$, $F(c_{n-1}, \ldots, c_1, c_0)/F$ is algebraic and finitely generated, so $[F(c_{n-1}, \ldots, c_1, c_0) : F] < \infty$. By the tower theorem, $[F(c_{n-1}, \ldots, c_1, c_0, \alpha) : F] < \infty$, so α is algebraic over F. $\square$

6.9 Proposition. *Let K/F be a extension. The set of elements of K which are algebraic over F form a subfield of K.*

Proof. Let L denote the elements algebraic over F. If $\alpha, \beta \in L$, then α, β, $\alpha - \beta$, $\alpha\beta$, and β^{-1} are all elements of $F(\alpha, \beta)$. Since $[F(\alpha, \beta) : F] < \infty$ and since finite implies algebraic, these elements are all algebraic. $\square$

6.2 SPLITTING FIELDS

Definition. Let $f(x) \in F[x]$ be non-constant. We say $f(x)$ *splits* in an extension K of F if it factors completely into linear factors over K.

6.10 Theorem (Kronecker). *Let $f(x) \in F[x]$ be non-constant. Then there exists an extension K of F such that $f(x)$ has a root in K.*

Proof. Let $f(x) \in F[x]$ be non-constant; since $F[x]$ is a UFD, let $p|f$ where p is irreducible. Let $K = F[t]/(p(t))$, so $t + (p(t))$ is a root of $p(x)$, which is also a root of $f(x)$. $\square$

6.11 Corollary. *Let $f(x) \in F[x]$ be non-constant. There exists an extension K of F such that $f(x)$ splits over K.*

Proof. Repeated application of Kronecker. $\square$

Definition. Let $f(x) \in F[x]$ be non-constant. A minimal extension K of F with the property that f splits over K is called a *splitting field* for f.

If $f(x) \in F[x]$, there is an extension K/F such that $f(x)$ splits over K. But then a splitting field for $f(x)$ over F is $F(\alpha_1, \ldots, \alpha_n)$ where the α_i are the roots of f.

Example. Find a splitting field for $f(x) = x^4 + x^2 - 6$ over $\mathbb{Q}$. Over $\mathbb{C}$, $f(x) = (x + \sqrt{3}i)(x - \sqrt{3}i)(x - \sqrt{2})(x + \sqrt{2})$. Thus a splitting field for $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3}i)$.

6.12 Lemma. *Let F, F' be fields. If $\phi : F \to F'$ is an isomorphism, then the natural map $\tilde{\phi} : F[x] \to F'[x]$ is an isomorphism.*

Proof. It's long but easy. $\square$

We'll just write $\tilde{\varphi} \equiv \varphi$.

6.13 Lemma (Isomorphism Extension). *Let F, F' be fields, $\phi : F \to F'$ be an isomorphism. Let $f(x) \in F[x]$ be irreducible, α a root of $f(x)$ in an extension of F. β is a root of $\phi(f(x))$ in some extension of F'. Then there exists an isomorphism $\psi : F(\alpha) \to F'(\beta)$ such that $\psi|_F = \phi$ and $\psi(\alpha) = \beta$.*

Proof. The following diagram commutes:

$$\begin{tikzcd}
F(\alpha) \arrow[rrr, dashed, "\psi"] \arrow[dd, "\rho_1"', "\wr"] & & & F'(\beta) \\
& F \arrow[ul, hook] \arrow[r, "\phi"] & F' \arrow[ur, hook] & \\
F[x]/\langle f(x)\rangle \arrow[rrr, "\sim", "\sigma:\overline{g(x)}\mapsto\overline{\phi(g(x))}"'] & & & F'[x]/\langle \phi(f(x))\rangle \arrow[uu, "\rho_2"', "\wr"]
\end{tikzcd}$$

where ψ exists by composing maps. If $a \in F$, then

$$\psi(a) = \rho_2 \circ \sigma \circ \rho_1(a) = \rho_2 \circ \sigma(\overline{a}) = \rho_2(\overline{\phi(a)}) = \phi(a) = a$$

As well, we verify that

$$\psi(\alpha) = \rho_2 \circ \sigma \circ \rho_1(\alpha) = \rho_2 \circ \sigma(\overline{x}) = \rho_2(\overline{\phi(x)}) = \rho_2(\overline{x}) = \beta \qquad \square$$

6.14 Corollary. *Let F be a field, $f(x) \in F[x]$ non-constant. Let K be a splitting field for $f(x)$ over F. If F' is a field and $\phi : F \to F'$ is an isomorphism, then for any K' splitting field for $\phi(f(x))$ over F', there is an isomorphism $\psi : K \to K'$ such that $\psi|_F = \phi$.*

Proof. Repeatedly apply the isomorphism extension lemma (Lemma 6.13) to the roots of f. $\square$

6.15 Corollary. *Let $f(x) \in F[x]$ be non-constant. If K and K' are splitting fields for $f(x)$ over F, then $K \cong K'$.*

Proof. Take $\phi = \mathrm{id}$ in the previous corollary. $\square$

6.3 ALGEBRAIC CLOSURE

Definition. A field $\overline{F}$ is an *algebraic closure* of a field F if

- $\overline{F}/F$ is algebraic
- Every non-constant polynomial in $F[x]$ splits over $\overline{F}$.

A field F is **algebraically closed** if every non-constant polynomial $f(x) \in F[x]$ has a root in F.

Example. $\mathbb{C}$ is an algebraic closure for $\mathbb{R}$, but not for $\mathbb{Q}$.

6.16 Proposition. *If $\overline{F}$ is an algebraic closure for F, then $\overline{F}$ is algebraically closed.*

Proof. Let $\overline{F}$ be an algebraic closer for F. Let $f(x) \in \overline{F}(x)$ be non-constant; by Kronecker, $f(x)$ has a root α in some extension of $\overline{F}$. Since $\overline{F}(\alpha)/\overline{F}$ is algebraic and $\overline{F}/F$ is algebraic, $\overline{F}(\alpha)/F$ is algebraic. Thus α is the root of some non-zero polynomial $p(x) \in F[x]$. Now, $p(x)$ splits over $\overline{F}$ so $\alpha \in \overline{F}$ and $\overline{F}$ is algebraically closed. $\square$

6.17 Theorem. *For every field F, there exists an algebraically closed field containing F.*

Proof. Exercise. $\square$

6.18 Theorem. *Let K be an algebraically closed field which contains F. The collection of elements in K which are algebraic over F is an algebraic closure.*

Proof. Let $L = \{\alpha \in K : \alpha \text{ is algebraic over} F\}$. We claim that L is an algebraic closure for F. By construction, L/F is algebraic. Let $f(x) \in F[x]$, $\deg f(x) \geq 1$. Since $f(x)$ splits over K, $f(x) = u(x - \alpha_1) \cdots (x - \alpha_n)$. Since $u \in F$, $\alpha_i \in K$. But, $f(\alpha_i) = 0$ for $i = 1, \ldots, n$ and so $\alpha_i \in L$ and $f(x)$ splits over L. $\square$

7 EXAMPLES OF FIELD EXTENSIONS

7.1 CYCLOTOMIC EXTENSIONS

What is the splitting field of $f(x) = x^n - 1$?

Definition. We call the roots of $x^n - 1$ (in $\mathbb{C}$) the n^{th} *roots of unity.*

If $\zeta_n = e^{2\pi i/n}$, they are $1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}$. Thus, the splitting field over $\mathbb{Q}$ is $\mathbb{Q}(\zeta_n)$. What is $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$? When $n = p$ is prime, $x^p - 1 = (x-1)(1 + x + x^2 + \cdots + x^{p-1})$. Since $\Phi_p(x) = x^{p-1} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$ (from before), so $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

Example. Since $\zeta_5 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$, $\mathbb{Q}(\zeta_6) = \mathbb{Q}(i\sqrt{3})$ so $\deg(x^2+3) = 2$.

Note that the n^{th} roots of unity form a finite cyclic subgroup of $\mathbb{C}$; in fact, they are the only finite cyclic subgroups of $\mathbb{C}$. A generator of this group is called a *primitive n^{th} root of unity*, which happens precisely for ζ_n^k where $\gcd(k, n) = 1$. Thus there are $\phi(n)$ primitive n^{th} roots of unity.

Definition. The n^{th} *cyclotomic polynomial* is

$$\Phi_n(x) = \prod_{k \in (\mathbb{Z}_n)^\times} (x - \zeta_n^k)$$

7.1 Theorem. *$\Phi_n(x)$ is the minimal polynmial for ζ_n, and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.*

Proof. Note that ζ_n is a root of $x^n - 1$, so ζ_n is algebraic over $\mathbb{Q}$. By Gauss' lemma, let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of ζ_n over $\mathbb{Q}$ so that $f(x) \div (x^n - 1)$ over $\mathbb{Z}[x]$. Recall that

$$x^n - 1 = \prod_{j \in \mathbb{Z}_n} (x - \zeta_n^j)$$

If $j \notin (\mathbb{Z}_n)^\times$, then ζ_n^j satisfies $x^{\frac{n}{\gcd(n,j)}} - 1$ but ζ_n does not, so ζ and ζ_n^j are not conjugates. Thus the only possible conjugates for ζ_n are the ζ_n^j where $j \in (\mathbb{Z}_n)^\times$; it suffices to show that these are precisely the conjugates. In particular, let's show that if $\theta = \zeta_n^t$ and p is prime with $p \nmid n$, then θ^p is conjugate to θ. With this, the result follows: if j is coprime to n, write $j = p_1^{e_1} \cdots p_m^{e_m}$ with $p_i \nmid n$ and repeatedly apply the above result to ζ_n for each p_i, e_i times.

Thus let's prove the claim. Write $x^n - 1 = f(x)g(x)$ with $f, g \in \mathbb{Z}[x]$; since θ^p is a root of $x^n - 1$, either it is a root of $f(x)$ - in which case we're done - or it is a root of $g(x)$. Suppose $g(\theta^p) = 0$, so θ is a root of $g(x^p) \in \mathbb{Z}[x]$ so $f(x) \div g(x^p)$ over $\mathbb{Z}[x]$. Modulo p, $\overline{f}(x) \div \overline{g}(x^p) = \overline{g}(x)^p$ in $\mathbb{Z}_p[x]$. Since $\mathbb{Z}_p[x]$ is a UFD, let $s(x)$ be an irreducible factor of $f(x)$ so that $s|\overline{f}$ and thus $s|\overline{g}$. But then $x^n - \overline{1} = \overline{f}\overline{g}$, so $s^2 \div (x^n - 1)$ and $s \div \overline{n}x^{n-1}$. Since n is coprime to p, this implies $s = cx$ for some $c \in \mathbb{Z}_p$. But then $cx \div x^n - \overline{1}$, a contradiction.□

7.2 FINITE FIELDS

Definition. Let F be a field of characteristic p. Then the map $\phi : F \to F$ given by $x \mapsto x^p$ is called the *Frobenius map.*

7.2 Proposition. *The Frobenius map is an injective ring homomorphism.*

Proof. We have that $\phi(xy) = x^p y^p = (xy)^p$, and

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

since $p \div \binom{p}{i}$ for all $1 \leq i \leq p-1$. Injectivity is immediate since $\phi(1) = 1$ and the only ideals of F are $\{0\}$ and $\{F\}$, forcing $\ker(\phi) = \{0\}$. $\square$

7.3 Corollary. *If F is a finite field, the Frobenius map is an automorphism.*

7.4 Proposition. *Suppose F is finite. Then*

1. *$F^\times = \langle \alpha \rangle$ is a cyclic group.*
2. *$|F| = p^n$.*
3. *$|F| = p^n$ if and only if F is the splitting field for $x^{p^n} - x$ over $\mathbb{Z}_p$.*
4. *Finite fields of a fixed size are unique up to isomorphism.*

Proof.

1. Write $F^\times \cong C_{n_1} \times \cdots \times C_{n_k}$ where $n_1 | n_2 | \cdots | n_k$. Then each C_{n_i} has a subgroup $D_i \cong C_{n_k}$; but then every $x \in D_1 \times \cdots \times D_k$ satisfies $x^{n_k} = 1$. Since there are ${n_k}^k$ such elements and $x^{n_k} = 1$ has at most n_k roots, this forces $k = 1$ and $F^\times$ is cyclic.
2. Recall that $F/\mathbb{Z}_p$ where $p = \operatorname{char} F$. Thus $[F : \mathbb{Z}_p] = n < \infty$ so that $F = \mathbb{Z}_p(\alpha)$ and $|F| = p^n$.
3. Suppose $|F| = p^n$; by Lagrange, every $a \in F^\times$ satisfies $x^{p^n - 1} - 1$ so that every $a \in F$ satisfies $x^{p^n} - x$, so $x^{p^n} - x$ splits over F. Take $f(x) = x^{p^n} - x$, so that $f'(x) = -1$ and f is separable. Thus, any splitting field F must have at least p^n elemenets, so $|F|$ is minimal and F is a splitting field of $x^{p^n} - x$.
   Conversely, suppose F is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$. Consider $K = \{\alpha \in F : f(\alpha) = 0\}$, so that $K \leq F$. In particular, F splits in K, forcing $K = F$. Thus, $|F| = |K| \leq p^n$ since f can have at most p^n roots. However, as above, $f(x)$ is separable, so $|F| = |K| = p^n$.
4. Splitting fields are unique up to isomorphism. $\square$

Since the splitting field is unique, for any prime p and $n \in \mathbb{N}$, there exists a unique field of order p^n (up to isomorphism). We denote the field $\mathbb{F}_{p^n}$.

7.5 Theorem. *If E is a subfield of $\mathbb{F}_{p^n}$, then $E \cong \mathbb{F}_{p^r}$, where $r|n$. Moreover, if $r|n$, then $\mathbb{F}_{p^n}$ has a unique subfield of order p^r.*

Proof. Let E be a subfield of $\mathbb{F}_{p^n}$, so $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : E][E : \mathbb{F}_p]$. Set $r = [E : \mathbb{F}_p]$, $r|n$, and $|E| = p^r$.

Conversely, suppose $r|n$, and consider $\mathbb{F}_{p^n} = \{\alpha \in \overline{\mathbb{F}_p} : \alpha^{p^n} - \alpha = 0\}$. Since $r|n$, write $p^n - 1 = (p^r - 1)(p^{n-r} + p^{n-2r} + \cdots + p^r + 1)$. From before,

$$\begin{aligned} E &= \{\alpha \in \overline{\mathbb{F}_p} : \alpha^{p^r} - \alpha = 0\} \\ &= \{\alpha \in \overline{\mathbb{F}_p} : \alpha^{p^r - 1} - 1 = 0\} \cup \{0\} \\ &\subseteq \mathbb{F}_{p^n} \end{aligned}$$

Moreover, $|E| = p^r$. If K is any other subfield and $|K| = p^r$, then for any $0 \neq \alpha \in K$, $\alpha^{p^r - 1} = 1$ since $K^\times$ is cyclic, and $K \subseteq E$. $\square$

III. Galois Theory

TODO

- talk about maps $\sigma : K \hookrightarrow k^a$ (algebraic closure of k).
- full proof of algebraic closure
- isomorphism extension lemma in terms of emebeddings
- use lower case k for base field to distinguish.
- Use universal property of simple field extensions

8 Galois Groups

Let $f(x) \in F[x]$ be non-constant, and $\alpha_1, \dots, \alpha_n$ be the roots of $f(x)$ in its splitting field. Our goal is to study these roots by permuting them using automorphisms of K.

Definition. Let K/F. Recall that $\mathrm{Aut}(K)$ is the group of automorphisms of K. We define $\mathrm{Gal}(K/F) = \{\phi \in \mathrm{Aut}(K) : \phi|_F = \mathrm{id}\} \leq \mathrm{Aut}(K)$.

8.1 Lemma. *Let K/F. If $\alpha \in K$ is a root of $f(x) \in F[x]$ and $\phi \in \mathrm{Gal}(K/F)$, then $\phi(\alpha)$ is also a root of $f(x)$.*

Proof. Note that $0 = \phi(f(\alpha)) = f(\phi(\alpha))$ since ϕ fixes the coefficients of f. □

8.2 Corollary. *If $\alpha \in K$ is algebraic over F and $\phi \in \mathrm{Gal}(K/F)$, then $\phi(\alpha)$ is algebraic over F and has the same minimal polynomial in $F[x]$.*

Example. Compute $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$. If $\phi \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, then $\phi(\sqrt{2}) = \pm\sqrt{2}$ and $\phi(\sqrt{3}) = \pm\sqrt{3}$. Thus the automorphisms are given by.

$$\phi_1 = \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \phi_2 = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases}$$

$$\phi_3 = \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \qquad \phi_4 = \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

and $G = \{\phi_1, \phi_2, \phi_3, \phi_4\}$. Since $|\phi_i| = 2$ for all i, G is abelian, so $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Example. Consider $G = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$. If $\phi \in G$, then $\phi(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2\}$, so $\phi(\sqrt[3]{2}) = \sqrt[3]{2}$. Thus $\phi = \mathrm{id}$ and $G = \{\mathrm{id}\}$.

Let F be a field, $f(x) \in F[x]$, $\deg f(x) = n \geq 1$. Let K be the splitting field for $f(x)$ over F, so the roots of $f(x)$ are $\alpha_1, \alpha_2, \dots, \alpha_n$. Let $G = \mathrm{Gal}(K/F)$, so for any $\phi \in G$, $\phi(\alpha_i) = \alpha_j$. In particular, for any $\phi \in \mathrm{Gal}(K/F)$, $\phi(\alpha_i) = \alpha_{\pi(i)}$ for some $\pi \in S_n$. Thus the map $\mathrm{Gal}(K/F) \to S_n$ given by $\phi \mapsto \pi$ is injective.

Remark. If $f(x) \in F[x]$, K the splitting field for $f(x)$, then we write $\mathrm{Gal}(K/F) = \mathrm{Gal}(f(x))$.

Example. Consider $f(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$. Then $\mathrm{Gal}(f(x)) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Let $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$, $\alpha_4 = -\sqrt{3}$, so $\mathrm{Gal}(f(x)) = \{\epsilon, (34), (12), (12)(34)\}$.

Example. $\mathrm{Gal}(x^2+1) \cong \mathbb{Z}_2$ over $\mathbb{Q}[x]$, but $\mathrm{Gal}(x^2+1) = \{1\}$ over $\mathbb{Z}_2[x]$.

8.3 Corollary. *Let F be a field, $f(x) \in F[x]$ irreducible, K the splitting field for $f(x)$ over F. Then for any roots $\alpha, \beta \in K$ of $f(x)$, there exists $\phi \in \mathrm{Gal}(K/F)$ such that $\phi(\alpha) = \beta$.*

Proof. By the isomorphism extension lemma (Lemma 6.13), $\mathrm{id} : F \to F$ extents to an automorphism $\phi : F(\alpha) \to F(\beta)$ such that $\alpha \mapsto \beta$, which extends to an isomorphism $K \to K$. □

Definition. A subgroup H of S_n is *transitive* if for all $i, j \in \{1, 2, \ldots, n\}$, there exists $\pi \in H$ such that $\pi(i) = j$.

8.4 Corollary. *Let $f(x) \in F[x]$, $\deg f(x) = n \geq 1$, $f(x)$ separable and irreducible. Then $\mathrm{Gal}(f(x))$ is isomorphic to a transitive subgroup of S_n.*

Example. Compute $G = \mathrm{Gal}(x^3 - 2)$ over $\mathbb{Q}[x]$. Since $f(x) = x^3 - 2$ is irreducible, $f(x)$ is also separable. Then G is isomorphic to a transitive subgroup of S_3. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $f(x)$, and $x = \{\alpha_1, \alpha_2, \alpha_3\}$. Then G acts on X via $\phi \cdot \alpha_i = \phi(\alpha_i)$. By Orbit-Stabilizer, $|G| = |G \cdot \alpha| \cdot |\mathrm{Stab}(\alpha_1)|$. By transitivity, $|G \cdot \alpha| = 3$, so $3 \div |G|$ and $G \cong A_3$ or S_3.

Consider G as a subgroup of S_3 relative to the order $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \alpha_1\zeta_3$, $\alpha_3 = \alpha_1\zeta_3^2$. Note that $x^3 - 2$ is irreducible over $\mathbb{Q}(\zeta_3)$ since $x^3 - 2$ has no roots in $\mathbb{Q}(\zeta_3)$. Thus by the isomorphism extension lemma, there exists $\phi \in G$ such that the following diagram commutes:

$$\begin{tikzcd}
\mathbb{Q}(\zeta_3, \alpha_1) \arrow[r, "\phi : \phi(\alpha_1) = \alpha_1"] & \mathbb{Q}(\zeta_3, \alpha_1) \\
\mathbb{Q}(\zeta_3) \arrow[u, hook] \arrow[r, "\zeta_3 \mapsto \zeta_3^2"] & \mathbb{Q}(\zeta_3) \arrow[u, hook] \\
\mathbb{Q} \arrow[u, hook] \arrow[r, "\mathrm{id}"] & \mathbb{Q} \arrow[u, hook]
\end{tikzcd}$$

Thus $\phi(\alpha_1) = \alpha_1$, $\phi(\alpha_2) = \alpha_3$ and $\phi(\alpha_3) = \alpha_2$. Hence $\phi \sim (23) \in G$ is an element of order 2, so $G \cong S_3$.

Remark. When computing $G = \mathrm{Gal}(K/F)$, it is useful to know $|G|$.

Definition. Suppose K/F and E/F are field extensions. Any homomorphism $\phi : K \to E$ which fixes F is called an $F-$*map* from K to E.

Remark. If $\phi : K \to E$ is a $F-$map, since K is a field, ϕ is automatically injective. Furthermore, for any $\alpha \in F$, $v \in K$, $\phi(\alpha v) = \alpha\phi(v)$, so ϕ is $F-$linear.

If $\phi : K \to K$ and $[K : F] < \infty$, then ϕ is surjective and $\phi : K \to K$ is an $F-$map if and only if $\phi \in \mathrm{Gal}(K/F)$.

8.5 Lemma. *Let K/F, E/F, $[K : E] < \infty$. The number of distinct $F-$maps $\phi : K \to E$ is at most $[K : F]$.*

Proof. We proceed inductively on the number of generators of K/F. If $K = F(\alpha_1)$ and $\phi : K \to E$ is an $F-$map, then α_1 and $\phi(\alpha_1)$ have the same minimal polynomial over F. Thus there are at most $[F(\alpha_1) : F] = [K : F]$ options $\phi(\alpha_1)$, so there are at most $[K : F]$ many such $F-$maps.

Now assume $K = F(\alpha_1, \ldots, \alpha_n)$, and let $L = F(\alpha_1, \ldots, \alpha_{n-1})$. Let $\phi : K \to E$ be an $F-$map, so $\phi|_L : L \to E$ is an $F-$map. By induction, the number of possible $\phi|_L$ is at most $[L : F]$. Since ϕ is completely determined by $\phi|_L$ and $\phi(\alpha_n)$, there are at most $[L : F][L(\alpha_n) : L] = [K : F]$ possibilities for ϕ. □

Remark. How can it happen that $|\operatorname{Gal}(K/F)| < [K : F]$? It could be that the extension is not normal; i.e. the extension has conjugates not contained in the extension.

It can also happen that there are repeated roots: consider $G = \operatorname{Gal}(\mathbb{Z}_2(t)/\mathbb{Z}_2(t^2))$, so $[\mathbb{Z}_2(t) : \mathbb{Z}_2(t^2)] = 2$. Then $t \mapsto x^2 - t^2 \in \mathbb{Z}(t^2)[x]$, so $(x-t)^2 \in \mathbb{Z}(t)[x]$. Thus if $\phi \in G$, then $\phi(t) = t$, so $\phi = \mathrm{id}$ and $G = \{1\}$.

9 SEPARABLE AND NORMAL EXTENSIONS

Definition. We say $\alpha \in K$ is *separable* if α is algebraic over F and its minimal polynomial is separable (over F). We say K/F is *separable* if K/F is algebraic and all elements of K are separable over F. A field F is *perfect* if every algebraic extension of F is separable.

Remark. Suppose $f(x) \in F[x]$ is irreducible. Then $f(x)$ is separable if and only if $f'(x) \neq 0$.

9.1 Proposition. *Let $f(x) \in F[x]$ be irreducible.*
1. *If $\operatorname{char}(F) = 0$, then $f(x)$ is separable.*
2. *If $\operatorname{char}(F) = p > 0$ then $f(x)$ is not separable if and only if $f(x) = g(x^p)$ for some $g(x) \in F[x]$.*

Proof. Immediate from the preceding remark. □

9.2 Corollary.
1. *If $\operatorname{char}(F) = 0$, then F is perfect.*
2. *If $\operatorname{char}(F) = p$, then F is perfect if and only if $\phi(x) = x^p$ is an automorphism.*

Proof. (1) is clear, so we prove (2). In characteristic p, ϕ is always injective.

First suppose $\phi(x) = x^p$ is also surjective. Suppose there exists $f(x) \in F[x]$ irreducible but not separable. Thus $f(x) = g(x^p)$, and write

$$\begin{aligned} f(x) &= a_n x^{pm_n} + \cdots + a_1 x^{pm_1} + a_0 \\ &= b_n^p x^{pm_n} + \cdots + b_1^p x^{pm_1} + b_0^p \\ &= (b_n x^{m_n} + \cdots + b_x x^{m_1} + b_0)^p \end{aligned}$$

Conversely, suppose x^p is not an automorphism; in particular, x^p is not surjective. Let $\alpha \notin \operatorname{im}(\phi)$. But then $f(x) = x^p - \alpha$ is irreducible, but if K is the splitting field for F, then r is a root so $r^p = \alpha$ and $(x-r)^p = x^p - \alpha$ and f is not separable. □

Remark. Since the Frobenius map is an isomorphism when F is a finite field, every finite field is perfect.

9.3 Theorem. *Let $f(x) \in F[x]$ be non-constant and separable, and K the splitting field for $f(x)$ over F. Then $|\operatorname{Gal}(K/F)| = [K : F]$.*

Proof. We proceed by induction on $[K : F]$. If $[K : F] = 1$, this is obvious.

Otherwise, let $[K : F] = n > 1$. Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$, so $p(x)$ is also separable over F. Say the roots of $p(x)$ are $\alpha_1, \alpha_2, \dots, \alpha_m$ where $m = \deg p(x)$; suppose $\alpha_1 \notin F$ and let $E = F(\alpha_1)$. Then $K/E/F$ is a tower of fields with $[K : E] = \frac{n}{m} < n$. Furthermore, K is the splitting field for $f(x)$ over E, so by induction, $|\operatorname{Gal}(K/E)| = [K : E] = \frac{n}{m}$.

Since $p(x) \in F[x]$ is irreducible, for all j, get $\phi_j \in \operatorname{Gal}(K/F)$ such that $\phi_j(\alpha_1) = \alpha_j$; note that $\phi_1, \dots, \phi_m$ are distinct in $\operatorname{Gal}(K/F)$. Moreover, $\phi_j^{-1} \circ \phi_i(\alpha_1) \neq \alpha_1 \in E$. Thus $\phi_j^{-1} \circ \phi_i \notin \operatorname{Gal}(K/E)$, so $\phi_i \operatorname{Gal}(K/E) \neq \phi_j \operatorname{Gal}(K/E)$. Thus $|\operatorname{Gal}(K/F)/\operatorname{Gal}(K/E)| \geq m$. Thus $|\operatorname{Gal}(K/F)| \geq m |\operatorname{Gal}(K/E)| = n$, and we're done. □

Definition. We say an extension K/F is *simple* if there exists $\alpha \in K$ such that $K = F(\alpha)$. We say α is a *primitive element* for K/F.

9.4 Theorem (Primitive Element). *If K/F is finite and separable, then K/F is simple.*

Proof. Suppose K/F is finite and separable.

First suppose F is finite, so that K is also finite and $K^\times = \langle \alpha \rangle$ for some $\alpha \in K$. Thus, $K = F(\alpha)$.

Otherwise, F is infinite, and write $K = F(\pi_1, \dots, \pi_n)$ for some $\pi_i \in K$. It suffices to prove the result for $n = 2$; say, $K = F(\alpha, \beta)$. Let p, q be the minimal polynomial of α and β respectively. Let L be the splitting field for $p(x)q(x)$ over K, and let $\alpha = \alpha_1, \dots, \alpha_n$ and $\beta = \beta_1, \dots, \beta_k$ the distinct conjugates in L of α and β (since K/F is separable). Let

$$S = \left\{ \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j} : 1 < i \leq n, 1 < j \leq m \right\}$$

Since S is finite and F is infinite, get $u \in S \setminus F$ so that $\gamma := \alpha + u\beta \neq \alpha_i + u\beta_j$ for any $i, j \neq 1$. Certainly $F(\gamma) \subseteq F(\alpha, \beta)$. Let $h(x)$ be the minimal polynomial for β over $F(\gamma)$. Since $q(x) \in F(\gamma)[x]$ and $q(\beta) = 0$, $h(x) | q(x)$. As well, $h(x) | p(\gamma - ux)$ since $p(\gamma - u\beta) = 0$; but the only shared root is β by choice of u, $\deg h = 1$ and $\beta \in F(\gamma)$. □

9.5 Corollary. *If F is perfect and $[K : F] < \infty$, then K/F is simple.*

TODO: move def'n of conjugates somewhere more logical.

Definition. Let $[K : F] < \infty$. We say K/F is *normal* if K is the splitting field of some non-constant $f(x) \in F[x]$ over F. Suppose $\alpha \in K$ has minimal polynomial $p(x) \in F[x]$. The roots of $p(x)$ in its splitting field are called the *$F-$conjugates* (or just *conjugates* when the base field is clear) of α.

Remark. If $\phi : K \to E$ is an $F-$map and α has minimal polynomial $p(x) \in F[x]$, then $p(\phi(\alpha)) = \phi(p(\alpha)) = \phi(0) = 0$, so that $\phi(\alpha)$ is also a conjugate of $p(x)$ in a splitting field L/F.

9.6 Theorem (Characterization of Normal Extensions). *Let $[K : F] < \infty$. The following are equivalent:*

1. *K/F is normal.*
2. *For every L/K, if ϕ is an $F-$map from L to L, then $\phi|_K \in \operatorname{Gal}(K/F)$.*
3. *If $\alpha \in K$, then all of the $F-$conjugates of α are in K.*

4. *If $\alpha \in K$, then its minimal polynomial splits over K.*

Proof. ($1 \Rightarrow 2$) If K/F is normal, then K is the splitting field of some $f(x) \in F[x]$. Let $\phi : L \to L$ be an $F-$map. Write $K = F(\alpha_1, \ldots, \alpha_n)$ where α_i are the roots of $f(x)$ in K. It suffices to show that $\phi|_K(K) \subseteq K$. For each i, there exists j such that $\phi|_K(\alpha_i) = \phi(\alpha_i) = \alpha_j \in K$. Since each $x \in K$ is a $F-$linear combination of the α_i, it follows that $\phi(x) \in K$, and the result follows.

($2 \Rightarrow 3$) Let $\alpha \in K$ with minimal polynomial $f(x) \in F[x]$. Since $[K : F] < \infty$, $K = F(\alpha_1, \ldots, \alpha_n)$ with $\alpha_i \in K$. For each i, let h_i be the minimal polynomial for α_i over F. Let $p(x) = f(x)h_1(x)h_2(x)\cdots h_n(x)$ and L be the splitting field of $p(x)$ over F. Such a choice is necessary to ensure $L/K/F$. Let $\beta \in L$ be a root of $f(x)$, and get $\phi \in \mathrm{Gal}(L/F)$ such that $\phi(\alpha) = \beta$. By assumption, $\phi|_K \in \mathrm{Gal}(K/F)$, so $\beta = \phi(\alpha) \in K$, as required.

($3 \Rightarrow 4$) Immediate.

($4 \Rightarrow 1$) Since $[K : F] < \infty$, $K = F(\alpha_1, \ldots, \alpha_n)$ for $\alpha_i \in K$. Let $h_i(x)$ be the minimal polynomial for α_i over F, and set $f(x) = h_1(x)\cdots h_n(x)$. Then the splitting field for $f(x)$ over F is $F(\alpha_1, \ldots, \alpha_n) = K$. □

Example. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal. $\mathbb{F}_{p^n}/\mathbb{F}_p$ is normal, since it is the splitting field of $x^{p^n} - x$. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is normal with $\Phi_n(x)$. $\mathbb{Z}_p(t)/\mathbb{Z}_p(t^n)$ is normal with $x^p - t^p$.

10 GALOIS EXTENSIONS AND THE FUNDAMENTAL THEOREM

Definition. We say that K/F is *Galois* if K/F is normal and separable.

Remark. If F is perfect and K/F is finite, then K/F is Galois if and only if K/F is normal.

Definition. Let K be a field and $G \leq \mathrm{Aut}(K)$. Then the *fixed field* of G is

$$\mathrm{Fix}(G) = \{a \in K : \phi(a) = a \text{ for all } \phi \in G\}$$

Remark. Certainly $\mathrm{Fix}(\mathrm{Gal}(K/F)) \supseteq F$ by definition.

10.1 Theorem (Characterization of Galois Extensions). *The following are equivalent:*

1. *K is the splitting field of a non-constant separable $f(x) \in F[x]$ over F.*
2. $|\mathrm{Gal}(K/F)| = [K : F]$
3. $\mathrm{Fix}(\mathrm{Gal}(K/F)) = F$
4. *K/F is Galois*

Proof. ($1 \Rightarrow 2$) This is Theorem 9.3.

($2 \Rightarrow 3$) Assume $|\mathrm{Gal}(K/F)| = [K : F]$ and set $E = \mathrm{Fix}(\mathrm{Gal}(K/F))$ so that $K/E/F$ is a tower of fields. Moreover, $\mathrm{Gal}(K/E) \leq \mathrm{Gal}(K/F)$ is a subgroup so $[K : F] = |\mathrm{Gal}(K/F)| \geq |\mathrm{Gal}(K/E)|$. Let $a \in E$ and $\phi \in \mathrm{Gal}(K/F)$. Then $\phi(a) = a$ by the definition of E, so $\mathrm{Gal}(K/E) = \mathrm{Gal}(K/F)$. Thus

$$[K : F] = |\mathrm{Gal}(K/F)| = |\mathrm{Gal}(K/E)| \leq [K : E] \leq [K : F]$$

so equality holds and $[E : F] = 1$ by the tower theorem.

($3 \Rightarrow 4$) Assume $\mathrm{Fix}(\mathrm{Gal}(K/F)) = F$. Let $\alpha \in K$ with minimal polynomial $p(x) \in F[x]$; we must show $p(x)$ that splits over K with no repeated roots. Let $G = \mathrm{Gal}(K/F)$

and $\{\alpha_1, \ldots, \alpha_n\} = \{\phi(\alpha) : \phi \in G\} \subseteq K$. Without loss of generality, $\alpha = \alpha_1$, and consider $h(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in K[x]$. Then if $\phi \in G$, $\phi(h(x)) = h(x) \in (\operatorname{Fix} G)[x] = F[x]$ since ϕ acts by permutation on the α_i. Thus $h(x)$ splits over K with no repeated roots, and in fact $h(x) = p(x)$ since every root of $h(x)$ is a $F-$conjugate of α, and thus a root of $p(x)$.

($4 \Rightarrow 1$) Since K/F is finite, $K = F(\alpha_1, \ldots, \alpha_n)$, $\alpha_i \in K$. For each i, let $q_i(x) \in F[x]$ be its minimal polynomial. Say $p_1(x), \ldots, p_m(x)$ is a list of distinct $q_i(x)$. Then $f(x) = p_1(x) \cdots p_m(x)$, and since K/F is normal, its splitting field over F is K, and by A6, $f(x)$ is separable. □

Example. Consider $\alpha = \sqrt{2 + \sqrt{3}} \in \mathbb{C}$, with minimal polyomial $x^4 - 4x^2 + 1$. Since $\mathbb{Q}$ is perfect, we only need to check normality, and $f(x)$ has roots $\pm\sqrt{2 \pm \sqrt{3}}$. The $\mathbb{Q}-$conjugates of α are $\pm\alpha, \pm\beta$ where $\beta = \sqrt{2 - \sqrt{3}}$. Since $\alpha\beta = 1$, $\beta = \alpha^{-1}$. Thus $\pm\alpha, \pm\beta \in \mathbb{Q}(\alpha)$ and $\mathbb{Q}(\alpha)/\mathbb{Q}$ is normal.

	α	$-\alpha$	β	$-\beta$	S_4
ϕ_1	α	$-\alpha$	β	$-\beta$	ϵ
ϕ_2	$-\alpha$	α	$-\beta$	β	$(12)(34)$
ϕ_3	β	$-\beta$	α	$-\alpha$	$(13)(24)$
ϕ_3	$-\beta$	β	$-\alpha$	α	$(14)(23)$

so $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

10.2 Theorem (Artin). *Let K be a field, H a finite subgroup of $\operatorname{Aut}(K)$. Let $F = \operatorname{Fix} H$. Then*

1. *K/F is Galois*
2. *$\operatorname{Gal}(K/F) = H$*
3. *$|H| = [K : F]$*

Proof. Let $\alpha \in K$ and $\sigma_1, \ldots, \sigma_r \in H$ with r maximal such that the $\sigma_i(\alpha)$ are distinct. If $\tau \in G$ is arbitrary, then $(\tau \circ \sigma_i(\alpha))$ differs from $(\sigma_i(\alpha))$ only by a permutation: by maximality of r, $\tau \circ \sigma_i(\alpha) = \sigma_j(\alpha)$ for every i and some j. Injectivity of τ shows that it is indeed a permutation. Thus taking $\tau = \sigma_1^{-1}$ if necessary, we may assume that $\sigma_1(\alpha) = \alpha$ and α is a root of the polynomial

$$f(x) = \prod_{i=1}^{r} (x - \sigma_i(\alpha))$$

and for any $\tau \in G$, $\tau(f) = f$. Thus $f(x) \in (\operatorname{Fix} H)[x] = F[x]$. Since the $\sigma_i(\alpha)$ are distinct, f is separable.

Since $\alpha \in K$ was arbitrary and $r \leq |H|$, we see that every $\alpha \in K$ is the root of a separable polynomial with degree at most $|H|$ and coefficients in F, and the polynomial splits in K. Thus K/F and since the minimal polynomial of each $\alpha \in F$ splits completely in K, K/F is normal by Theorem 9.6. In particular, by the primitive element theorem (Theorem 9.4), $K = F(\alpha)$ where the degree of α is at most $|H|$, so that $[K : F] \leq |H|$.

Note that $H \subseteq \operatorname{Gal}(K/F)$ and $|H| \leq |\operatorname{Gal}(K/F)| \leq [K : F]$; we have shown that $[K : F] \leq |H|$, so we're done. □

10.1 THE FUNDAMENTAL THEOREM OF GALOIS THEORY

We adopt the following notation for the rest of this section. Suppose K/F: then $\mathcal{E} = \{E : F \subseteq E \subseteq K\}$ is the set of intermediate subfields of K/F, and $\mathcal{H}$ is the set of subgroups of $\operatorname{Gal}(K/F)$. We then define the *Galois correspondence* by

$$\begin{aligned}
\mathcal{E} &\longleftrightarrow \mathcal{H}\\
E &\longmapsto \operatorname{Gal}(K/E)\\
\operatorname{Fix} H &\longleftarrow\!\shortmid\ H
\end{aligned}$$

Note that if $E_1 \subseteq E_2$ in $\mathcal{E}$, then $\operatorname{Gal}(K/E_1) \supseteq \operatorname{Gal}(K/E_2)$. Similarly, if $H_1 \subseteq H_2$ in $\mathcal{H}$, then $\operatorname{Fix} H_1 \supseteq \operatorname{Fix} H_2$. Thus the Galois correspondence is inclusion reversing.

10.3 Theorem (Fundamental Theorem of Galois Theory). *Let K/F be a finite Galois extension. The Galois correspondences give an inclusion-reversing bijection (antitone Galois connection) between $\mathcal{E}$ and $\mathcal{H}$:*

1. *If $E \in \mathcal{E}$, then $\operatorname{Fix}(\operatorname{Gal}(K/E)) = E$. In particular, K/E is Galois.*
2. *If $H \in \mathcal{H}$, then $\operatorname{Gal}(K/\operatorname{Fix}(H)) = H$.*

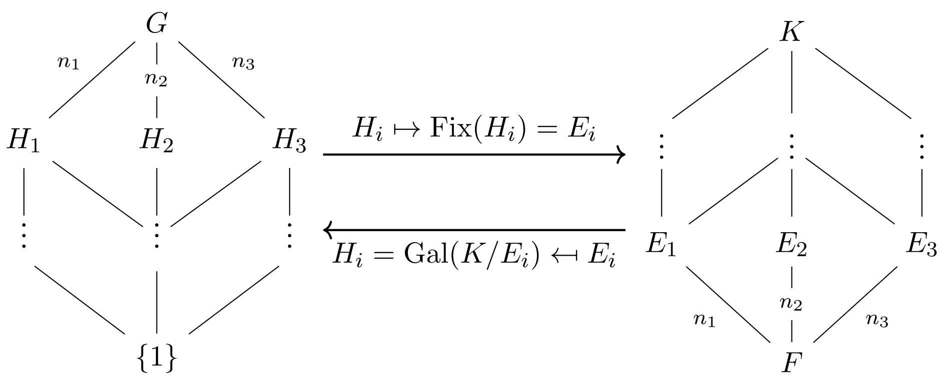
Proof. 1. K/F is normal and separable, so K/E is also normal and separable so that K/E is Galois. Thus the result follows by Theorem 10.1.
2. This is a direct application of Theorem 10.2. □

10.4 Corollary. *Suppose K/F is finite Galois. If $H_1 \subseteq H_2$ in $\mathcal{H}$, then $[H_2 : H_1] = [\operatorname{Fix} H_1 : \operatorname{Fix} H_2]$.*

Proof. We have

$$\begin{aligned}
[\operatorname{Fix} H_1 : \operatorname{Fix} H_2] &= \frac{[K : \operatorname{Fix} H_2]}{[K : \operatorname{Fix} H_1]}\\
&= \frac{|\operatorname{Gal}(K/\operatorname{Fix} H_2)|}{|\operatorname{Gal}(K/\operatorname{Fix} H_1)|}\\
&= \frac{|H_2|}{|H_1|} = [H_2 : H_1]
\end{aligned}$$ □

To summarize the previous results, perhaps the easiest way to visualize it is with a digram. On the left, we have the subgroup lattice of $G = \operatorname{Gal}(K/F)$, and on the right, we have the intermediate fields of K/F.



Example. Consider $G = \mathrm{Gal}(x^3 - 2)$ and set $\alpha = \sqrt[3]{2}$. Since $\mathbb{Q}$ is perfect and $x^3 - 2$ is irreducible, then $x^3 - 2$ is separable, so $\mathbb{Q}(\alpha, \zeta_3)$ is the splitting field for $x^3 - 2$ over $\mathbb{Q}$. Then $|G| = [\mathbb{Q}(\alpha, \zeta_3) : \mathbb{Q}] = 6$ and since $G \leq S_3$, $G \cong S_3$.

10.5 Proposition. *Let E be an intermediate subfield of K/F. For any $\phi \in \mathrm{Gal}(K/F)$, $\phi \,\mathrm{Gal}(K/E)\phi^{-1} = \mathrm{Gal}(K/\phi(E))$.*

Proof. For any $\psi \in \mathrm{Aut}(K)$,

$$\begin{aligned} \psi \in \mathrm{Gal}(K/E) &\iff \psi(\alpha) = \alpha \text{ for all } \alpha \in E \\ &\iff \psi \circ \phi^{-1} \circ \phi(\alpha) = \phi^{-1} \circ \phi(\alpha) \text{ for all } \alpha \in E \\ &\iff \psi \circ \phi^{-1}(\beta) = \phi^{-1}(\beta) \text{ for all } \beta \in \phi(E) \\ &\iff \phi \circ \psi \circ \phi^{-1}(\beta) = \beta \text{ for all } \beta \in \phi(E) \\ &\iff \phi \circ \psi \circ \phi^{-1} \in \mathrm{Gal}(K/\phi(E)) \end{aligned}$$ □

Definition. Let $K/E/F$ and $H \leq \mathrm{Gal}(K/F)$. We say E is *invariant* under H if $\phi(E) = E$ for all $\phi \in H$.

10.6 Proposition. *Suppose K/F is finite and Galois. If E is an intermediate subfield of K/F, then the following are equivalent:*

1. *E/F is Galois*
2. *E is $\mathrm{Gal}(K/F)-$invariant*
3. $\mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F)$

Proof. $(2 \Leftrightarrow 3)$ This is straightfoward in light of Proposition 10.5.

$(1 \Rightarrow 2)$ Suppose E/F is Galois and take $\phi \in \mathrm{Gal}(K/F)$. Since E/F is Galois, $\phi|_E \in \mathrm{Gal}(E/F)$; thus, $\phi|_E(E) = \phi(E) = E$.

$(2 \Rightarrow 1)$ Suppose E is $G-$invariant where $G = \mathrm{Gal}(K/F)$. By A7, E/F is separable. To show normality, we show that E is closed under conjugation. Let $\alpha \in E$ with minimal polynomial $f(x) \in F[x]$. Since K/F is normal, $f(x)$ splits over K. Let $\beta \in K$ be a $F-$conjugate of α. Since $f(x) \in F[x]$ is irreducible, there exists $\phi \in G$ such that $\phi(\alpha) = \beta$ so that $\beta = \phi(\alpha) \in \phi(E) = E$. □

10.7 Proposition. *Let $K/E/F$, K/F finite and Galois. If E/F is Galois, then* $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$.

Proof. Consider the map $\psi : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F)$ given by $\psi(\phi) = \phi|_E$. Then $\ker \psi = \mathrm{Gal}(K/E)$ and the result follows by the first isomorphism theorem. □

11 GALOIS GROUP COMPUTATIONS

Example (Cyclotomic Galois Group). Let's compute $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Note that $\mathbb{Q}(\zeta_n)$ is the splitting field for the separable polynomial $\Phi_n(x)$ over $\mathbb{Q}$ so that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois. To see that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^\times$, one can realize that the map $\psi : \mathbb{Z}_n^\times \to G$ by $\psi(k) = \{\zeta_n \mapsto \zeta_n^k\}$ is an isomorphism.

Example (Finite Field Galois Group). We can also compute $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Since $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$, $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois with index n. Consider the Frobenius map $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ such that $\phi(a) = a^p$; by Fermat, $\phi \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Let $j = |\phi|$, so $j \leq n$. Furthermore, since ϕ is an automorphism, every element of $\mathbb{F}_{p^n}$ is a root of $x^{p^j} - x$, which is only possible if $j \geq n$. Thus equiality holds and $G = \langle \phi \rangle$.

We now turn towards computing the Galois groups of arbitrary splitting fields of cubic and quadratic polynomials. To do this, we need to introduce some new machinery.

Definition. Let $f(x) \in F[x]$ be non-constant with splitting field K. Say $f(x) = u(x - \alpha_1)\cdots(x - \alpha_n) \in K[x]$. We say

$$\mathrm{disc}\, f(x) = \prod_{i<j}(\alpha_i - \alpha_j)^2$$

is the *discriminant* of $f(x)$.

Remark. (i) $\mathrm{disc}(f(x)) \neq 0$ if and only if $f(x)$ is separable.
(ii) If $f(x) = x^2 + bx + c$, then $\mathrm{disc}\, f(x) = b^2 - 4c$.

11.1 Lemma. *Suppose $f(x) \in F[x]$ is non-constant. Then $\mathrm{disc}\, f(x) \in F$.*

Proof. If $f(x)$ is not separable, this is obvious, so suppose $f(x)$ is separable. For all $\phi \in \mathrm{Gal}(f(x))$, $\phi(\mathrm{disc}\, f(x)) = \mathrm{disc}\, f(x)$, so $\mathrm{disc}\, f(x) \in \mathrm{Fix}(\mathrm{Gal}(f(x))) = F$. ☐

11.2 Proposition. *Suppose $\mathrm{char}\, F \neq 2$, $f(x)$ separable with degree $n \geq 2$. Set $G = \mathrm{Gal}\, f(x)$ and $d = \prod_{i<j}(\alpha_i - \alpha_j)$.*

If $\phi \in G \subseteq S_n$, then $\phi(d) = \pm d$. Moreover, $\phi(d) = d$ if and only if $\phi \in A_n$. In particular, $\mathrm{Gal}(K/F(d)) = G \cap A_n$ and $G \subseteq A_n$ if and only if $d \in \mathrm{Fix}(G) = F$.

Proof. Let $\phi \in G$, so $d, \phi(d)$ are roots of $x^2 - d^2 \in F[x]$; thus, $\phi(d) = \pm d$. Observe that S_n acts on $X = \{d, -d\}$ by

$$\sigma \cdot \prod_{i<j}(\alpha_i - \alpha_j) = \prod_{i<j}(\alpha_{\sigma(i)} - \alpha_{\sigma(j)})$$

Moreover, $\epsilon \cdot d = d$ and $((n)(n-1)) \cdot d = -d$, so the action is transitive. By Orbit-Stabilizer, $n! = |S_n| = |\mathrm{Stab}(d)| \cdot |S_n \cdot d| = |\mathrm{Stab}(d)| \cdot 2$, so $\mathrm{Stab}(d) = A_n$ since A_n is the only index 2 subgroup of S_n. ☐

For the remainder of this section, we will assume that $\mathrm{char}\, F \neq 2, 3$.

11.1 Galois Groups from Cubic Splitting Fields

We first treat the case where $f(x)$ is cubic. If $f(x) \in F[x]$ is irreducible and separable, then $\operatorname{Gal} f(x) \cong S_3$ or A_3. Suppose $g(x) = x^3 + \alpha x^2 + \beta x + \gamma \in F[x]$ irreducible and separable and consider $f(x) = g(x - \alpha/3) = x^3 + bx + c \in F[x]$. Note that $f(x)$ is still irreducible and separable; in particular, $\operatorname{Gal} f(x) = \operatorname{Gal} g(x)$. Such a cubic is called a *depressed cubic*. One can compute $\operatorname{disc} f(x) = -4b^3 - 27c^2$. Then by applying Proposition 11.2, we see that

$$\operatorname{Gal} f(x) = \begin{cases} A_3 & : \operatorname{disc} f(x) = d^2, d \in F \\ S_3 & : \text{otherwise} \end{cases}$$

11.2 Galois Groups from Quartic Splitting Fields

Suppose $f(x) = x^4 + \alpha x^3 + \beta x^2 + \gamma x + \delta \in F[x]$; as before, we take $g(x) = f(x - \alpha/4) = x^4 + bx^2 + cx + d$, and $\operatorname{Gal}(f(x)) = \operatorname{Gal}(g(x))$. If $G = \operatorname{Gal} f(x)$, then G is a transitive subgroup of S_4 with $4 \div |G|$. Thus, the possible options are S_4, A_4, D_4, V, C_4, where $V = \{\epsilon, (12)(34), (13)(24), (14)(23)\}$.

Let the roots of $f(x)$ be given by $\alpha_1, \ldots, \alpha_4$. Let $K = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and set

$$\begin{aligned} u &= \alpha_1\alpha_2 + \alpha_3\alpha_4 \\ v &= \alpha_1\alpha_3 + \alpha_2\alpha_4 \\ w &= \alpha_1\alpha_4 + \alpha_2\alpha_3 \end{aligned}$$

We define the *resolvent cubic* of $f(x)$

$$\operatorname{Res} f(x) = (x-u)(x-v)(x-w) = x^3 - bx^2 - 4dx + 4bd - c^2 \in F[x]$$

where the coefficients may be evaluated by the reader.

Let $L = F(u, v, w)$, so that $K/L/F$. Since K/F is Galois, K/L is Galois, and

$$\operatorname{Gal}(\operatorname{Res} f(x)) = \operatorname{Gal}(L/F).$$

Since $\operatorname{Gal}(K/L) = G \cap V$ and L/F is Galois, $\operatorname{Gal}(K/L) \trianglelefteq \operatorname{Gal}(K/F)$, and $\operatorname{Gal}(L/F) = G/G \cap V$. Let $m = |\operatorname{Gal}(\operatorname{Res} f(x))|$.

G	S_4	A_4	D_4	V	C_4
$G \cap V$	V	V	V	V	C_2
$G/(G \cap V)$	S_3	C_3	C_2	$\{1\}$	C_2
m	6	3	2	1	2

Note that G is uniquely determined when $m \in \{1, 3, 6\}$, so let's examine the case $m = 2$. Since $\deg(\operatorname{Res} f(x)) = 3$ and $m = 2$, exactly one of u, v, or w is in F. Without loss of generality, assume $u \in F$. Either option for G has a 4-cycle which fixes u, so $\sigma = (1324) \in G$ and $\sigma^2 = (12)(34) \in G$. Consider

$$\begin{aligned} (x - \alpha_1\alpha_2)(x - \alpha_3\alpha_4) &= x^2 - ux + d \\ (x - (\alpha_1 + \alpha_2))(x - (\alpha_3 + \alpha_4)) &= x^2 + (b - u) \end{aligned}$$

Let's see that $G = \langle \sigma \rangle \cong C_4$ if and only if both of these polynomials split over L.

($\Longrightarrow$) Suppose $G = \langle\sigma\rangle$. Then $\mathrm{Gal}(K/L) = G \cap V = \langle\sigma^2\rangle$, so $\alpha_1\alpha_2$, $\alpha_3\alpha_4$,$\alpha_1+\alpha_2$,$\alpha_3+\alpha_4 \in \mathrm{Fix}\langle\sigma^2\rangle = L$.

($\Longleftarrow$) Conversely, suppose $\alpha_1\alpha_2$, $\alpha_3\alpha_4$,$\alpha_1+\alpha_2$,$\alpha_3+\alpha_4 \in L$. Then $\alpha_1\alpha_2 \in L(\alpha_1)$ that $\alpha_1, \alpha_2 \in L(\alpha_1)$. Then since $v - w = (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4) \in L$, so $\alpha_3 - \alpha_4 \in L(\alpha_1)$ as well, so that $\alpha_3, \alpha_4 \in L(\alpha_1)$.

Now, $K = F(\alpha_1, \ldots, \alpha_4) = L(\alpha_1)$, and $[K : L] = [L(\alpha_1) : L] = |\operatorname{Gal}(K/L)|$. The polynomial $p(x) = x^2 - (\alpha_1+\alpha_2)x + \alpha_1\alpha_2 \in L[x]$ has $p(\alpha_1) = 0$ so that $[K : L] \le 2$. Thus $[K : F] \le 4$, which forces $G = C_4$. TODO: why is $[L : F] \le 2$?

Example. Consider $f(x) = x^4 - 2x - 2$. Then $\operatorname{Res} f(x) = x^3 + 8x - 4$ has no rational roots, and is irreducible. Now, $\operatorname{disc}(\operatorname{Res} f(x)) = -4 \cdot (8^3) - 27 \cdot 4^2 < 0$ is not a square in $\mathbb{Q}$, so $\operatorname{Gal}(\operatorname{Res} f(x)) = S_3$. Thus $\operatorname{Gal} f(x) \cong S_4$.

Example. Consider $g(x) = x^4 + 5x + 5$, irreducible by Eisenstein, so $\operatorname{Res} g(x) = x^3 - 20x - 25 = (x-5)(x^2+5x+5)$. Thus $\operatorname{Gal}\operatorname{Res} g(x) = \mathbb{Z}_2$, and $m = 2$. We let $u = 5 \in \mathbb{Q}$. Consider $x^2 - 5x - 5$ and $x^2 - 5$. The roots of $x^2 + 5x + 5$ are $\frac{-5\pm\sqrt{5}}{2}$, so $L = \mathbb{Q}(\sqrt{5})$. The roots of $x^2 - 5$ are also in L. Thus $\operatorname{Gal} f(x) = \mathbb{Z}_4$.

12 SOLVABILITY AND RADICAL EXTENSIONS

Throughout this section, we assume that $\operatorname{char} F = 0$.

Definition. A group G is *solvable* if there exists a chain of subgroups $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = \{1\}$ such that ${G_i}/{G_{i+1}}$ is abelian.

Example. Any abelian solvable is abelian. We have $S_4 \supseteq A_4 \supseteq V \supseteq \{1\}$, so S_4 is solvable. If G is simple, then G is solvable if and only if G is abelian. For example, A_5 is simple and non-abelian, and thus not solvable.

12.1 Proposition. *If G is solvable and $N \le G$, then N is solvable; if $N \trianglelefteq G$, then G/N is solvable.*

Proof. Since G is solvable, get $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_n = \{1\}$. Then

- Consider the sequence $N = G_0 \cap N \trianglerighteq G_1 \cap N \trianglerighteq \cdots \trianglerighteq G_n \cap N = \{1\}$, since normality is preserved under intersection. Furthermore,
$$ {N \cap G_i}/{N \cap G_{i+1}} \cong {(N \cap G_i)G_{i+1}}/{G_{i+1}} \subseteq {G_i}/{G_{i+1}} $$
is abelian.
- Consider the sequence $G/N = G_0/N \trianglerighteq G_1/N \trianglerighteq \cdots \trianglerighteq G_n/N = \{1\}$ and use the third isomorphism theorem. TODO: finish this, something is weird: N is not a normal subgroup of G_i, use correspondence theorem for normal subgroups. $\square$

12.2 Proposition. *Let $N \trianglelefteq G$; then N is solvable if and only if N and ${G}/{N}$ are solvable.*

Proof. The forward direction is done; conversely, suppose N and G/N are solvable. Let
$$ N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_m = \{1\} $$
$$ G/N = G_0/N \supseteq G_1/N \supseteq \cdots \supseteq G_l/N = \{N\} $$
By the third isomorphism theorem, ${G_i/N}/{G_{i+1}/N} \cong {G_i}/{G_{i+1}}$, so $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq N$. TODO: fix this. $\square$

Remark. Let G be finite, solvable. By refining the chain as much as possible, we may assume $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ with G_i/G_{i+1}, and no $H_i \leq G$ with $G_i \supsetneq H_i \supseteq G_{i+1}$ normal. That is to say, G_i/G_{i+1} is abelian and simple, so $\left|G_i/G_{i+1}\right|$ prime.

Definition. We say K/F is a *simple radical extension* if $K = F(\alpha)$ for some $\alpha \in K$ such that $\alpha^n \in F$ for some $n \in \mathbb{N}$. A *radical tower* over F is a tower $K_m/K_{m-1}/\cdots/K_1/F$ such that K_1/F and K_{i+1}/K_i are each simple radical extensions. We say K/F is *radical* if there exists a radical tower over F starting at K. We say $f(x) \in F[x]$ is *solvable by radicals* over F if its splitting field is contained in a radical extension of F.

Example. Consider $f(x) = x^4 - 4x^2 + 2$. Then $\mathbb{Q}(\sqrt{2+\sqrt{2}}) \supseteq \mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$ is solvable by radicals over $\mathbb{Q}$.

Definition. We say an extension K/F is *cyclic* if K/F is finite and Galois, and $\mathrm{Gal}(K/F)$ is cyclic.

12.3 Proposition. *If F contains a primitive n^{th} root of unity and $K = F(\alpha)$ with $\alpha^n \in F$, then K/F is cyclic.*

Proof. Consider $f(x) = x^n - \alpha^n \in F[x]$. Let $\zeta \in F$ be a primitive n^{th} root of unity. The roots of $f(x)$ in K are $\alpha\zeta^i$ for $i \in \{0, 1, \ldots, n-1\}$. Thus K is the splitting field for $f(x)$ over F, so K/F is Galois. For each $\phi \in \mathrm{Gal}(K/F)$, there exists a unique $0 \leq i \leq n-1$ such that $\phi(\alpha) = \alpha\zeta^i$. Write $i = \Gamma(\phi)$, and it is straightforward to verify that $\Gamma : \mathrm{Gal}(K/F) \to \mathbb{Z}_n$ is an injective homomorphis. Thus $\mathrm{Gal}(K/F)$ is isomorphic to a cyclic subgroup of Z_n, and thus cyclic. □

TODO: finish all the proofs in this section.

Definition. We say $\{\sigma_1, \ldots, \sigma_n\} \subseteq \mathrm{Aut}\, K$ is *linearly dependent* over K if there exists $a_i \in L$, not all zero, such that $a_1\sigma_1(\alpha) + \cdots + a_n\sigma_n(\alpha) = 0$ for all $\alpha \in K$. Otherwise, we say $\{\sigma_1, \ldots, \sigma_n\}$ is *linearly independent*.

12.4 Lemma. *Let $[K : F] < \infty$. Then any finite subset of $\mathrm{Gal}(K/F)$ is linearly independent over K.*

Proof. Suppose not; it suffices to prove the result for $\mathrm{Gal}(K/F)$. Let $\{\sigma_1, \ldots, \sigma_r\}$ be a minimal linearly dependent subset of $\mathrm{Gal}(K/F)$ and let

$$a_1\sigma_1 + \cdots + a_r\sigma_r = 0$$

be a non-trivial dependence relation; note that each $a_i \in K^\times$ by minimality. Certainly, $r > 1$.

Let $\beta \in K$ be such that $\sigma_1(\beta) \neq \sigma_2(\beta)$. We then have for any $\alpha \in K$ that

$$a_1\sigma_1(\alpha)\sigma_1(\beta) + a_2\sigma_2(\alpha)\sigma_2(\beta) + \cdots + a_r\sigma_r(\alpha)\sigma_r(\beta) = 0 \tag{12.1}$$
$$a_1\sigma_1(\alpha)\sigma_1(\beta) + a_2\sigma_2(\alpha)\sigma_1(\beta) + \cdots + a_r\sigma_r(\alpha)\sigma_1(\beta) = 0 \tag{12.2}$$

where (12.1) follows since $\sigma_i(\alpha\beta) = \sigma_i(\alpha)\sigma_i(\beta)$. Subtracting (12.1) and (12.2), we get

$$a_2\sigma_2(\alpha)[\sigma_2(\beta) - \sigma_1(\beta)] + \cdots + a_r\sigma_r(\alpha)[\sigma_r(\beta) - \sigma_1(\beta)] = 0$$

which is a dependence relation on $\{\sigma_2, \ldots, \sigma_r\}$, contradicting minimality. □

We now provide a converse to Proposition 12.3. TODO: maybe merge the theorems?

12.5 Proposition. *Let F be a field which contains a primitive n^{th} root of unity. If K/F is cyclic with $[K : F] = n$, then K/F is simple radical.*

Proof. Suppose $\zeta \in F$ is a primitive n^{th} root of unity and K/F is cyclic of degree n. Let $G = \operatorname{Gal}(K/F) = \langle\sigma\rangle$, $|G| = n$ for some $\sigma \in G$. For $\alpha \in K$, define

$$g(\alpha) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha)$$

Note that $\zeta\sigma(g(\alpha)) = g(\alpha)$ so that $\sigma(g(\alpha)) = \zeta^{-1}g(\alpha)$. In particular,

$$\sigma(g(\alpha)^n) = \sigma(g(\alpha))^n = \left(\zeta^{-1}g(\alpha)\right)^n = g(\alpha)^n$$

Thus for all $\alpha \in K$, since $G = \langle\sigma\rangle$, $g(\alpha)^n \in \operatorname{Fix} G = F$. Moreover, since G is linearly independent over K, there exists $\alpha \in K$ such that $g(\alpha) \neq 0$. Furthermore, $\sigma^i(g(\alpha)) = \zeta^{-i}g(\alpha) \neq g(\alpha)$ for any $1 \leq i \leq n-1$; thus $g(\alpha) \notin \operatorname{Fix} H$ for any $\{1\} \neq H \leq G$. Thus by the fundamental theorem of galois theory (Theorem 10.3), $g(\alpha) \notin E$ for any $F \subseteq E \subsetneq K$, so $F(g(\alpha)) = K$. □

12.6 Proposition. *Let $K/E/F$, E/F Galois, K/E radical. Then there exists L/K such that L/F is Galois and L/E is radical such that* $\operatorname{Gal}(L/E)$ *is solvable.*

Proof. We prove the result when K/E is simple radical; the more general case follows by induction. Suppose $K = E(\alpha)$ where $\alpha^n = \beta \in E$. Also suppose $G = \operatorname{Gal}(E/F) = \{\sigma_1, \ldots, \sigma_r\}$. Consider

$$f(x) = \Phi_n \prod_{i=1}^{r}(x^n - \sigma_i(\beta)) \in (\operatorname{Fix} G)[x] = F[x]$$

and let L be the splitting field for $f(x)$ over K; let's show that L has the desired properties.

- L/F is Galois. First note that L is the splitting field for $f(x)$ over E. Since E/F is Galois, E is the splitting field of some separable polynomial $h(x) \in F[x]$. Then L is the splitting field for $h(x)f(x)$, and since $\operatorname{char} F = 0$ so that F is perfect, L/F is Galois.

- L/E is radical. Let ζ be a root of $\Phi_n(x)$ in L. We extend each $\sigma_i \in G$ to a $\sigma_i^* \in \operatorname{Gal}(L/F)$. Thus, the roots of $f(x)$ are of the form $\zeta^i\sigma_i^*(\alpha)$, so

  $$L = E(\zeta, \sigma_1^*(\alpha), \ldots, \sigma_r^*(\alpha)).$$

  Let $E_0 = E(\zeta)$ and for $1 \leq i \leq r$, $E_i = E(\zeta, \sigma_1^*(\alpha), \ldots, \sigma_i^*(\alpha))$ so $E_r = L$. Note that $\zeta^n = 1 \in E$ and $\sigma_i^*(\alpha)^n = \sigma_i^*(\alpha^n) = \sigma_i^*(\beta) = \sigma_i(\beta) \in E$. Thus,

  $$E \subseteq E_0 \subseteq E_1 \subseteq \cdots \subseteq E_r = L$$

  is a radical tower, so that L/E is radical.

- $\mathrm{Gal}(L/E)$ is solvable. Let $G_i = \mathrm{Gal}(L/E_i)$, so by the fundamental theorem of galois theory,
$$\{1\} = G_r \leq G_{r-1} \leq \cdots \leq G_2 \leq G_1 \leq G_0 \leq G'$$
where $G_0 = \mathrm{Gal}(L/E(\zeta))$. Moreover, $G_0 \leq G' := \mathrm{Gal}(L/E)$. First,
$$G_0 = \mathrm{Gal}(L/E(\zeta)) \trianglelefteq \mathrm{Gal}(L/E)$$
since $E(\zeta)/E$ is Galois (splitting field of $\Phi_n(x)$ over E). Furthermore, $G'/G_0 \cong \mathrm{Gal}(E(\zeta)/E)$ is abelian in the same way that $\mathbb{Q}(\zeta)/\mathbb{Q}$ is abelian.

  Now, $\mathrm{Gal}(L/E_{i+1}) \trianglelefteq \mathrm{Gal}(L/E_i)$ since E_{i+1}/E_i is Galois (E_{i+1}/E_i is simple radical with $\zeta \in E_i$ and $\sigma^*_{i+1}(\alpha)^n \in E_i$. By the proposition, E_{i+1}/E_i is cyclc. Also, $G_i/G_{i+1} \cong \mathrm{Gal}(E_{i+1}/E_i)$ is cyclic (correspondence between simple radical and cyclic). ☐

12.7 Corollary. *Take $E = F$. If K/F is radical, then there exists L/K such that L/F is radical and Galois with $\mathrm{Gal}(L/F)$ is solvable.*

12.8 Theorem (Galois). *Let $f(x) \in F[x]$. Then $f(x)$ is solvable over F if and only if $\mathrm{Gal}\, f(x)$ is solvable.*

Proof. ($\Longrightarrow$) Reading

($\Longleftarrow$) Suppose $f(x)$ is solvable by radicals over F. Say $f(x) = p_1(x)^{i_1} \cdots p_l(x)^{i_l}$ where the p_i are distinct and irreducible. By replacing $f(x)$ with $p_1(x) \cdots p_l(x)$, we may assume $f(x)$ is separable. Let E be the splitting field of $f(x)$ over F. Then E/F is Galois. Moreover, $E \subseteq K$, K/F is radical. Then by the proposition, there exists L/K such that L/F is Galois and radical. Since E/F is Galois, $\mathrm{Gal}(L/E) \trianglelefteq \mathrm{Gal}(L/F$. Thsn $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(L/F)/\mathrm{Gal}(L/E)$. ☐

Example. If $1 \leq \deg(x) < 5$, then $f(x)$ is solvable by raicals. Let $g(x)$ be the product of distinct factors of $f(x)$. Then $\mathrm{Gal}(g(x)) \leq S_4$ since $g(x)$ is separable, and S_4 is solvable.

Remark. Note that $S_n = \langle (12), (123 \cdots n) \rangle$. If p is prime, then $S_p = \langle \tau, \sigma \rangle$ where τ is any transposition and σ is any $p-$cycle.

12.9 Lemma. *Let $f(x) \in \mathbb{Q}[x]$ be irreducible with prime degree p. If $f(x)$ has exactly 2 non-real roots, then $\mathrm{Gal}\, f(x) = S_p$.*

Proof. Let α be a root of $f(x)$, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f(x) = p$. Thus $p \div [K : \mathbb{Q}]$ where k is the splitting field of $f(x)$ over $\mathbb{Q}$. Thus there exists $\sigma \in \mathrm{Gal}\, f(x)$, $|\sigma| = p$. Without loss of generality, $\sigma = (123 \cdots p)$. Moreover, $\phi : \mathbb{C} \to \mathbb{C}$ by $\phi(z) = \overline{z}$ is a $\mathbb{Q}-$map. By the normality theorem, $\phi|_K \in \mathrm{Gal}\, f(x)$. Since $f(x)$ has only 2 non-real roots, $\phi|_K = (ij)$. Thus $\mathrm{Gal}\, f(x) = S_p$. ☐

Example. Consider $f(x) = x^5 + 2x^3 - 24x - 2$, irreducible by Eisenstein. By IVT, $f(x)$ has at least 3 real roots. Computing the sum of squares of roots as $\sum \alpha_i^2 = \left(\sum \alpha_i\right)^2 - 2\sum_{i<j} \alpha_i \alpha_j = -4$, one sees that not all rots of $f(x)$ are real. Since non-real roots of $f(x)$ appear in conjugate pairs, $f(x)$ has exactly 2 non-real roots. By the lemma, $\mathrm{Gal}\, f(x) = S_5$, S_5 is not solvable, so $f(x)$ is not solvable by radicals.