Lecture Notes for Math 627B
Modern Algebra
Groups, Fields, and Galois Theory

Michael E. O'Sullivan
mosulliv@math.sdsu.edu
www-rohan.sdsu.edu/ ~ mosulliv

January 23, 2016

1 Groups, Subgroups, and Homomorphisms

Definition 1.1. A **binary operation** on a set S is a function from $S \times S$ to S. Similarly, a **unary operation** is a function $S \longrightarrow S$ and a **ternary operation** is a function $S \times S \times S \longrightarrow S$. An "operation" on S is usually assumed to be binary if not state otherwise.

Definition 1.2. A **group** is a set G with a binary operation $*$ satisfying the following properties.

(1) Associativity of $*$: for all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

(2) Identity for $*$: There is an element, usually denoted e, such that $e * a = a = a * e$ for all $a \in G$.

(3) Inverses for $*$: For each $a \in G$ there is an element, usually denoted a^{-1}, such that $a * a^{-1} = e = a^{-1}a$.

A group which also satisfies $a * b = b * a$ is called commutative or abelian (after the mathematician Abel).

The most basic properties are contained in the following proposition. The proofs of all of these are simple "card tricks." It's worthwhile reviewing them, but I leave them as exercises (see any text book).

Proposition 1.3. *Let $G, *$ be a group. Then*

(1) The identity element is unique.

(2) The inverse of any element is unique.

(3) The cancellation law holds: $a * b = a * c$ implies $b = c$ (and similarly for cancellation on the right).

(4) If $a * g = g$ for some $g \in G$, then $a = e_G$.

(5) $(a * b)^{-1} = b^{-1} * a^{-1}$.

(6) $(a^{-1})^{-1} = a$.

When there is risk of confusion we will use $*_G$ for the operation on the group G and e_G for the identity element.

Definition 1.4. A nonempty subset H of a group G is a **subgroup**, when H is a group using the operation $*_G$ on G.

If H is a subgroup of G then it must have an identity element. Let's call it e_H. For any $h \in H$, $e_h *_G h = h$ (using that $*_H = *_G$). Proposition 1.3 (4) shows that it must be the case that $e_H = e_G$, since $h \in G$. Let $h \in H$ and let h^{-1} be its inverse in G. This h^{-1} is also the inverse of h in the subgroup H because $h * h^{-1} = e_G = e_H$. (Thank goodness for both of these facts.)

Proposition 1.5. *If H is a nonempty subset of G that is closed under inversion and closed under $*_G$ then H is a subgroup of G (i.e. it also contains e_G).*

If H is a nonempty subset of G such that $h' *_G h^{-1} \in H$ for all $h, h' \in H$ then H is a subgroup of G.

Proof. Since H is nonempty, it contains some element h. Since H is closed under inversion, $h^{-1} \in H$. Since H is closed under $*_G$, $h *_G h^{-1} = e_G \in H$. Thus we have associativity (immediate since $*_H$ is the restriction of $*_G$), an identity element, and inverses (by assumption).

Suppose H is a nonempty subset of G such that $h' *_G h^{-1} \in H$ for all $h, h' \in H$. For any $h \in H$, let $h' = h$ in the assumed property. We get $h *_G h^{-1} = e_G \in H$. Letting $h' = e_G$ gives $e_G * h^{-1} = h^{-1} \in H$, so H is closed under inversion. Now for any $h', h \in H$ we know $h^{-1} \in H$, so $h' *_G (h^{-1})^{-1} = h' *_G h \in H$. This shows H is closed under multiplication. □

Exercises 1.6.

(a) Let G be a group. Show that the set $Z(G) = \{a \in G : ag = ga \text{ for all} g \in G\}$ is an abelian subgroup of G. It is called the **center** of G.

(b) Let H and K be subgroups of G. Show that their intersection is also a subgroup of G.

Definition 1.7. For groups G, H a function $\varphi : G \longrightarrow H$ is a homomorphism iff

(1) $\varphi(g_1 *_G g_2) = \varphi(g_1) *_H \varphi(g_2)$ for all $g_1, g_2 \in G$, and

(2) $\varphi(e_G) = e_H$, and

(3) $\varphi(g^{-1}) = (\varphi(g))^{-1}$ for all $g \in G$.

A homomorphism φ that is also a bijection (one-to-one and onto) is called an **isomorphism**.

I like to speak informally about a homomorphism as a function that **respects structure**: A homomorphism of groups "respects" the property of the identity element, multiplication, and inversion.

It is fairly easy to show that the first item in the definition of homomorphism implies the other two. This result and two others are contained in the following proposition. Proofs are a worthwhile exercise.

Proposition 1.8 (Homomorphisms)**.** *Let G, H, K be groups.*

If $\varphi : G \longrightarrow H$ is a function such that $\varphi(g_1 *_G g_2) = \varphi(g_1) *_H \varphi(g_2)$ then φ is a group homomorphism.

If $\varphi : G \longrightarrow H$ and $\theta : H \longrightarrow K$ are group homomorphisms then the composition $\theta \circ \varphi$ is also a group homomorphism.

When there exists an isomorphism $\varphi : G \longrightarrow H$ we say G and H are isomorphic and write $G \cong H$. The following proposition shows that being isomorphic satisfies symmetry, and transitivity so determines an equivalence relation.

Proposition 1.9. *If φ is an isomorphism of groups, then the inverse function φ^{-1} is also an isomorphism of groups.*

If $\varphi : G \longrightarrow H$ and $\theta : H \longrightarrow K$ are group isomomorphisms then the composition $\theta \circ \varphi$ is also a group isomorphism.

On any set of groups $\mathcal{G}$, the relation of being isomorphic is an equivalence relation.

Proof. □

If there is an isomorphism between groups G and H then G and H have the same algebraic structure, so we consider them equivalent.

Example 1.10. The integers, $\mathbb{Z}$, the rational numbers, $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ are all abelian groups under addition. We sometimes write $\mathbb{Z}, +$ (for example) to emphasize that we are are ignoring multiplication, and are just considering the additive properties of $\mathbb{Z}$.

Example 1.11. The set of integers modulo n forms a group under addition. This group is called the **cyclic group of order** n and written $\mathbb{Z}_n, +$ or sometimes C_n (I will just use $\mathbb{Z}_n$).

Problems 1.12.

(1) Show that for each $a \in \mathbb{Z}_n$ there is a unique homomorphism $\varphi_a : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ such that $\varphi_a(1) = a$.

(2) Under what conditions on a is φ_a an isomorphism?

(3) Identify all subgroups of $\mathbb{Z}_n$.

Example 1.13. The **dihedral group** of order $2n$ is the group of symmetries of a regular n-gon. Some sources, including Hungerford, write this group as D_n. The group has $2n$ elements: the identity, $n-1$ non-trivial rotations, and n reflections. Consequently, some authors, including Ash, write this group as D_{2n}. I will use D_n.

Problems 1.14.

(1) Check that the function $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ such that $\varphi(a) = -a$ is an isomorphism from $\mathbb{Z}$ to $\mathbb{Z}$.

(2) Identify all homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$.

(3) Show that there is an injective homomorphism from $\mathbb{Z}_n$ into D_n taking 1 to rotation by $2\pi/n$.

(4) Identify all subgroups of D_n for $n = 3, 4, 5, 6$. Draw a diagram showing containment of subgroups (I'll explain in class).

Example 1.15. Let S be any set. Let's show that the set $\mathrm{Bij}(S)$ of bijections from S to itself forms a group using composition of functions as the operation. First, the composition of two bijections is also a bijection, so composition is indeed an operation on $\mathrm{Bij}(S)$. Composition of functions (when defined) is associative (think about that!). The identity map id_S is the identity element of $\mathrm{Bij}(S)$. If $\varphi : S \longrightarrow S$ is a bijection, there is an inverse function to φ, written φ^{-1}, and $\varphi^{-1} \circ \varphi = \mathrm{id}_S$.

The most important special case is the **symmetric group on n elements**, written S_n, which is the set of bijections on $\{1, \ldots, n\}$. Section **??** is devoted to symmetric groups and their subgroups.

The following result has a straightforward proof, but is worth doing carefully: Think of $\mathrm{Aut}(G)$ as a subgroup of $\mathrm{Bij}(G)$, the group of bijections of the set G.

Proposition 1.16. *Let G be a group, show that the set of all isomorphisms from G to itself is a group. This new group is called* $\mathrm{Aut}(G)$*, the group of* **automorphisms** *of G.*

Problems 1.17.

(1) Show that $\mathrm{Aut}(\mathbb{Z})$ has two elements and $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

(2) Compute $\mathrm{Aut}(\mathbb{Z}_n)$ for $n = 2, 3, 4, 5, 6$. [In each case the answer is a cyclic group.]

Notation 1.18. Let G be a group. Unless there is some reason to be very clear (as there is in the next example), we rarely write the group operation: $g_1 g_2$ means $g_1 *_G g_2$. For a positive integer n, g^n is shorthand for $\underbrace{gg \cdots g}_{n \text{ factors}}$ and g^{-n} is shorthand for $\underbrace{g^{-1} g^{-1} \cdots g^{-1}}_{n \text{ factors}}$. It is straightforward to check that the usual rules for exponents apply.

For an additive group, $\underbrace{g + g + \cdots + g}_{n \text{ terms}}$ is written ng. Think of this as repeated addition, not as multiplication: the group just has one operation, and n is an integer, not necessarily an element of the group.

Example 1.19. Let G and H be groups. The Cartesian product of the sets G and H, $G \times H$, can be made into a group by using componentwise inversion and multiplication.

$$(g,h)^{-1} = (g^{-1}, h^{-1})$$
$$(g_1,h_1) *_{G\times H} (g_2,h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

The identity element is of course (e_G, e_H).

Proposition 1.20 (Direct Product)**.** *Let G and H be groups.*

(1) The above definition does, indeed, make $G \times H$ a group.

(2) The associative law holds: $G_1 \times (G_2 \times G_3) \cong (G_1 \times G_2) \times G_3$.

(3) G timesH is abelian iff A and B are abelian.

(4) If G' is a subgroup of G and H' is a subgroup of H then $G' \times H'$ is a subgroup of $G \times H$. In particular $G \times \{e_H\}$ and $\{e_G\} \times H$ are subgroups of $G \times H$.

(5) The projection maps $G \times H \longrightarrow G$ and $G \times H \longrightarrow H$ are surjective homomorphisms. There is also an obvious injective homomorphism $G \longrightarrow G \times H$ taking g to (g, e_H) (and similarly for H).

(6) The construction and the observations above can be generalized to the direct product of any set of groups $\{G_i : i \in I\}$ indexed by some set I. (Well, there is a subtle issue when I is infinite.)

Proof. A straightford but worthwhile exercise. □

Proposition 1.21 (Universal Property of the Product)**.** *Let G, H, K be groups, and let $\varphi : G \longrightarrow H$ and $\psi : G \longrightarrow K$ be homomorphisms. The function $\alpha : G \longrightarrow H \times K$ defined by $g \longmapsto (\varphi(g), \psi(g))$ is a homomorphism.*

Problems 1.22.

(1) Not all subgroups of $G \times H$ are direct products of subgroups of G and H. Illustrate with some examples: $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_4$.

Definition 1.23. The **order** of a finite group G—written $|G|$ or $\#G$—is the number of elements of G.

For $g \in G$ the **order of the element** g is the smallest positive integer n such that $g^n = e$, if such an n exists. If no such n exists then g has infinite order. We use $|g|$ or $\text{ord}(g)$ for the order of g.

The **exponent** of G is the least common multiple of the orders of the elements of G, if such an integer exists. We write $\exp(G) = \text{lcm}\,\{\text{ord}(g) : g \in G\}$.

Only the identity element of a group has order 1. Every nonzero element of $\mathbb{Z}$ has infinite order. In $\mathbb{Z}_n$ some elements have order n, but other non-identity elements may have a different order. For any finite group there is a well defined exponent, but an infinite group may not have one.

Theorem 1.24 (Order Theorem: A. 1.1.5, H 7.8)**.** *Let g be an element of the group G.*

(1) If g has infinite order then elements g^t for $t \in \mathbb{Z}$ are all distinct. The function below is an injective homomorphism.

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow G \\ t &\longmapsto g^t \end{aligned}$$

(2) If g has order n then

(a) $g^i = g^j$ iff $i \equiv j \mod n$;

(b) $\text{ord}(g^r) = \frac{n}{\gcd(r,n)}$.

(c) The function below is an injective homomorphism.

$$\begin{aligned} \varphi : \mathbb{Z}_n &\longrightarrow G \\ t &\longmapsto g^t \end{aligned}$$

Proof. See Hungerford. □

If $g \in G$ has order n then the set of powers of g is $\left\{g^0 = e_G, g, g^2, \ldots, g^{n-1}\right\}$ (any other power of g is one of these). This set is a subgroup of G of order n. It is called the cyclic subgroup generated by g and is written $\langle g \rangle$.

Problems 1.25.

(1) If $g \in G$ has order m and $h \in H$ has order n, find the order of $(g, h) \in G \times H$.

(2) Suppose that $a, b \in G$ commute (that is $ab = ba$). If $\text{ord}(a)$ and $\text{ord}(b)$ are coprime find the order of ab.

(3) Let A be an abelian group. Show that there is some $a \in A$ such that $\text{ord}(a) = \exp(A)$.

Problems 1.26.

(1) If $\varphi : G \longrightarrow H$ is a homomorphism, then $\text{ord}(\varphi(g))$ divides $\text{ord}(g)$.

(2) If $\varphi : G \longrightarrow H$ is an isomorphism, then $\text{ord}(\varphi(g)) = \text{ord}(g)$.

The previous exercises give important restrictions on homomorphisms. If you want to create a homomorphism from G to H, each element g in G must go to an element of H that has order dividing $\text{ord}(g)$.

Problems 1.27.

(1) Show that there is a nontrivial homomorphism from D_3 to $\mathbb{Z}_2$ but that any homomorphism from D_3 to $\mathbb{Z}_3$ is trivial.

The next proposition is a key result about the relationship between homomorphims and subgroups. Recall that for an arbitrary function $f : X \longrightarrow Y$, we define $f(X') = \{f(x) : x \in X'\}$. In general, f^{-1} may not be a function, but for a subset Y' of Y we define $f^{-1}(Y)$ to be $\{x \in X : f(x) \in Y'\}$.

Proposition 1.28. *Let $\varphi : G \longrightarrow H$ be a homomorphism.*

- *If G' is a subgroup of G then $\varphi(G')$ is a subgroup of H.*
- *If H' is a subgroup of H then $\varphi^{-1}(H')$ is a subgroup of G.*

Proof. A valuable exercise! □

Definition 1.29. Let $\varphi : G \longrightarrow H$ be a homomorphism. The **kernel** of φ is $\{g \in G : \varphi(g) = e_H\}$. Since e_H is a subgroup of H, $\ker(\varphi)$ is a subgroup of G by the previous proposition.

Proposition 1.30. *Let $\varphi : G \longrightarrow H$ be a homomorphism of groups. The kernel of φ is trivial (just $\{e_G\}$) iff φ is injective.*

Proof. Suppose φ is injective. By definition $\varphi(e_G) = e_H$, and since only one element of G has image e_H, $\ker(\varphi) = \{e_G\}$.

Conversely, assume $\ker(\varphi) = \{e_G\}$. Suppose that $\varphi(g) = \varphi(a)$. Then

$$e_H = \varphi(g) * \varphi(a)^{-1} = \varphi(ga^{-1})$$

using the properties of homomorphisms. By assumption $ga^{-1} = e_G$, so $g = a$. This shows φ is injective. □

An *injective* homomorphism $\varphi : G \longrightarrow H$ gives a bijection from G to $\varphi(G)$, which by proposition 1.28 is a subgroup of H. Thus $\varphi : G \longrightarrow \varphi(G)$ is an isomorphism. We will often call an injective homomorphism an **embedding** since the image is a "copy" of G inside of H.

Proposition 1.31. *Let $H_1, \ldots, H_t$ be subgroups of G. The intersection $\bigcap_{i=1}^{t} H_i$ is a subgroup of G.*

More generally if $\mathcal{H}$ is a set of subgroups of G then $\bigcap_{H \in \mathcal{H}} H$ is a subgroup of G.

Proof. Suppose h and h' are in $\bigcap_{H \in \mathcal{H}} H$. Since each $H \in \mathcal{H}$ is a subgroup of G, $h'h^{-1} \in H$ for each $H \in \mathcal{H}$. Thus $h'h^{-1} \in \bigcap_{H \in \mathcal{H}} H$, and Proposition 1.5 shows $\bigcap_{H \in \mathcal{H}} H$ is a subgroup of G. □

Let S be an arbitrary subset of a group G. Let $\mathcal{H}$ be the set of all subgroups of G containing S. Then $\bigcap_{H \in \mathcal{H}} H$ is a group of G, and it contains S, since each $H \in \mathcal{H}$ contains S. Furthermore, any subgroup K of G containing S is in $\mathcal{H}$ so $\bigcap_{H \in \mathcal{H}} H \subseteq K$. This argument justifies the following definition.

Definition 1.32. Let G be a group and let S be a subset of G. By $\langle S \rangle$ we mean the smallest subgroup of G containing S. It is the intersection of all subgroups of G containing S.

If H and K are subgroups of G their **join**, written $H \vee K$, is $\langle H \cup K \rangle$.

We are often interested in finding a minimal size set that generates a group. For example, the elements 1 and -1 both generate $\mathbb{Z}$. The element 1 generates $\mathbb{Z}_n$ as does any $a \in \mathbb{Z}_n$ that is coprime to n.

If a group G is generated by a single element, say $a \in G$, then $G = \{a^i : i \in \mathbb{Z}\}$ so G is equal to the cyclic subgroup generated by a. We call G a cyclic group. It is isomorphic to $\mathbb{Z}$ if a has infinite order, or to $\mathbb{Z}_n$ if a has order n. So, cyclic groups are not that complicated.

Groups generated by two elements can be quite complicated. We will see that D_n and S_n are each generated by two elements.

2 Permutation Groups

For n an integer, the **symmetric group** S_n is the set of all bijections on $\{1, \ldots, n\}$. These are also called permutations of $\{1, \ldots, n\}$. The number of elements in S_n is $n!$. Informally, we may justify this claim by noting that there are n possible images for the number 1. Once the image for 1 is chosen, there are $n - 1$ choices for the number 2. Continuing in this manner we count $n!$ bijections from $\{1, \ldots, n\}$ to itself. One can give a more formal inductive proof.

We will sometimes write an element π of S_n in tabular form with i in the top row and $\pi(i)$ in the bottom row.

Problems 2.1.

(1) Here are two elements of S_5:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} \quad \text{and} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}.$$

(2) Compute the inverse of each.

(3) Compute the products $\pi\sigma$ and $\sigma\pi$, using the usual convention for compositions: $(\pi\sigma)(i) = \pi(\sigma(i))$. You should see that the results are not equal.

Let $n = 3$, and enumerate the vertices of a triangle clockwise as 1, 2, 3. Each element of D_3 gives rise to a permutation of $\{1, 2, 3\}$.

Let r be rotation clockwise by $2\pi/3$. Then

$$r = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{and} \quad r^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

There are three reflections, each fixes one element of $\{1, 2, 3\}$ and transposes the other two

$$u_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad u_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad u_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

This exhausts all permutations of $\{1, 2, 3\}$ so by enumerating the vertices of the triangle we have established a bijection between D_3 and S_3. This is actually an isomorphism since the operation for D_3 is composition, as it is for S_n.

Problems 2.2.

(1) How many ways are there to embed $\mathbb{Z}_4$ in S_4?

(2) How many ways are there to embed D_4 in S_4?

definition

Definition 2.3. Let $a_1, a_2, \ldots, a_t$ be distinct elements of $\{1, \ldots, n\}$. We use the notation $(a_1, a_2, \ldots, a_t)$ to define an element of S_n called a t-**cycle**. This permutation takes a_i to a_{i+1}, for $i = 1, 2, 3 \ldots, t-1$ and it takes a_t to a_1. Every element of $\{1, \ldots, n\} \setminus \{a_1, \ldots, a_t\}$ is fixed (i.e. taken to itself) by the cycle $(a_1, a_2, \ldots, a_t)$. We will call the set $\{a_1, \ldots, a_t\}$ the **support** of the cycle $(a_1, a_2, \ldots, a_t)$.

A two-cycle is often called a **transposition**.

Two cycles are called **disjoint** when their supports are disjoint sets.

Problems 2.4.

(1) Suppose σ is a t-cycle. For which r is σ^r a t-cycle? What can happen for other r?

(2) A t-cycle has order t.

(3) The cycles $(a_1, \ldots, a_s)$ and $(b_1, b_2, \ldots, b_t)$ commute iff their support is disjoint.

Definition 2.5. Let $\pi \in S_n$. The **orbit** of $a \in \{1, \ldots, n\}$ under π is the set $\{\pi^i(a) : i \in \mathbb{Z}\}$.

Let $\pi \in S_n$. A **cycle decomposition** for π is a product of disjoint cycles that is equal to π.

Proposition 2.6. *Every permutation in S_n has a cycle decomposition, and it is unique up to reordering the factors.*

Proof. This is just a sketch that should make sense. One could formalize using induction. Take an element $a \in \{1, \ldots, n\}$. Notice that $\pi^i(a) = \pi^j(a)$ implies $\pi^{i-1}(a) = \pi^{j-1}(a)$ and so forth until $\pi^{i-j}(a) = a$. Since $\{1, \ldots, n\}$ is finite, there is some minimal positive integer such that $\pi^r(a) = a$. Let r be the minimum such positive integer. Now consider the cycle $(a, \pi(a), \ldots, \pi^{r-1}(a))$. The orbit of a is this list of elements, $\text{orb}(a) = \{a, \pi(a), \ldots, \pi^{r-1}(a)\}$. No element outside of this orbit can have an image in the orbit, for we already know the unique preimage of $\pi^i(a)$ is $\pi^{i-1}(a)$ (and the preimage of a is $\pi^{r-1}(a)$). Consequently, π can be written as the product of $(a, \pi(a), \ldots, \pi^{r-1}(a))$ and some other permutation that fixes each element in $\text{orb}(a)$. Now choose an element of $\{1, \ldots, n\} - \text{orb}(a)$ and look at its orbit; continue. □

Definition 2.7. We will call the list of cycle lengths, in decreasing order, the **signature** of the permutation.

We will include one-cycles in the definition of the cycle decomposition, although we will not write them unless it is needed for clarity.. For example, the permutation π in S_5 from Exercise 1 has cycle decomposition $\pi = (1, 3)(2, 5, 4)$ and signature $3, 2$. If we consider π as an element of S_6, we have $\pi = (1, 3)(2, 5, 4)(6)$ and the signature is $3, 2, 1$.

Problems 2.8.

(1) Use intelligent brute force to show that S_4 has no element with order equal to $\exp(S_4)$.

(2) For $\pi \in S_n$, the sum of the signature list is n.

(3) If $\pi = \sigma_1\sigma_2 \cdots \sigma_r$ is a cycle decomposition, then $\pi^k = \sigma_1^k\sigma_2^k \cdots \sigma_r^k$. Under what conditions is this also a cycle decomposition?

(4) The order of π is the lcm of the signature list.

(5) Identify all possible signatures for elements of S_5.

(6) For each signature, count how many elements have that signature. Check that you get the correct total number of elements in S_5.

There is a another factorization that is important.

Proposition 2.9. *Every permutation can be written as a product of transpositions.*

Proof. Since every permutation is a product of cycles, it is enough to show that every cycle is a product of transpositions. This is shown by verifying that

$$(a_1, a_2, \ldots, a_t) = (a_1, a_2) * (a_2, a_3) * \cdots * (a_{t-2}, a_{t-1}) * (a_{t-1}, a_t)$$

□

We may interpret the previous result as saying that S_n is generated by transpositions. That is somewhat good news: there are $n!$ elements of S_n but only $\binom{n}{2}$ transpositions. Thus $n(n-1)/2$ elements of S_n are enough to generate S_n. In fact we can do much better!

Problems 2.10.

(1) Show that S_n is generated by the $n-1$ elements $(1, k)$ for $k = 2, \ldots, n$. [Show that you can get an arbitrary transposition by conjugating $(1, k)$ by some $(1, j)$.]

(2) Show that S_n is generated by 2 elements: $(1, 2)$ and $(1, 2, 3, \ldots, n-1, n)$. [Show that you can get all $(1, k)$ from these two.]

We know from the previous proposition that a permutation can be written as a product of transpositions. This "factorization" is not unique, for example $\mathrm{id} = (1, 2)(2, 1) = (1, 3)(3, 1)$, but the next proposition shows that the parity of the factorization is.

Proposition 2.11. *The identity element of S_n cannot be written as the product of an odd number of transpositions.*

Consequently, any permutation can be written as a product of an even number of transpositions, or an odd number of transpositions, but not both.

Proof. I refer you to the standard texts for the proof of the first part of this result.

For the second part, suppose that π is the product of transpositions in two ways: $\pi = \sigma_1\sigma_2 \ldots \sigma_m = \theta_1\theta_2 \ldots \theta_k$. Then $\mathrm{id} = \sigma_1\sigma_2 \ldots \sigma_m\theta_1^{-1}\theta_2^{-1} \ldots \theta_k^{-1}$. Thus $m + k$ must be even, and this implies that m and k must have the same parity. □

We now have an important and easy consequence.

Theorem 2.12. *The set of even parity permutations forms a subgroup of S_n. This is called the* **alternating group** *and is denoted A_n.*

Problems 2.13.

(1) Show that there is a homomorphism from S_n to $\mathbb{Z}_2$ whose kernel is A_n.

(2) Find all subgroups of A_4. Draw a diagram of the subgroup lattice.

(3) What is the intersection of A_4 and D_4?

3 Cosets and Conjugates

The following bit of notation is useful.

Notation 3.1. Let S and T be subsets of a group G.

$$ST = \{st : s \in S, t \in T\}$$

We may use analogous notation for the set of all products from 3 or more sets. Similarly, $gS = \{gs : s \in S\}$.

Notice that ST and TS are not necessarily equal when the group G is not abelian.

It is sometimes useful to have notation that says that H is a subgroup of G.

Notation 3.2. Henceforth, $H \leq G$ means H is a subgroup of G and $H < G$ means H is a proper subgroup of G.

Definition 3.3. Let $H \leq G$ and let $g \in G$. Then gH is called a **left coset** of H in G. and Hg is called a **right coset** of H in G.

We will prove several results for left cosets. There are analogous results for right cosets.

Lemma 3.4. *The function*

$$\begin{aligned} \lambda_g : H &\longrightarrow gH \\ h &\longmapsto gh \end{aligned}$$

is a bijection.

Proof. It is a surjection by definition of gH. Suppose $gh = gh'$, multiplying on the left by g^{-1} gives $h = h'$, so λ_g is injective. □

Lemma 3.5. *If $gH \cap aH \neq \{\}$ then $gH = aH$.*

Proof. First we show that if $g \in aH$ then $gH \subseteq aH$. For $g \in aH$, we have $g = ak$ for some $k \in H$. Now for any $h \in H$, any $gh = akh \in aH$. This shows $gH \subseteq aH$.

Suppose $x \in gH \cap aH$. Then there are $h, k \in H$ such that $x = gh = ak$. Then $g = akh^{-1} \in aH$ and similarly $a = ghk^{-1} \in gH$. From the previous paragraph, we have $aH \subseteq gH$ and $gH \subseteq aH$, so $aH = gH$. □

Proposition 3.6. *For any $H \leq G$ the set of cosets of H partition H.*

Proof. Any $g \in G$ is in some coset, namely gH, so the cosets cover G. The previous lemma shows that any two unequal cosets are disjoint. Thus the cosets partition G. □

Proposition 3.7 (Lagrange)**.** *If G is a finite group with subgroup G then the order of H divides the order G. In particular the order of any element of G divides $|G|$.*

Proof. By the previous proposition the cosets of H partition G, say G is the disjoint union of $a_1H, a_2H, \ldots, a_tH$. The cosets of H all have the same number of elements by Lemma 3.4. Thus $|G| = \sum_{i=1}^{t} |a_iH| = t|H|$. Thus the number of elements of G is a multiple of $|H|$.

For any $a \in G$ the number of elements in the subgroup $\langle a \rangle$ is $\operatorname{ord} a$. So $\operatorname{ord} a$ divides $|G|$. □

Definition 3.8. Let $H \leq G$. The **index** of H in G, written $[G : H]$, is the number of cosets of H in G, which may be infinite.

If G is finite and $H \leq G$ then $[G : H] = |G|/|H|$, since all cosets have $|H|$ elements.

Now we consider conjugation.

Definition 3.9. Let $a \in G$ and $g \in G$. The element aga^{-1} is called the **conjugation of g by a**. If S is a subset of G, we define aSa^{-1} to be $\{asa^{-1} : s \in S\}$. It is the **conjugation of S by a**.

Problems 3.10.

(1) Show that A_n is invariant under conjugation: for any $\pi \in S_n$, $\pi A_n \pi^{-1} = A_n$. (Problem 3.13a)

(2) Let C_n be the rotation subgroup of D_n. Find two elements of C_4 that are conjugate as elements of D_4 but are not conjugate as elements of C_4.

(3) Find two elements of D_4 that are conjugate as elements of S_4 but are not conjugate as elements of D_4. You may use sage.

(4) Consider D_n as a subset of S_n by enumerating the vertices of an n-gon clockwise $1, 2, \ldots, n$. Show that the n-cycle $(1, 2, \ldots, n)$ and any reflection generate D_n.

Problems 3.11.

(1) Let $a \in G$. For H a subgroup of G show that aHa^{-1} is a subgroup of G.

(2) Show that aHa^{-1} has the same number of elements as H.

(3) Define a function $\varphi_a : G \longrightarrow G$ by $\varphi(g) = aga^{-1}$. Show that φ_a is an automorphism of G.

(4) Show that $\varphi : G \longrightarrow \mathrm{Aut}(G)$ defined by $\varphi : a \longmapsto \varphi_a$ is a homomorphism. The image, $\{\varphi_a : a \in G\}$, is therefore a subgroup of $\mathrm{Aut}(G)$. It is called $\mathrm{Inn}(G)$, the group of **inner automorphisms** of G.

(5) What is the kernel of φ?

Proposition 3.12. *Let $\pi \in S_n$. For any $\sigma \in S_n$, the signature of σ and the signature of $\pi\sigma\pi^{-1}$ are the same.*

One proof is contained in the following problem.

Problems 3.13.

(1) Consider first the case where σ is a t-cycle and π is a transposition. Show that $\pi\sigma\pi^{-1}$ is a t-cycle. [You will have to consider 3 cases based on $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\pi)$.]

(2) Extend to arbitrary π by noting that every permutation is the product of transpositions.

(3) Extend to arbitrary σ by writing σ as the product of disjoint cycles and using the fact that conjugation by π "respects products."

4 Problems

Problem 1: Subgroup lattice diagrams.

Problems 4.1.

(1) Draw the diagrams for $\mathbb{Z}_4 \times \mathbb{Z}_2$, the Quaternions, Q, and the Alternating Group A_4.

(2) Notice that the diagrams that we did in class and the ones you created establish that $\mathbb{Z}_8$, $\mathbb{Z}_2^3$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, D_4 and Q are pairwise nonisomorphic.

(3) Use sage to compute the dicyclic group of order 12. Find as many qualities of this group as you can to distinguish it from A_4 and from D_6.

5 Normality and the First Isomorphism Theorem

Let's pause for a moment to think about homomorphisms, particularly the special cases: injective homomorphisms (one-to-one) and surjective homomorphisms (onto).

Suppose H is a subgroup of G. There is a injective function from H to G, which is called the **inclusion map**, that simply takes $h \in H$ to itself, as an element of G. Since H is a subgroup of G (it's multiplication is the same as the one on G), the inclusion map is an injective homomorphism from H to G.

On the other hand, suppose that H and G are arbitrary groups and that $\varphi : H \longrightarrow G$ is an injective homomorpism. Proposition 1.28 shows that $\varphi(H)$ is a subgroup of G. Thus $\varphi : H \longrightarrow \varphi(H)$ is a bijective homomorphism. This shows that the image of an injective homomorphism $\varphi : H \longrightarrow G$ is a subgroup that is isomorphic to H. Thus, the study of injective homomorphisms is essentially the study of subgroups.

This section and the next are devoted to surjective homomorphisms, which are intimately related to subgroups that have a special property, treated in the next proposition.

Theorem 5.1 (Normal)**.** *Let N be a subgroup of G. The following are equivalent.*

(1) $Na = aN$ for all $a \in G$.

(2) $aNbN = abN$ for all $a, b \in G$.

(3) $aNa^{-1} \subseteq N$ for all $a \in G$.

(4) $aNa^{-1} = N$ for all $a \in G$.

Proof. (1) $\Longrightarrow$ (2): $aNbN = abNN = abN$.
(2) $\Longrightarrow$ (3): Set $b = a^{-1}$. Then $aNa^{-1}N = aa^{-1}N = eN$. In particular, this shows that $aNa^{-1} \subseteq N$. (3) $\Longrightarrow$ (4): For any $a \in G$, applying (3) to a^{-1}, we have that $a^{-1}Na \subseteq N$. Conjugating by a, we get

$$a(a^{-1}Na)a^{-1} \subseteq aNa^{-1}$$

The left hand side is N. Thus, assuming (3) we have both $aNa^{-1} \subseteq N$ and $N \subseteq aNa^{-1}$, which proves (4).
(4) $\Longrightarrow$ (1): Multiplying $aNa^{-1} = N$ on the right by a gives (1).

These arguments may seem slippery since they deal with computations with sets. The proofs can also be done elementwise. Consider (4) $\Longrightarrow$ (1), and let $a \in G$. Given any $n \in N$, we know $ana^{-1} \in N$, say $ana^{-1} = n'$. Then $an = n'a \in Na$, which shows $aN \subseteq Na$. The reverse containment is proven analogously, using a^{-1}. □

Definition 5.2. A group satisfying the conditions of the theorem is called **normal**.

Problems 5.3.

(1) Let H be a subgroup of a group G such that for any $a \in G$ there is a b in G such that $aH = Hb$. (Every left coset is also a right coset, but not necessarily defined by the same element of G.) Prove that H is normal in G.

Let N be normal in G. Suppose $aN = bN$ and $rN = sN$. Then $a \in bN$ and $r \in sN$, so $ar \in bNsN = bsN$. By the Coset Theorem, $arN = bsN$. Consequently, there is a well-defined operation on cosets of N in G that takes the pair (aN, bN) to abN. The next theorem shows that this gives a group structure on the cosets of N in G.

Theorem 5.4. *Let N be a normal subgroup of G. Let G/N be the set of cosets of N in G with the binary operation by $aN * bN = abN$. Then G/N is a group.*

Proof. Associativity is inherited from associativity of $*_G$ (check!). The identity is eN. The inverse of aN is $a^{-1}N$. □

We call G/N the **quotient** of G by N. Some sources call it G/N a **factor** group. The homomorphism $G \longrightarrow G/N$ is called the **quotient map**.

Problems 5.5.

(1) If $\varphi : G \longrightarrow H$ is a homomorphism and N is normal in H, then $\varphi^{-1}(N)$ is normal in G.

(2) The **center** of G is the set of elements in G that commute with all elements of G, $Z(G) = \{a \in G : ag = ga \text{ for all } g \in G\}$. The center of G and any subgroup of $Z(G)$ is normal in G.

(3) Find all normal subgroups of D_4 and D_5.

(4) Show that any subgroup of index 2 is normal.

Generalizing the last problem, here is a result from Lam [MAA Monthly Mar. 2004 p. 256].

Theorem 5.6. *Let H be a subgroup of G with $[G : H] = p$ a prime number. The following are equivalent.*

(1) H is normal in G.

(2) For any $a \in G - H$, $a^p \in H$.

(3) For any $a \in G - H$, $a^n \in H$ for some positive integer n that has no prime divisor less than p.

(4) For any $a \in G - H$, $a^2, a^3, \ldots, a^{p-1} \notin H$.

Problems 5.7.

(1) Prove Lam's theorem by showing (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) $\Longrightarrow$ (4) $\Longrightarrow$ (1). The last step is the one requiring some cleverness.

(2) Show that Lam's theorem implies that any group whose index is the smallest prime dividing $|G|$ is normal in G.

Theorem 5.8 (First Isomorphism)**.** *Let $\varphi : G \longrightarrow H$ be a surjective homomorphism with kernel N. Then G/N is isomorphic to H.*

Proof. If $g \in aN$, say $g = an$ then $\varphi(g) = \varphi(a)\varphi(n) = phi(a)$. Consequently, there is a well defined map $\tilde{\varphi} : G/N \to H$ taking aN to $\varphi(a)$. For any $h \in H$ there is some $a \in G$ such that $\varphi(a) = h$. Then $\tilde{\varphi}(aN) = h$, so $\tilde{phi}$ is surjective.

To show that $\tilde{\varphi}$ is injective, suppose $\tilde{\varphi}(aN) = e_H$. Then $\varphi(a) = e_G$ so $a \in N$ and $aN = e_G N$. Thus the kernel of $\tilde{\varphi}$ just contains the identity element of G/N. □

Here is a typical snappy use of the 1st isomorphism theorem.

Theorem 5.9. *Let $G_1, G_2, \ldots G_r$ be groups and let $N_1, N_2, \ldots, N_r$ be normal subgroups, $N_i \trianglelefteq G_i$. There is a well defined map*

$$\begin{aligned}(G_1 \times G_2 \times \cdots \times G_r)/(N_1 \times N_2 \times \cdots \times N_r) &\longrightarrow (G_1/N_1) \times (G_2/N_2) \times \cdots \times (G_r/N_r)\\ (g_1, g_2, \ldots, g_r)\, N_1 \times N_2 \times \cdots \times N_r &\longmapsto (g_1N_1, g_2N_2, \ldots g_rN_r)\end{aligned}$$

and it is an isomorphism.

Proof. By the Direct Product Theorem, the projection of $G_1 \times G_2 \times \cdots \times G_r$ onto G_i is easily verified to be a homomorphism. Composing this with the quotient map $G_i \longrightarrow G_i/N_i$, we get maps $G_1 \times G_2 \times \cdots \times G_r \longrightarrow G_i/N$. Proposition 1.21 then gives a homomorphism

$$G_1 \times G_2 \times \cdots \times G_r \xrightarrow{\varphi} (G_1/N_1) \times (G_2/N_2) \times \cdots \times (G_r/N_r),$$

To be specific, let $(g_1, g_2, \ldots, g_r)$ and $(g_1', g_2', \ldots, g_r')$ be elements of $G_1 \times G_2 \times \cdots \times G_r$. Then

$$\begin{aligned}\varphi\Big((g_1, g_2, \ldots, g_r) * (g_1', g_2', \ldots, g_r')\Big) &= \varphi\Big(\,(g_1g_1', g_2, g_2', \ldots, g_rg_r')\,\Big)\\ &= (g_1g_1'N_1, g_2g_2'N, \ldots, g_rg_r'N_r)\\ &= (g_1N_1, g_2N, \ldots, g_rN_r) * (g_1'N_1, g_2'N, \ldots, g_r'N_r)\end{aligned}$$

We used, in order, the definition of multiplication in $G_1 \times G_2 \times \cdots \times G_r$, the definition of φ, the definition of multiplication in $G_1/N_1 \times G_2/N/2 \times \cdots \times G_r/N_r$.

The kernel of φ is the set of $(g_1, \ldots, g_r)$ such that $g_1N_1, g_2N_2, \ldots, g_rN_r = N_1 \times N_2 \times \cdots \times N_r$. Each g_i must be in N_i. So, the kernel is $N_1 \times N_2 \times \cdots \times N_r$. The 1st isomorphism theorem now gives the result. □

A generalization of the first isomorphism theorem that we will often use treats the case when φ is not necessarily injective.

Theorem 5.10 (Factor)**.** *Let $\varphi : G \longrightarrow H$ be a homomorphism with kernel N. Then φ can be factored into the canonical surjective homomorphism $\pi : G \longrightarrow G/N$ followed by an injective homomorphism $\bar{\varphi} : G/N \longrightarrow H$.*

6 Structure in the Quotient Group: The Third Isomorphism Theorem and the Correspondence Theorem

The next step is to understand the structure of a quotient group. The two main results—the third isomorphism theorem and the correspondence theorem—have fairly simple statements, which obscure some subtle issues. The proof of the third isomorphism theorem is an easy consequence of the first isomorphism theorem.

Theorem 6.1 (Third Isomorphism)**.** *Let N and K be normal subgroups of G with $N \leq K$. Then $G/K \cong (G/N)\Big/(K/N)$.*

Proof. We have two well defined quotient groups: G/N and G/K. I claim that there is a well defined function from G/N to G/K taking gN to gK. To prove

this we have to check that if two cosets aN and bN are equal then the cosets aK and bK are also equal. Suppose $aN = bN$. Then $a^{-1}b \in N$ and since $N \subseteq K$ we have $a^{-1}b \in K$. Consequently $aK = bK$.

It is easy to check that the function $\varphi : G/N \longrightarrow G/K$ defined above is surjective and a homomorphism. Given any gK there is an element, namely gN, that clearly maps to it, $\varphi(gN) = gK$, so we get surjectivity. Finally, φ respects multiplication: $\varphi(gN * g'N) = \varphi(gg'N) = gg'K = gK * g'K = \varphi(gN) * \varphi(g'N)$

The kernel of φ is $\{gN : gK = eK\} = K/N$. Now the result follows from the first isomorphism theorem. □

The more powerful theorem is the correspondence theorem, which we prove independently of the 3rd Isomorphism Theorem.

Theorem 6.2 (Correspondence)**.** *Let $\varphi : G \longrightarrow H$ be a surjective homomorphism with kernel N. There is a one-to-one correspondence, given by φ, between subgroups of G/N and subgroups G containing N.*

$$\begin{aligned} G &\longrightarrow H \\ N \leq A &\longleftrightarrow \varphi(A) \\ \varphi^{-1}(B) &\longleftrightarrow B \end{aligned}$$

The correspondence respects containment, normality, and quotients. For A, A' containing N,

- *$N \leq A \leq A'$ iff $\varphi(A) \leq \varphi(A')$.*
- *A is normal in G iff $\varphi(A)$ is normal in H. In this case $G/A \cong H/\varphi(A)$*

Proof. Some of these results are simply based on facts about functions. Let $f : X \to Y$ and let $A \subseteq X$ and $B \subseteq Y$. Then $A \subseteq f^{-1}(f(A))$ and $f(f^{-1}(B)) \subseteq B$. On the other hand, if f is surjective then for each $b \in B$ there is some $x \in X$ such that $f(x) = b$. Thus for f surjective, $f(f^{-1}(B)) = B$. Respecting containment is also immediate: If $A \subseteq A' \subseteq X$ then $f(A) \subseteq f(A')$ and similarly if $B \subseteq B' \subseteq Y$ then $f^{-1}(B) \subseteq f^{-1}(B')$.

Let A be a subgroup of G containing N and let B be a subgroup of H. We already know that $\varphi(A)$ is a subgroup of H and $\varphi^{-1}(B)$ is a subgroup of G. Based on the above discussion, to show the one-to-one correspondence, we need to show that $\varphi^{-1}(\varphi(A)) \subseteq A$. Let $g \in \varphi^{-1}(\varphi(A))$. Then $\varphi(g) = \varphi(a)$ for some $a \in A$. Consequently, $\varphi(ga^{-1}) = e_H$ and therefore $ga^{-1} \in \ker(\varphi) = N$. Since $N \subseteq A$, $ga^{-1} \in A$ so $g \in A$. Thus $\varphi^{-1}(\varphi(A)) = A$. Thus, we have established the one-to-one correspondence.

We have also shown that if B is normal then $\varphi^{-1}(B)$ is normal. These results are true for an arbitrary homomorphism. Let's now show that when φ is surjective, if A is normal in G then $\varphi(A)$ is normal in H.

Let $h \in H$. We need to show $h\varphi(A)h^{-1} = \varphi(A)$, or equivalently, $h\varphi(a)h^{-1} \in \varphi(A)$ for all $a \in A$. Since φ is surjective, there is some $g \in G$ such that $\varphi(g) = h$.

$$h\varphi(a)h^{-1} = \varphi(g)\varphi(a)\varphi(g)^{-1} = \varphi(gag^{-1}) \in \varphi(A)$$

The last step holds because A is normal in G, so $gag^{-1} \in A$.

Now we apply the first isomorphism theorem. Let B be normal in H. We have a composition of surjective homomorphisms

$$G \longrightarrow H \longrightarrow H/B$$

whose kernel is $\varphi^{-1}(B)$. Letting $A = \varphi^{-1}(B)$, the first isomorphism theorem says that $G/A \cong H/\varphi(A)$. □

We can derive the 3rd isomorphism theorem as a corollary.

Corollary 6.3 (3rd isomorphism theorem)**.** *Let N and K be normal subgroups of G with $N \leq K$. Then $G/K \cong (G/N)\Big/(K/N)$.*

Proof. Apply the correspondence theorem to $G \longrightarrow G/N$. The subgroup K of G corresponds to the subgroup K/N of G/N. Thus $G/K \cong (G/N)\Big/(K/N)$. □

7 Interaction between Two Subgroups: The Second Isomorphism Theorem

We now consider two subgroups of a group G and prove several results about the interaction between them. At first we make no additional assumptions on the two groups, then we assume that one is normal, and finally that both are.

Lemma 7.1. *Let K, H be subgroups of G. The following are equivalent:*

(1) $G = KH$ and $K \cap H = \{e_G\}$

(2) Every element of G can be uniquely written as kh for $k \in K$ and $h \in H$.

Proof. $G = KH$ is equivalent to saying that every element of G can be written in the form kh.

We'll next show $K \cap H = \{e_G\}$ iff any expression for $g \in G$ as kh is unique. Suppose $K \cap H = \{e_G\}$ and $k_1h_1 = k_2h_2$. Then $k_1^{-1}k_2 = h_1h_2^{-1}$. Since this is in

both K and in H, it must be the identity. Therefore, $h_1 = h_2$ and $k_1 = k_2$, which proves uniqueness.

Now suppose that, $K \cap H \neq e_G$; say $g \in K \cap H$ is not equal to e_G. Setting $h = g$ and $k = e_G$ or $h = e_G$ and $h = g$ gives two different ways to express g in the form kh. Thus we have non-uniqueness. □

As a prelude to the second isomorphism theorem we have the following lemma.

Lemma 7.2 ([A] 1.3.6)**.** *Let H, K be subgroups of G.*

$$HK = KH \quad \iff HK \text{ is a subgroup of } G$$

Proof. Suppose $HK = KH$. Then HK is closed under inversion: $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$.
HK is also closed under multiplication: $HKHK = HHKK = HK$. This shows HK is a subgroup of G.

Suppose HK is a subgroup of G. Since HK is closed under inversion, $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. □

Suppose now that H, N are subgroups of G with N *normal in* G. We can conclude the following.

- $HN = NH$ since $gN = Ng$ for any $g \in G$.
- HN is therefore a subgroup of G by the lemma.
- N is normal in HN, since it is normal in any subgroup of G that contains it.

Theorem 7.3 (Second Isomorphism)**.** *Let N be normal in G and H a subgroup of G. Then $H \cap N$ is normal in H and $H/(H \cap N) \cong HN/N$.*

Proof. Consider $G \xrightarrow{\pi} G/N$ restricted to the subgroup H, call the homomorphism $\pi' : H \longrightarrow G/N$. The kernel is $H \cap N$. The image is $HN/N = \{hN : h \in H\}$. By the 1st isomorphism theorem, $H/(H \cap N) \cong HN/N$. □

The following special case is of interest.

Corollary 7.4. *Let $H \leq G$ and $N \trianglelefteq G$. If $G = HN$ and $H \cap N = \{e_G\}$ then $G/N \cong H$. In other words, there is an exact sequence*

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$$

Definition 7.5. In the situation of the corollary we say that G is the *internal semi-direct product* of N by H and we write $G \cong N \rtimes H$.

Note the order is important: $N \rtimes H$ and $H \rtimes N$ mean two different things. The first assumes N is normal in G and the second assumes H is normal in G. If both H and N are normal then the two semidirect products are isomorphic to each other and to the direct product, as the following corollary shows.

Corollary 7.6. *Suppose $K \trianglelefteq G$ and $N \trianglelefteq G$ and $G = KN$ and $K \cap N = \{e_G\}$. Then elements of K and N commute: for any $k \in K$ and $n \in N$, $kn = nk$. Furthermore, $G \cong K \times N$.*

Proof. It is sufficient to show that $knk^{-1}n^{-1} = e$. Since N is normal, $knk^{-1} \in N$ and therefore $knk^{-1}n^{-1} \in N$. Similarly, since K is normal, $nk^{-1}n^{-1} \in K$ so $knk^{-1}n^{-1} \in K$. Now $K \cap N = \{e\}$ gives the result.

Consider the map $K \times N \xrightarrow{\varphi} G$ defined by $(k, n) \longmapsto kn$. The map is well defined. It is injective since $kn = e$ gives $k = n^{-1} \in K \cap N = \{e\}$. It is surjective since $G = KN$. It respects multiplication (so is a homomorphism):

$$\begin{aligned} \varphi((k_1, n_1)(k_2, n_2)) &= \varphi((k_1k_2, n_1n_2)) \\ &= k_1k_2n_1n_2 = k_1n_1k_2n_2 \\ &= \varphi((k_1, n_1))\varphi((k_2, n_2)) \end{aligned}$$

Thus φ is an isomorphism. □

Definition 7.7. In the situation of the last corollary, G is often called the *internal direct product* of K and N.

The distinction between internal direct product and the usual (external) direct product of two arbitrary groups G and H is subtle. In $G \times H$, let $\overline{G} = G \times \{e_H\}$ and similarly for $\overline{H}$. Then $G \times H$ is the internal direct product of $\overline{G}$ and $\overline{H}$. On the other hand $\mathbb{Z}_6$ is the internal direct product of $\mathbb{Z}_2$ and $\mathbb{Z}_3$.

One can also define the external semi-direct product of of two groups.

8 Finitely Generated Abelian Groups

We will write the group operation additively. For A an abelian group, $a \in A$, and m an integer, $mA = a + \cdots + a$ with m summands. The order of a is the smallest positive integer m such that $ma = 0$. One can check that $ma + na = (m + n)a$ and $(mn)a = m(na)$.

Definition 8.1. Let p be a prime. A p-group is one in which all elements have order a power of p. For A an abelian group we define the p-group of A to be $A(p) = \big\{a \in A : \mathrm{ord}(a) = p^k \text{ for some } k\big\}$.

The fact that $A(p)$ is a group follows from the basic result that if a and b commute, then the order of $a+b$ divides $\mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b))$.

Lemma 8.2. *Let A be an abelian group and let p be a prime number. We may write the order of A as $n = p^k m$ with m not divisble by p. Let $A(p)$ be the p-group of A and let $B = \{a \in A : ma = 0\}$. Then $A \cong A(p) \times B$.*

Note that k may be 0, in which case $A(p) = \{0\}$, which is not interesting!

Proof. First of all we note that B is a group. The proof is similar to the observation we made for $A(p)$. For $b, b' \in B$, the order of $b + b'$ divides $\mathrm{lcm}(\mathrm{ord}(b), \mathrm{ord}(b'))$. This last expression is a factor of m since both $\mathrm{ord}(b)$ and $\mathrm{ord}(b')$ divide m. Thus $b + b' \in B$.

We will show that $A(p) \cap B = \{0\}$ and $A(p) + B = A$ and conclude, by Corollary 7.6, that $A \cong A(p) \times B$. An element of $A(p) \cap B$ has order that is a power of p and also divides m. Since p and m are coprime this element can only be the identity. Let a be an arbitrary element of A, and let its order be $p^s t$ with $t \mid m$. We have $p^s a \in B$ and $ta \in A(p)$ since $p^s a$ has order t and ta has order p^s. Since $p \nmid t$ there are integers x, y such that $1 = xp^s + yt$. Then $a = (xp^s + yt)a = x(p^s a) + y(ta)$ can be expressed as a sum of an elment in $A(p)$ and one in B. □

Theorem 8.3. *Let A be a finite abelian group. The A is isomorphic to the direct product of its p-groups. That is, if $|A| = p_1^{e_1} \dots p_r^{e_r}$ then $A \cong A(p_1) \times \cdots \times A(p_r)$.*

Proof. For the purposes of this proof, lets define the index of A to be the number of distinct primes for which there exists an element of A with that order. Notice that if $\mathrm{ord}(a) = qm$ then $\mathrm{ord}(ma) = q$ so if any element has order divisible by q then there is an element of order q. Consequently, if the index is 1, then every element of A has order a power of some prime p. Thus the base case is immediate: if the index is 1, then $A = A(p)$ for some prime p.

Assume that the statement of the theorem is true for all primes with index less than r, let A have index r, and let p be a prime for which $A(p)$ is nonempty. By the lemma $A \cong A(p) \times B$ where B is the subgroup of elements of A with order not divisible by p. The index of B is less than r, so the induction applies. Clearly, for any $q \neq p$, $B(q) = A(q)$. This gives the result. □

The previous theorem is the first step in the classification of finite abelian groups. The next step is to classify p-groups. The key lemma follows. Its proof is quite technical and not very illuminating, so we state it without proof (see Hungerford).

Lemma 8.4. *Let A be a p-group and let a be an element of maximal order. Then $A = \langle a \rangle + K$ for some subgroup K of A.*

Theorem 8.5. *Let A be a p-group. Then A is the direct product of cyclic groups each of which has order a power of p. Consequently, the order of A is also a power of p.*

The decomposition is unique (up to reordering). Put another way, two p-groups are isomorphic iff their decompositions have the same number of factors for each power of p.

Proof. The proof is by induction. Using the lemma we can write $A = \langle a \rangle + K$. The subgroup $\langle a \rangle$ is cyclic of order p^k for some k. Applying the induction hypothesis to K gives the result. Since A is the direct product of groups of order a power of p, A itself must have order a power of p.

Clearly, if two groups have the same number of factors for each power of p they are isomorphic. To prove the converse, consider the groups $p^i A$ and the quotients $p^i A / p^{i-1} A$. It can be shown that each of the quotients is a vector space over $\mathbb{F}_p$ (which is just $\mathbb{Z}_p$ considered as a field). The list of dimensions $\dim_{\mathbb{F}_p} p^{i-1} A / p^i A$ can be used to recover the number of $\mathbb{Z}_{p^i}$-factors for each i. □

From the two previous theorems we obtain the fundamental theorem.

Theorem 8.6 (Fundamental Theorem of Finite Abelian Groups)**.** *Let A be an abelian group of order $p_1^{e_1} \dots p_r^{e_r}$. Then A is a direct product of cyclic groups, each having order a power of one of the p_i. If we write*

$$A(p_i) \cong \mathbb{Z}_{p_i^{a_{i,1}}} \times \mathbb{Z}_{p_i^{a_{i,2}}} \times \dots \mathbb{Z}_{p_i^{a_{i,s_i}}}$$

then for each i, $\sum_{\ell=1}^{s_i} a_{i,\ell} = e_i$. The decomposition is unique, up to reordering.

Definition 8.7. The groups $\mathbb{Z}_{p^a}$ occurring in the decomposition are called the *elementary divisors* of A.

9 Rings and Homomorphisms

Definition 9.1. A **ring** is a set R, with two operations $+$ and $*$ satisfying the following properties.

(1) $+$ and $*$ are both associative. That is $(a+b)+c = a+(b+c)$ and $a*(b*c) = (a*b)*c$.

(2) $+$ and $*$ are both commutative. That is $a+b = b+a$ and $a*b = b*a$.

(3) $+$ and $*$ both have identity elements. There is some element in R, that we call 0, such that $a+0 = a$ and there is an element, that we call 1, such that $a*1 = a$.

(4) $+$ admits inverses. That is, for each $a \in R$ there is some other element, that we write $-a$, such that $a+(-a) = 0$.

(5) $*$ distributes over $+$. That is $a*(b+c) = a*b+a*c$.

A few comments are in order. Strictly speaking, the definition above is for a **commutative ring with identity**. The modifier "commutative" is referring to commutativity of multiplication, and "with identity" is referring to the multiplicative identity. There is a rich study of rings where multiplication is non-commutative (for example the ring of $n \times n$ matrices over $\mathbb{R}$), but we will rarely discuss them, so a ring for us is assumed to be commutative and have an identity.

A **commutative ring** is a ring in which multiplication is commutative.

One may also say that a ring R is an abelian group under $+$ and a *monoid* (look it up!) under $*$, with the additional property that $*$ distributes over $+$.

There are a bunch of little results one should verify: each identity is unique, the additive inverse of an element is unique, $-(a+b) = (-a)+(-b)$, etc. See §3.1-2 of [**?**].

Definition 9.2. An element u of a ring R is a **unit** when there is another element v such that $uv = vu = 1$. An element a of a ring R is a **zero divisor** when $a \neq 0$ and there is some $b \neq 0$ in R such that $ab = 0$ or $ba = 0$.

Exercises 9.3.

(a) Show that the identity for multiplication in a ring R is unique. If x satisfies $xa = ax = a$ for all $a \in R$ then $x = 1$.

(b) The inverse of a unit is unique.

(c) The inverse of a unit is also a unit.

(d) A unit cannot be a zero divisor.

Definition 9.4. Let R, S be rings. A funtion $\varphi : R \longrightarrow S$ is a *ring homomorphism* when

(1) $\varphi(1_R) = 1_S$,

(2) and for $r_1, r_2 \in R$,

$$\varphi(r_1 +_R r_2) = \varphi(r_1) +_S \varphi(r_2),$$
$$\varphi(r_1 *_R r_2) = \varphi(r_1) *_S \varphi(r_2)$$

Notice that the operations $+, *$ on the left-hand side are in R and the operations $+, *$ on the right-hand side are in S. When we want to be careful we specify the ring as we did here, but generally this is unnecessary. We say φ *respects addition, multiplication and the identity lement.* That is, it respects the ring structure. There are several little results to establish for homomorphisms: e.g. $\varphi(-r) = -\varphi(r)$. See [**?**, §3.3].

The following theorem shows that the Integers are the "original (or initial) ring."

Theorem 9.5 (The Initial Ring)**.** *For any ring R there is a unique homomorphism from $\mathbb{Z}$ to R.*

Proof. A homomorphism $\varphi : \mathbb{Z} \longrightarrow R$ would have to take $1_\mathbb{Z}$ to 1_R. Applying the fact that a homomorphism has to respect addition we see inductively that we must have for $m > 0$,

$$\varphi(m) = \varphi(\underbrace{1_\mathbb{Z} + \cdots + 1_\mathbb{Z}}_{m \text{ terms}}) = \underbrace{1_R + \cdots + 1_R}_{m \text{ terms}}$$

We also must have $\varphi(-m) = -\varphi(m)$. Thus, there is at most one way to define a homomorphism from $\mathbb{Z}$ to R. Next, check that this function is indeed a homomorphism by verifying that the other properties of homomorphisms hold. □

Definition 9.6. The **kernel** of a homomorphism $\varphi : R \longrightarrow S$ is the preimage of 0_S: that is $\{r \in R : \varphi(r) = 0_S\}$. A homomorphism that is also a bijection (injective and surjective) is called an **isomorphism**.

Since a ring homomorphism φ is also a homomorphism of additive groups, φ is injective iff the kernel is trivial (just 0_R).

10 Rings and Unit Groups

Proposition 10.1. *Let R be a ring (not necessarily commutative). The set $U(R)$ of units in R forms a group.*

Proof. The main thing we have to prove is that multiplication is an operation on $U(R)$. We need to show the product of two units is a unit. But this is clear. If $u, v \in U(R)$ then (uv) is also a unit, with inverse $v^{-1}u^{-1}$ since $v^{-1}u^{-1}uv = v^{-1}v = 1$ and $uvv^{-1}u^{-1} = uu^{-1} = 1$. By the definition of ring, multiplication is associative. So we have an operation that is associative, and has an identity element, 1. By the definition of $U(R)$, each element of $U(R)$ has an inverse, Exercises **??** shows that the inverse of a unit is also in $U(R)$. □

Definition 10.2. A **division ring** is a ring in which each nonzero element is a unit. A **field** is a commutative division ring.

Of particular interest are the following groups derived from rings.

- U_n the unit group of $\mathbb{Z}_n$.
- The set of nonzero elements of a field (or a division ring, more generally) is a group under multiplication. We denote it with a $*$, for example: $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$. For these fields we also have the subgroups consisting of the positive field elements, $\mathbb{Q}^{**}$ and $\mathbb{R}^{**}$.
- For F a field, we may form the ring $\mathcal{M}(n, F)$ of $n \times n$ matrices over F. A matrix is invertible if and only if its determinant is nonzero. So the unit group of $\mathcal{M}(n, F)$ is the set of matrices with nonzero determinant. It is called the **general linear group** and is written $\mathrm{Gl}(n, F)$.

Problems 10.3.

(1) Prove that $\mathrm{Aut}(\mathbb{Z}_n) \cong U_n$, the group of units in $\mathbb{Z}_n$.

(2) Each group U_n is isomorphic to a cyclic group or a direct product of such. For each of $n = 8, 9, 10, 11, 12$ find the product of cyclic groups that is isomorphic to U_n.

There are many interesting subgroups of the general linear group.

Exercises 10.4.

(a) Show that the general linear group has these subgroups:

- The diagonal matrices with nonzero entries.
- The upper triangular matrices.
- The **special linear group** $\mathrm{Sl}(n, F)$ is the group of matrices with determinant 1.
- The **orthogonal group** $\mathrm{O}(n, F)$ is the group of matrices Q such that Q^{-1} is the transpose of Q.

(b) Show that det is a group homomorphism from $\mathrm{Gl}(n, F)$ to F^*.

(c) For any subgroup H of F^* the set of all matrices with determinant in H is a subgroup of $\mathrm{Gl}(n, F)$.

Example 10.5. In $\mathrm{Gl}(2, \mathbb{C})$ consider the matrices

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \qquad \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \qquad \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

The set of matrices $Q = \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ is a group called the Quaternions.

Problems 10.6.

(1) Show by brute force that the quaternions are indeed a group.

(2) Find the order of each element of Q.

(3) Show that no two of the groups $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_8$, D_4, and Q are isomorphic. [Investigate the number of elements of order 4.]

Problems 10.7.

(1) Show that the subgroup of upper triangular 2×2 matrices is conjugate to the group of lower triangular matrices. [Hint: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.]

(2) Show that the set of matrices with nonzero determinant of the form $\begin{bmatrix} 0 & a \\ b & c \end{bmatrix}$ is a coset of the upper triangular matrices.

11 The Integers

There are five main results for the integers that you should know. I will call them the Division Theorem, the GCD Theorem, The Euclidean Algorithm, the Prime-Irreducible Theorem, and the Unique Factorization Theorem.

Theorem 11.1 (Division)**.** *Let a and b be integers with $b > 0$. There exist unique integers q, r such that*

(1) $a = bq + r$, *and*

(2) $0 \leq r < b$

It is fairly common in programming languages (in particular in Python and Sage) to write the integer quotient as $a//b$ and the remainder as $a\%b$. We will use this notation as needed.

Let a and b be integers. The **common divisors** of a and b are the integers that divide both a and b. The **greatest common divisor** (gcd) is the largest positive integer dividing both a and b. The **common multiples** of a and b are the integers that are multiples of both a and b. The **least common multiple** (lcm) is the smallest positive integer that is a multiple of both.

A **linear combination** of a and b is an integer that can be expressed as $au + bv$ for some integers u and v.

Theorem 11.2 (GCD)**.** *Let a and b be integers, at least one of them nonzero. The gcd of a and b is the smallest positive linear combination of a and b. In particular,* $\gcd(a, b) = au + bv$ *for some integers u and v.*

The set of all linear combinations of a and b equals the set of multiples of $\gcd(a, b)$.

We say two integers are **coprime** (or **relatively prime**) when their gcd is 1.

Given a and b, how do we find their gcd? The answer (for arbitrary large integers) is not to factor each and look for common factors. Rather, use the Euclidean algorithm.

Let's assume $a \geq b \geq 0$. Set $r_{-1} = a$ and $r_0 = b$, and define inductively (while $r_k \neq 0$)

$$\begin{aligned} q_k &= r_{k-1}//r_k \\ r_{k+1} &= r_{k-1}\%r_k, \quad \text{so that} \\ r_{k+1} &= r_{k-1} - q_k r_k \end{aligned}$$

The r_k are a strictly decreasing sequence of nonnegative integers, so the process must terminate: for some n, $r_{n+1} = 0$. There is a lemma that says: For integers

a, b, c, x such that $a = bx + c$, we have $\gcd(a, b) = \gcd(b, c)$. Let's apply this to the sequence r_k, letting n be minimal such that $r_{n+1} = 0$. We have (since $r_{n+1} = 0$)

$$\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_n, r_{n+1}) = r_n$$

This argument shows that the Euclidean algorithm produces the gcd of a and b. In the following Sage code we only keep two of the remainders at any time, not the whole sequence: after the kth pass through the while loop, r in the algorithm is r_{k-1} and s is r_k.

```
def euclid_alg(a,b):
   if b == 0:
      print "division by zero"
      return false
   else:
      r = a
      s = b
      while s != 0:
         rem =  r %s
         r = s
         s = rem
      return r
```

There is a heftier Euclidean algorithm–often called the Extended Euclidean algorithm–which produces two integers u, v such that $au + bv = \gcd(a, b)$. I like the following matrix version of the algorithm. Let

$$Q_k = \begin{bmatrix} -q_k & 1 \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad R_k = \begin{bmatrix} r_k \\ r_{k-1} \end{bmatrix}$$

where the sequence r_k and q_k are the same as used above in the Euclidean algorithm. Verify that $R_{k+1} = Q_k R_k$. Consequently,

$$R_{n+1} = \begin{bmatrix} 0 \\ r_n \end{bmatrix} = Q_n Q_{n-1} \cdots Q_0 R_0$$

where $R_0 = \begin{bmatrix} b \\ a \end{bmatrix}$. Let $M = Q_n Q_{n-1} \cdots Q_0$. Then we have $M_{2,1} b + M_{2,2} a = r_n = \gcd(a, b)$.

By the way, you can use the following equation, along with a few observations about the Fibonacci numbers to bound the number of steps for the Euclidean algorithm. Ask me, or see [**?**] for details.

$$\begin{bmatrix} b \\ a \end{bmatrix} = Q_0^{-1} Q_1^{-1} \cdots Q_n^{-1} \begin{bmatrix} 0 \\ r_n \end{bmatrix}$$

Theorem 11.3 (Euclidean Algorithm)**.** *Let a, b be integers with $b \neq 0$. The Euclidean Algorithm outputs* $\gcd(a, b)$ *in at most* $1 + \log_2 b / \log \alpha$ *steps, where α is the golden ratio. The Extended Euclidean Algorithm outputs integers u, v with $|u| < b$ and $|v| < a$ such that $au + bv = \gcd(a, b)$.*

Here is the Sage code for the extended Euclidean algorithm.

```
def ext_euclid_alg(f,h):
   if h == 0:
      print "division by zero"
      return false
   else:
      M = matrix(2, 3, [f,  1, 0, h, 0, 1])
      s = M[0,0]
      r = M[1,0]
      while s != 0:
         q =  r // s
         M  = matrix(2,2,[ -q , 1, 1, 0]) * M
         s = M[0,0]
         r = M[1,0]
      return M
```

Definition 11.4. Let r be a nonzero integer. We say r is **irreducible** when $r = ab$ implies that either $a = \pm 1$ or $b = \pm 1$. We say r is **prime** when $r|ab$ implies $r|a$ or $r|b$.

The definition of irreducible is what we customarily use for primality, but the definitions given here are the accepted ones in more general contexts. Fortunately, we have the following theorem!

Theorem 11.5 (Prime-Irreducible)**.** *A nonzero integer is irreducible iff it is prime.*

The previous theorem is the key ingredient to establishing unique factorization.

Theorem 11.6 (Unique Factorization)**.** *Let a be a nonzero integer. There is a nonnegative integer t, positive prime numbers $p_1, \ldots, p_t$, and positive integers $e_1, \ldots e_t$ and choice of unit, $u = 1$ or -1, such that*

$$a = u p_1^{e_1} \cdots p_t^{e_t}$$

Each of t, p_i, e_i and u is uniquely determined.

Here are some computational exercises that will help solidify your understanding of the properties of the integers, and give you some practice programming. Some questions are a bit open-ended, just use them to play around with the ideas.

Exercises 11.7.

(a) Euclidean algorithm problems. Suppose a and b are fixed (for example $a = 12$ and $b = 7$).

(1) Fix some $N > 0$ and make a list of the elements in the set $S = \{ax+by : x, y \in \{-N, \ldots, N\}\}$. Explore how, as you increase N the set "fills in." How large does N need to be to guarantee that $\gcd(a, b) \in S$? What would the set be if we allowed x and y to vary over all integers?

(2) Compare the speed of the Euclidean algorithm above with built-in function.

(3) Amend our gcd funtion to tell how many divisions occurred.

(4) How many steps does the Euclidean algorithm take in general? Do most a, b take roughly $\log(b)$ steps, or do most take many fewer steps?

(5) For $t = 1, 2, 3, 4, 5$ find the smallest a, and the smallest b for that a such that the Euclidean algorithm requires t divisions.

(b) Prime factorization.

(1) The Prime Number Theorem states that the number of primes in the range $[2, n]$ is roughly $n/\ln(n)$. Check this result by sampling a lot of integers in the range $[2^k, 2^{k+1}]$ and checking for primality. What proportion should be prime?

(2) How is the number of prime factors of an integer in $[2^k, 2^{k+1}]$ distributed. Do most integers have lots of factors, or relatively few?

12 Integers modulo n

Let n be an integer. Integers a and b are **congruent modulo** n when n divides $a - b$.

Theorem 12.1. *Congruence modulo n is an eqivalence relation. The set $\{0, 1, \ldots, n-1\}$ is a system of representatives for congruence modulo n; each integer is congruent modulo n to exactly one element of $\{0, 1, \ldots, n-1\}$.*

Two special cases are worth noting. When $n = 0$, a is congruent to b iff and only if $a = b$. When $n = 1$ (or $n = -1$), a is congruent to b for all integers a and b. The integers n and $-n$ give the same equivalence relation, so we always use positive integers for the modulus.

It is common to write $[a]_n$ for the congruence class of a modulo n, whenever we need to be careful to distinguish between the integer a and the congruence class, or when we have more than one modulus to worry about. Otherwise, if it is clear from context, we may simply write a.

Theorem 12.2 (Arithmetic mod n)**.** *Suppose that $a \equiv b \mod n$ and $r \equiv s \mod n$. Then $a + r \equiv b + s \mod n$ and $ar = bs \mod n$. Thus, arithmetic on congruence classes modulo n is well-defined.*

We will write $\mathbb{Z}/n$ for the set of equivalence classes modulo n, with the operations $+$ and $*$. (It is common to use $\mathbb{Z}_n$, but $\mathbb{Z}/n$ is consistent with notation we will use later.) Usually, we write the equivalence classes as $0, 1, \ldots, n-1$ (without the brackets and using the least nonnegative representatives for each class). But, sometimes it is handy to be a bit flexible. For example it is good to remember that $n - b$ is equal to $-b$ in $\mathbb{Z}/n$. So (in $\mathbb{Z}/n$)

$$b(n-1) = (-1)b = n - b$$

Theorem 12.3 (Units, Zero Divisors)**.** *Let $n \geq 2$ be an integer and let a be an integer.*

(1) $[a]_n$ is a unit iff $\gcd(a, n) = 1$.

(2) $[a]_n$ is a zero divisor iff $1 < \gcd(a, n) < n$.

In particular, an element of $\mathbb{Z}/n$ is either 0, a unit, or a zero-divisor (and these are mutually exclusive).

The main result we need for Galois theory is the following.

Corollary 12.4. *Let p be a prime number. Then $\mathbb{Z}/p$ is a field; every nonzero element has an inverse.*

When working modulo a prime we usually use the notation $\mathbb{F}_p$ instead of $\mathbb{Z}/p$ to emphasize that we have a field.

The Arithmetic Mod n Theorem shows that the function taking $a \in \mathbb{Z}$ to $[a]_n \in \mathbb{Z}/n$ is a homomorphism. We actually defined addition and multiplication in $\mathbb{Z}/n$ so that this map is a homomorphism. If d divides m there is a well-defined function from $[a]_m$ to $[a]_d$— this is because $d|m$ and $m|(b-a)$ implies $d|(b-a)$—so any two integers that are congruent modulo m are also congruent modulo d. On the other hand if $d \not| m$, there is no well-defined function from $\mathbb{Z}/m$ to $\mathbb{Z}/d$. Since the arithmetic on $\mathbb{Z}/m$ is "inherited" from $\mathbb{Z}$, we have:

Theorem 12.5 (Homomorphism mod m)**.** *There is a homomorphism from $\mathbb{Z}/m$ to $\mathbb{Z}/d$ iff $d|m$. The homomomorphism is unique (since it takes $[1]_m$ to $[1]_d$).*

For any two integers m, n we have a homomorphism $\mathbb{Z}/mn \longrightarrow \mathbb{Z}/m$ and $\mathbb{Z}/mn \longrightarrow \mathbb{Z}/n$. This gives a homomorphism into the Cartesian product: $\mathbb{Z}/m \times \mathbb{Z}/n$. The Chinese Remainder Theorem says this is an isomorphism when m, n are coprime. See [**?**][§4.3] or [**?**][§13.1]for a formula for computing the inverse isomorphism.

Theorem 12.6 (Chinese Remainder Theorem)**.** *Let m, n be coprime. The natural maps give an isomorphism $\mathbb{Z}/mn \longrightarrow \mathbb{Z}/m \times \mathbb{Z}/n$.*

13 The Univariate Polynomial Ring over a Field

Let F be a field. By $F[x]$ we mean the polynomial ring in the indeterminate x. The key fact about polynomial rings is that all the theorems we discussed for integers hold with appropriate modifications, for polynomial rings over F.

We can think of the polynomial ring as (1) a vector space over F with an infinite basis $1, x, x^2, \ldots$, (2) the additional multiplicative structure defined by $x^i * x^j = x^{i+j}$ and the properties of a ring (e.g. distributivity). Sometimes it is useful to write a polynomial $f(x) \in F[x]$ as a sum $f(x) = \sum_{i=0}^{\infty} f_i x^i$ with the understanding that only a finite number of the f_i are nonzero. Suppose $f(x) \neq 0$ and let d be the largest integer such that $f_d \neq 0$. We call d the **degree** of $f(x)$; $f_d x^d$ is the **leading term** of $f(x)$; x^d is the **leading monomial** of $f(x)$; and f_d is the **leading coefficient** of $f(x)$. If $f_d = 1$ we say $f(x)$ is **monic**. When $d = 0$ we say $f(x)$ is a **constant** polynomial. The zero polynomial is also considered a constant polynomial and the degree is sometimes defined to be $-\infty$.

It should be clear that $F[x]$ has no zero-divisors, so it is an integral domain. The product of a polynomial of $f(x)$ of degree α and $g(x)$ of degree β has degree $\alpha + \beta$. In order for $f(x)$ to be a unit it must therefore have degree 0, so the units in $F[x]$ are the constant polynomials.

Theorem 13.1 (Division)**.** *Let $f(x)$ and $h(x)$ be in $F[x]$ with $g(x) \neq 0$. There exist unique $q(x)$, $r(x)$ such that*

(1) $f(x) = h(x)q(x) + r(x)$*, and*

(2) $\deg r(x) < \deg h(x)$

We will usually omit the (x) to simplify notation, but use it when it makes the discussion more clear. We will write the quotient as $f//h$ and the remainder as $f\%h$. This notation works in Sage for polynomials as well as integers.

The greatest common divisor of two integers was easy to define since the integers are well ordered. It is not obvious that, among the common divisors of $f, h \in F[x]$, there is just one monic divisor of maximal degree. The following theorem shows the gcd can be uniquely defined, and extends the GCD Theorem to polynomials. A **polynomial combination** of f and h is a polynomial that can be expressed as $fu + hv$ for some $u, v \in F[x]$.

Theorem 13.2 (GCD)**.** *Let $f, h \in F[x]$ with at least one of them nonzero. There is a unique polynomial d satisfying*

(1) d is a common divisor of f and h,

(2) d is monic,

(3) d has maximal degree among common divisors of f and h.

Furthermore, there exist $u, v \in F[x]$ such that $d = fu + hv$. The set of all polynomial combinations of f and h equals the set of multiples of d.

The proof of the theorem can be adapted for any set of polynomials $S \subseteq F[x]$. We may look at the largest degree monic polynomial that divides all the elements of S. You can show that it is also the smallest degree monic polynomial that can be expressed as a combination of the elements of S.

The discussion of the Euclidean algorithm for integers carries over almost verbatim (just think of a and b as polynomials). The r_k are strictly decreasing in degree, so we must eventually get the 0 polynomial. The algorithm takes at most $\deg(b)$ steps. The Sage code appearing earlier needs no modification to be used with polynomials.

Let $f \in F[x]$ have degree at least one. As with integers, we say f is **irreducible** when it can't be factored in a nontrivial way: whenever $f = ab$ either $a \in F$ or $b \in F$. We say f is **prime** when $f|ab$ implies $f|a$ or $f|b$.

As with integers, we have the equivalence of primality and irreducibility, which is a key step towards proving unique factorization.

Theorem 13.3 (Prime-Irreducible)**.** *Any nonconstant element of $F[x]$ is irreducible iff it is prime.*

Theorem 13.4 (Unique Factorization)**.** *Let $f(x) \in F[x]$ be nonzero. There is a nonnegative integer t, a constant $u \in F$, monic irreducible polynomials $p_1(x), \ldots, p_t(x)$, and positive integers $e_1, \ldots e_t$ such that*

$$f(x) = up_1(x)^{e_1} \cdots p_t(x)^{e_t}$$

Each of t, p_i, e_i and u is uniquely determined.

The polynomial ring has additional properties that make it easier to work with than the integers. Each $f(x) \in F[x]$ defines a function from F to F, which we call **evaluating** f. The function is $c \longmapsto f(c) = f_0 + f_1 c + f_2 c^2 + \cdots + f_d c^d$ where $d = \deg(f(x))$. When $f(c) = 0$ we say that c is a **root of** $f(x)$.

Let me turn things around now.

Exercises 13.5.

(a) Fix $c \in F$ and consider the function $\mathrm{ev}_c : F[x] \longrightarrow F$ defined by $f(x) \longrightarrow f(c)$. Show that this function is a homomorphism.

(b) Show furthermore that the remainder $f \,\%\, (x - c) = f(c)$.

Theorem 13.6. *Let $f(x) \in F[x]$. Any $c \in F$ is a root of $f(x)$ iff $f(c) = 0$. Consequently, a polynomial of degree d can have at most d roots.*

The computational exercises for the integers have analogues for $F[x]$.

Exercises 13.7.

(a) Euclidean algorithm problems. Suppose f and h are fixed.

(1) Fix some $d > 0$ and make a list of the elements in the set $S = \{fu + hv : u, v \in F[x], \deg(u), \deg(v) \leq d\}$. Explore how, as you increase d the set "fills in." How large does d need to be to guarantee that $\gcd(f, h) \in S$? What would the set be if we allowed u and v to vary over all $F[x]$?

(2) Compare the speed of the Euclidean algorithm above with built-in function.

(3) Amend our gcd funtion to tell how many divisions occurred.

(4) How many steps does the Euclidean algorithm take in general? Do most f, h take roughly $\deg(h)$ steps, or do most take many fewer steps?

(b) Factorization of polynomials.

(1) What proportion of the polynomials of degree d are irreducible? Test this first for polynomials over $\mathbb{F}_p$ for p prime. You can do an exhaustive search. For $\mathbb{Q}[x]$, you can sample the coefficients integer $d + 1$ integer coefficients from some range (say $[-N..N]$). This, at least, gives some idea.

(2) How is the number of factors of a polynomial of degree d distributed?

14 Polynomial modulus

We now extend the notion of modular arithmetic to the polynomial ring over a field.

Let $m(x) \in F[x]$ have degree d. Polynomials $f(x)$ and $h(x)$ are **congruent modulo** $m(x)$ when $m(x)$ divides $f(x) - h(x)$.

Theorem 14.1. *Congruence modulo $m(x)$ is an eqivalence relation. The set of polynomials of degree less than $d = \deg(m(x))$ is a system of representatives for congruence modulo $m(x)$. That is, each polynomial is congruent modulo $m(x)$ to its remainder when divided by $m(x)$, which has degree less than d.*

Two special cases are worth noting. When $m(x) = 0$, $f(x)$ is congruent to $h(x)$ iff and only if $f(x) = h(x)$. When $m(x)$ is a constant, $f(x)$ is congruent to $h(x)$ for all $f(x), h(x)$. Any constant multiple of $m(x)$ will define the same equivalence relation as $m(x)$ so we usually take $m(x)$ to be monic.

We will write $[f(x)]_{m(x)}$ for the congruence class of $f(x)$ modulo $m(x)$, whenever we need to be careful to distinguish between $f(x)$ and its congruence class. We hope this rarely occurs!

Theorem 14.2 (Arithmetic mod $m(x)$)**.** *Suppose that $f(x) \equiv h(x) \mod m(x)$ and $r(x) \equiv s(x) \mod m(x)$. Then $f(x) + r(x) \equiv b(x) + s(x) \mod m(x)$ and $f(x)r(x) = b(x)s(x) \mod m(x)$. Thus, arithmetic on congruence classes modulo $m(x)$ is well-defined.*

We will write $F[x]/m(x)$ for the set of equivalence classes modulo $m(x)$, with the operations $+$ and $*$.

Theorem 14.3 (Units, Zero Divisors)**.** *Let $m(x) \in F[x]$, and $f(x) \in F[x]$.*

(1) $f(x)$ is a unit in $F[x]/m(x)$ iff $\gcd(f(x), m(x)) = 1$.

(2) $f(x)$ is a zero-divisor in $F[x]/m(x)$ iff $0 < \deg(\gcd(f(x), m(x))) < \deg(m(x))$.

In particular, an element of $F[x]/m(x)$ is either 0, a unit, or a zero-divisor (and these are mutually exclusive).

Corollary 14.4. *Let $p(x) \in \mathbb{F}[x]$ have degree at least one. Then $\mathbb{F}[x]/p(x)$ is a field iff $p(x)$ is irreducible.*

The Arithmetic Mod $p(x)$ Theorem also shows that the function taking $f(x)$ to $[f(x)]_{m(x)}$ is a homomorphism from $F[x]$ to $F[x]/m(x)$. If $d(x)$ divides $m(x)$ then there is a well defined function from $F[x]/m(x)$ to $F[x]/d(x)$. This is because $m(x)|(a(x) - b(x))$ implies $d(x)|(a(x) - b(x))$, so any two polynomials that are congruent modulo $m(x)$ are also congruent modulo $d(x)$. On the other hand if $d(x) \not| m(x)$ there is no well defined function from $F[x]/m(x)$ to $F[x]/d(x)$ (e.g. $m(x)$ is congruent to 0 modulo $m(x)$ but is not congruent to 0 mod $d(x)$). Since the arithmetic on $F[x]/m(x)$ is "inherited" from $F[x]$ we have:

Theorem 14.5 (Homomorphism mod $m(x)$)**.** *There is a homomorphism from $F[x]/m(x)$ to $F[x]/d(x)$ iff $d(x)|m(x)$. The homomomorphism is unique (since it takes $[1]_{m(x)}$ to $[1]_{d(x)}$ and $[x]_{m(x)}$ to $[x]_{d(x)}$).*

For any two polynomials $m(x), n(x)$ we have a homomorphism $F[x]/(m(x)n(x)) \longrightarrow F[x]/m(x)$ and $F[x]/(m(x)n(x)) \longrightarrow F[x]/n(x)$. This gives a homomorphism into the Cartesian product: $F[x]/m(x) \times F[x]/n(x)$. There is a straightforward generalization of the CRT (and the associated algorithm).

Theorem 14.6 (Chinese Remainder Theorem)**.** *Let $m(x), n(x) \in F[x]$ be coprime. There is an isomorphism $F[x]/(m(x)n(x)) \longrightarrow F[x]/m(x) \times F[x]/n(x)$.*

15 Special Properties of The Polynomial Ring $F[x]$

In this section we establish some fundamental, but very subtle properties of polynomial rings.

Notation 15.1. We will often use simplifying notation when working with polynomials. We will write $f \in F[x]$, and use $f(x)$ when we need to be very clear. I will always use f_i for the coefficients of f, and I will write $f = \sum_i f_i x^i$. The sum is implicitly for $i = 0$ to ∞, but only a finite number of terms are nonzero.

Here is an additional result about polynomial rings that will be useful. It is similar to The Initial Ring Theorem 9.5 for the integers.

Theorem 15.2 (Universal property of polynomial rings)**.** *Let R, S be rings and let $\varphi : R \longrightarrow S$ be a ring homomorphism. For any $s \in S$ there is a unique homomorphism from $R[x]$ to S that agrees with φ on R and takes x to s, namely*

$$\begin{aligned} \overline{\varphi} : R[x] &\longrightarrow S \\ \Big(\sum_i r_i x^i\Big) &\longmapsto \sum_i \varphi(r_i) s^i \end{aligned}$$

Proof. If there is a homomorphism $\overline{\varphi}$ taking x to s and agreeing with φ on R then we must have

$$\overline{\varphi}\Big(\sum_i r_i x^i\Big) = \sum_i \overline{\varphi}(r_i x^i) = \sum_i \overline{\varphi}(r_i)\overline{\varphi}(x)^i = \sum_i \varphi(r_i) s^i$$

The key observation is that $\overline{\varphi}$ is well defined because there is a unique way to write each element of $R[x]$ and we have used this unique formulation to define $\overline{\varphi}$.

To show this function is indeed a homomorphism we check that it respects the operations. I leave sums to you. Notice that

$$(\sum_i a_i x^i)(\sum_i r_i x^i) = \sum_i \sum_j a_i r_j x^{i+j}$$

Set $k = i + j$ and gather terms in x^k,

$$= \sum_k x^k \sum_{i=0}^{k} (a_i r_{k-i})$$

A similar derivation shows that for $b_i, t_i \in S$

$$(\sum_i b_i s^i)(\sum_i t_i s^i) = \sum_k s^k \sum_{i=0}^{k} b_i t_{k-i}$$

Thus we have

$$\begin{aligned}
\overline{\varphi}\Big(\Big(\sum_i a_i x^i\Big)\Big(\sum_i r_i x^i\Big)\Big) &= \overline{\varphi}\Big(\sum_k x^k \Big(\sum_{i=0}^{k} a_i r_{k-i}\Big)\Big) \\
&= \sum_k s^k \Big(\sum_{i=0}^{k} \varphi(a_i r_{k-i})\Big) \\
&= \Big(\sum_i \varphi(a_i) s^i\Big)\Big(\sum_j \varphi(r_j) s^j\Big) \\
&= \overline{\varphi}\Big(\sum_i a_i x^i\Big)\overline{\varphi}\Big(\sum_i r_i x^i\Big)
\end{aligned}$$

This shows $\overline{\varphi}$ respects products □

Here is a fundamental application of the universal property. It shows that composition (with a fixed $g(x)$) may be considered as a homomorphism.

Proposition 15.3. *Let $g(x) \in F[x]$. There is a homomorphism $F[x] \longrightarrow F[x]$ taking $f(x)$ to $f(g(x))$. This map is an isomorphism iff $g(x)$ has degree 1.*

Proof. We apply the universal property of polynomial rings to the embedding of F into $F[x]$. The Theorem says that for any $g(x)$ there is a homomorphism $\varphi : F[x] \longrightarrow F[x]$ taking x to $g(x)$.

If $g(x)$ has degree 1, then $g(x) = ax + b$ with $a \neq 0$. I claim that φ defined by $\varphi(x) = ax + b$ (and $\varphi(c) = c$ for $c \in F$) is an isomorphism of $F[x]$ with inverse

$\psi(x) = x/a - b/a$. We have $\psi(\varphi(x)) = \psi(ax+b) = a\psi(x)+b = a(x/a-b/a)+b = x$. Thus $\psi \circ \varphi$ is the identity map on $F[x]$. Similarly, one can show $\varphi \circ \psi$ is the identity map.

If $g(x)$ is 0 or if $\deg(g(x)) = 0$ then φ is clearly not surjective, so is not an isomorphism.

Now suppose $\deg(g(x)) = d > 1$ with $g(x) = g_d x^d + \cdots + g_0$. Let us show that there is no inverse to φ. Let $\psi : F[x] \longrightarrow F[x]$ be any other homomorphism and let $\psi(x) = h(x)$. Then $\varphi \circ \psi(x) = g_d(h(x))^d + \cdots + g_1 h(x) + g_0$. The degree of this sum is the degee of $(h(x))^d$, which is $d \deg(h(x))$. Since $d > 1$ the degree of $\varphi \circ \psi(x)$ cannot be 1. Thus $\varphi \circ \psi(x) \neq x$ and φ must not have an inverse.

□

One more consequence of the universal property follows. This result is similar to the order theorem (Theorem 1.24), following the general theme that many properties for $\mathbb{Z}$ extend to polynomial rings over a field.

Proposition 15.4. *Let R be a ring containing a field F. For any $r \in R$ there is a unique homomorphism φ from $F[x]$ to R that is the identity on F and takes x to r. If the kernel of φ is not just 0 then there is some polynomial $m(x)$ such that every element of the kernel is a multiple of $m(x)$.*

Proof. The existence of the homomorphism is guaranteed by the universal property. Suppose that the kernel is non-trivial and let $m(x)$ be a nonzero polynomial of minimal degree in the kernel. For any $f(x)$ in the kernel, write $f(x) = q(x)m(x) + r(x)$ with $\deg(r(x)) < \deg(m(x))$. Then $r(x) = f(x) - q(x)m(x)$ is also in the kernel, so $\varphi(r(x)) = 0$. Since $m(x)$ was chosen to have minimal degree, $r(x) = 0$, and $f(x)$ is a multiple of $r(x)$. □

The proposition may be proven more quickly by noting that the kernel is an ideal in $F[x]$ and all ideals in $F[x]$ are principal.

Definition 15.5. In the situation of the previous proposition, the polynomial $m(x)$, when it exists, is called the **minimal polynomial** of r. If $m(x) = x^d + m_{d-1}x^{d-1} + m_1 x + m_0$ then applying φ we have $r^d + m_{d-1}r^{d-1} + m_1 r + m_0 = 0$ in R. We say r is **a root** of $m(x)$ and that r is **algebraic of degree d over F**. If the kernel of φ is trivial r is said to be **transcendental** over F.

16 Irreducibility

Now to the question of irreducibility. It is not always easy to check whether a polynomial is irreducible, but here is one easy case: If a polynomial of degree 2

or 3 factors, then one of the factors must be linear. The linear factor then has a root, which is also a root of the original polynomial. Thus, we have:

Proposition 16.1. *Let $f(x) \in F[x]$ have degree 2 or 3. If $f(x)$ has no roots then it is irreducible.*

If you want to check whether an integer n is prime, it is enough to check whether it is divisible by a prime number less than or equal to $\sqrt{n}$. We have a similar result for polynomials.

Proposition 16.2. *Let $f(x) \in F[x]$ have degree n. If $f(x)$ is not divisible by any irreducible polynomial of degree d for all $d \leq n/2$ then $f(x)$ is irreducible.*

Proposition 16.3. *Let $f(x) \in F[x]$ and $a \in F$. Then $f(x)$ is irreducible iff $f(x-a)$ is irreducible.*

Proof. There is an isomorphism φ from $F[x]$ to itself taking x to $x-a$. If $f(x)$ factors then $\varphi(f) = f(x-a)$ also factors, and conversely. □

Definition 16.4. Let $f \in \mathbb{Z}[x]$. The gcd of the coefficients of f is called the **content** of f: $\gcd\{f_i : i \in \mathbb{N}_0\} = c(f)$. A polynomial whose content is 1 is often called primitive, but we will use that term for a different meaning later, so we will just say content 1. We can factor any $f \in \mathbb{Z}[x]$ as $c(f)f^*$ where f^* has content 1.

These definitions and the following results may be extended to any unique factorization domain D and its field of quotients $K(D)$.

Proposition 16.5. *Let $f = f_0 + f_1 x + \cdots + f_d x^d \in \mathbb{Z}[x]$ have degree d and content 1. If $r/s \in \mathbb{Q}$ is a root of f then $r \mid f_0$ and $s \mid f_d$.*

Proposition 16.6. *Let $f \in \mathbb{Z}[x]$ have content 1. f is irreducible in $\mathbb{Z}[x]$ iff f is irreducible in $\mathbb{Q}[x]$.*

There is a natural homomorphism $\mathbb{Z} \longrightarrow \mathbb{Z}/n$ and there is a natural inclusion $\mathbb{Z}/n$ to $\mathbb{Z}/n[x]$. Composing the two, we have a homomorphism $\mathbb{Z} \longrightarrow \mathbb{Z}/n[x]$. Consequently, Proposition 15.2 tells us there is a homomorphism, $\mathbb{Z}[x] \longrightarrow \mathbb{Z}/n[x]$ taking x to x. This map is simply reducing the coefficients modulo n.

Proposition 16.7. *Let $f \in \mathbb{Z}[x]$ have degree d and content 1. Let $\bar{f}$ be the image of f in $\mathbb{F}_p[x]$ for some prime p that doesn't divide f_d. If $\bar{f}$ is irreducible in $\mathbb{F}_p[x]$ then f is irreducible in $\mathbb{Z}[x]$ and also in $\mathbb{Q}[x]$.*

Proposition 16.8 (Eisenstein's criterion)**.** *Let $f \in \mathbb{Z}[x]$ had degree $d \geq 1$ and content 1. If there is a be a prime number p such that*

- $p \nmid a_d$
- $\mid a_i$ *for* $i < d$
- $p^2 \nmid a_0$

then f *is irreducible.*

Problems 16.9.

(1) Let p be prime. It is clear that $(x^p - 1)$ is not irreducible since it has a root, 1. Show that $\frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible over $\mathbb{Q}$. Use the isomorphism $x \longmapsto (x + 1)$ and Eisenstein's criterion.

(2) Test whether the following polynomials are irreducible over the rationals.

- $3x^2 - 7x - 5$
- $2x^3 - x - 6$
- $x^3 - 9x - 9$

(3) Show that $x^4 - 10x + 1$ is irreducible over the rationals as follows.

- Show it has no roots.
- Try to factor it as a product of quadratics and derive a contradiction.

(4) Quadratic fields over $\mathbb{F}_3$.

- Find all monic irreducibles of degree 2 over $\mathbb{F}_3$.
- Let α be the class of x in the field $\mathbb{F}_3[x]/(x^2 + 2x + 2)$. Show that the powers of α give all nonzero element of this field.
- Show that all the monic irreducibles found earlier have two roots in this field.

(5) A field with 32 elements.

- Using arguments similar to what we did in class, find all irreducible polynomials of degree 5 over $\mathbb{F}_2$.
- Let $m(x)$ be one of the polynomials you found. Use sage to create the field $\mathbb{F}_2[x]/m(x)$. Let a be the class of x.
- Explain why the powers of a give all elements of this field.
- Use sage to show that all the irreducibles of degree 5 have 5 roots in this new field.

17 First Fields and Automorphisms

There are a few fields that should be familiar to you. We are going to start the discussion of fields by enlarging this collection and by studying field automorphisms.

The fields you should know are:

- The rational numbers $\mathbb{Q}$. This is the smallest field that contains the integers.
- The prime fields $\mathbb{F}_p$ for each prime number p. A fundamental result from modular arithmetic is that each nonzero element in $\mathbb{Z}_p$, the ring of integers modulo p, is invertible. You can compute the inverse using the extended Euclidean algorithm. This shows that $\mathbb{Z}_p$ is a field. When studying fields we will write $\mathbb{F}_p$ instead of $\mathbb{Z}_p$.
- The real field, $\mathbb{R}$.
- The field of complex numbers $\mathbb{C}$. The complex numbers is a vector space of dimension 2 over $\mathbb{R}$ with basis $\{1, i\}$ where $i = \sqrt{-1}$. That is, every element of $\mathbb{C}$ may be written in a unique way as $a + bi$ for $a, b \in \mathbb{R}$.

Definition 17.1. For fields (or division rings) F and K, a function $\varphi : F \longrightarrow K$ is a homomorphism iff

(1) φ is a homomorphims of the groups $F, +_F$ and $K, +_K$, and

(2) φ is a homomorphism of the groups $F^*, *_F$ and $K^*, *_K$.

Applying Proposition 1.8, $\varphi : F \longrightarrow K$ is a homomorphism of fields if it respects addition and multiplication: $\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$ and $\varphi(a_1 * a_2) = \varphi(a_1) * \varphi(a_2)$. Note: In the last two equations the addition and multiplication on the left is done in F and the addition and multiplication on the right is in K. Henceforth I'm going to follow standard practice and *not* write the subscripts on the operation signs to make the equations more legible. BUT, don't forget the distinction! We will also usually not write the multiplication sign, unless there is some important reason to use it.

It turns out that a homomorphisms of fields is always injective!

Proposition 17.2. *Let $\varphi : F \longrightarrow K$ be a homomorphism of fields. Then $\varphi(a) = \varphi(b)$ implies $a = b$.*

Proof. Let $\varphi : F \longrightarrow K$ be a homomorphism. Let a be a nonzero element of F. Since $aa^{-1} = 1_F$, applying φ we get $\varphi(a)\varphi(a^{-1}) = 1_K$. Since 0_K does not have a multiplicative inverse, $\varphi(a)$ cannot be 0_K. Thus $a \neq 0_F$ implies $\varphi(a) \neq 0_K$.

Now suppose $\varphi(a) = \varphi(b)$. Then $\varphi(a-b) = 0_K$, and the contrapositive of what we showed in the previous paragraph gives $a - b = 0$, so $a = b$. □

Of particular interest is the set of all isomorphisms from a field F to itself. The following proposition is another *very* worthwhile exercise.

Proposition 17.3.

(1) The composition of two field homomorphisms is a field homomorphism.

(2) The composition of two isomorphisms of fields is an isomorphism of fields.

(3) Let $\varphi : F \longrightarrow K$ be an isomorphism of fields. The inverse function $\varphi^{-1} : K \longrightarrow F$ is also an isomorphism of fields.

And now the culmination of this section!

Definition 17.4. Let F be a field. The *automorphism group* of F is the set of all isomorphisms from F to itself, with the operation of composition. It is written $\mathrm{Aut}(F)$.

Proposition 17.5. *For F a field, $\mathrm{Aut}(F)$ is indeed a group.*

What can we say about automorphisms of the fields introduced above? First note that any automorphism has to take 1 to itself. Consider an automorphism φ of $\mathbb{Q}$. We must have $\varphi(1) = 1$. Since φ respects addition,

$$\varphi(\underbrace{1 + \cdots + 1}_{b \text{ terms}}) = \underbrace{\varphi(1) + \cdots + \varphi(1)}_{b \text{ terms}}$$

which shows that $\varphi(b) = b$ for each positive integer b. Since φ also respects additive inverses, $\varphi(-b) = -b$ for positive integers b, so φ is the identity map on the integers. Since φ respects multiplicative inverses, $\varphi(1/b) = 1/\varphi(b) = 1/b$ for any integer b, and since φ respects products $\varphi(a/b) = \varphi(a)\varphi(1/b) = a/b$. Thus we have shown that the only automorphism of $\mathbb{Q}$ is the identity map. A similar (shorter argument) shows that the only automorphism of $\mathbb{F}_p$ is the identity map.

Notice also that there can be no homomorphism from $\mathbb{Q}$ to $\mathbb{F}_p$ since any homomorphism must be injective.

The reals are vastly more complicated, so let's consider automorphims of $\mathbb{C}$ that fix $\mathbb{R}$. By "fix" we mean that the automorphism φ of $\mathbb{C}$ is the identity map on the reals, $\varphi(r) = r$ for $r \in \mathbb{R}$. We know that $i * i = -1$ so $\varphi(i) * \varphi(i) = \varphi(-1) = -1$. Thus there are only two possibilities, $\varphi(i)$ is either i itself or $-i$. In the first case φ has to be the identity map, $\varphi(a + bi) = \varphi(a) + \varphi(b)\varphi(i) = a + bi$ since φ fixes the reals. In the second case φ is the conjugation map: $\varphi(a + bi) = a - bi$.

This simple example is the model for our work this semester. For a field K containing another field F, we seek to understand the automorphisms of K that fix F, and to use that knowledge to better understand the field K.

18 Constructing Fields: Quadratic Fields

We have two main tools for constructing new fields.

Construction I: The first method is to work inside a known field, usually the complex numbers, and find the smallest field containing some specified elements.

Construction II: The second method is based on Theorem 14.3 about units and zero divisors in $F[x]/m(x)$ for F a field, which is analogous to the result that $\mathbb{Z}/p$ is a field.

Corollary 14.4 Let F be a field and let $p(x)$ be an irreducible polynomial in $F[x]$. The ring $F[x]/p(x)$ is a field.

Let's start with Construction I.

Example 18.1. Consider the smallest field inside the complex numbers that contains $\mathbb{Q}$ and i. I claim this is $F = \{a + bi : a, b \in \mathbb{Q}\}$. Certainly this set is a small as possible, since any field in $\mathbb{C}$ must contain $\mathbb{Q}$ and any field containing i must contain $a + bi$ for any rationals a, b. To show this set is a field we have to show that it satisfies the field axioms.

- Associativity and commutativity of $+, *$ (and distributivity of $*$ over $+$) are immediate, since they hold in $\mathbb{C}$.
- The additive indentity $0 + 0i$ and the multiplicative identity $1 + 0i$ are in F.
- For $a + bi \in F$, the additive inverse of $a + bi$ is $(-a) + (-b)i$, which is also in F. The multiplicative inverse of $a + bi$ is $\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i$, which is also in F.
- We must also check that $+$ and $*$ operations on F. This means that we must check *closure*: for $a + bi$ and $r + si$ in F their sum and their product must be in F.

$$(a + bi) + (r + si) = (a + r) + (b + s)i$$
$$(a + bi) * (r + si) = (ar - bs) + (as + br)i$$

These are in F since $a + r$ and $b + s$ and $ar - bs$ and $as + br$ are all rational.

This completes the proof that $\{a + bi : a, b \in \mathbb{Q}\}$ is a field. This field is called the *Gaussian integers* and is usually written $\mathbb{Q}[i]$. We can show that $\mathrm{Aut}(\mathbb{Q}[i])$ just has two elements—the identity map, and the map taking $a + bi$ to $a - bi$. The argument is exactly the same as used above for the automorphisms of the complex numbers that fix the reals.

Now let's consider Construction II.

Example 18.2. The polynomial x^2+1 is irreducible as an element of $\mathbb{Q}[x]$ since it has no roots. Thus $\mathbb{Q}[x]/(x^2+1)$ is a field. The rule for addition is simple $(a+bx)+(r+sx)=(a+r)+(b+s)x$. The rule for multiplication of $a+bx$ and $r+sx$ is: compute the product, then take the remainder after division by x^2+1. We get $(a+bx)(r+sx)=ar+(as+br)x+bsx^2$, and dividing by x^2+1 gives the remainder $(ar-bs)+(as+br)x$.

I leave it to you to check that there is an isomorphism

$$\begin{aligned}\frac{\mathbb{Q}[x]}{x^2+1} &\longrightarrow \mathbb{Q}[i]\\ a+bx &\longmapsto a+bi\end{aligned}$$

Show this functions respects $+$ and respects $*$.

More generally, we have the following, which you should prove. The main issue in (1) is to show that the set given is closed under multiplication and (multiplicative) inversion.

Proposition 18.3. *Let D be a rational number that is not a perfect square.*

(1) The set $\left\{a+b\sqrt{D} : a,b\in\mathbb{Q}\right\}$ is a field (it is denoted $\mathbb{Q}[\sqrt{D}]$).

(2) The polynomial x^2-D is irreducible.

(3) The field $\mathbb{Q}[x]/(x^2-D)$ is isomorphic to $\mathbb{Q}[\sqrt{D}]$.

(4) The field $\mathbb{Q}[\sqrt{D}]$ is equal to $\mathbb{Q}[\sqrt{a}]$ for some square free integer *a.*

(5) There are two automorphisms of $\mathbb{Q}[\sqrt{D}]$. The nontrivial one takes $\sqrt{D}$ to $-\sqrt{D}$ (and $\sqrt{a}$ to $-\sqrt{a}$).

The quadratic formula

There is a relationship between the quadratic formula and field extensions.

Consider a quadratic $m(x)=ax^2+bx+c$ with $a,b,c\in\mathbb{Q}$. The roots of this polynomial are $r=-b/2a+\sqrt{b^2-4ac}/2a$ and $\bar{r}=-b/2a-\sqrt{b^2-4ac}/2a$. Let $D=b^2-4ac$ be the discriminant of $m(x)$ and suppose D is not a perfect square (Then $\sqrt{D}$ is irrational).

I claim that $\mathbb{Q}[r]=\{a+br : a,b\in\mathbb{Q}\}$ and $\mathbb{Q}[\sqrt{D}]$, are the same (not just isomorphic, they include the same elements from $\mathbb{C}$). One inclusion is easy, r is evidently in $\mathbb{Q}[\sqrt{D}]$ since r is the sum of a rational number, $-b/2a$, and a rational multiple of $\sqrt{D}$. Consequently any $s+tr$ with $s,t\in\mathbb{Q}$ is also in $\mathbb{Q}[\sqrt{D}]$.

To prove the reverse inclusion, note that $b + 2ar = \sqrt{D}$ so $\sqrt{D} \in \mathbb{Q}[r]$. Then $s + t\sqrt{D} = s + t(2ar + b) = (s + tb) + (2at)r$ will also be in $\mathbb{Q}[r]$. Thus the two fields are equal.

Since $m(x)$ has no rational roots, it is irreducible. Consider the field $\mathbb{Q}[x]/m(x)$. It is a straightforward calculation to show that it is isomorphic to $\mathbb{Q}[r]$. We now know that $\mathbb{Q}[x]/m(x)$ is isomorphic to $\mathbb{Q}[r]$ that $\mathbb{Q}[r]$ is equal to $\mathbb{Q}[\sqrt{D}]$ and by Proposition 18.3 $\mathbb{Q}[\sqrt{D}]$ is equal to $\mathbb{Q}[\sqrt{a}]$ for some square free integer a. Furthermore, the automorphism group of $\mathbb{Q}[x]/m(x)$ has just two elements.

19 Cubic Extensions of the Rationals

In this section we take what may seem a modest step forward. We look at extending $\mathbb{Q}$ by the cube root of a rational number, and we consider $\mathbb{Q}[x]$ modulo an irreducible cubic. The story is more subtle than you might expect!

Let's start by studying the smallest field in $\mathbb{C}$ that contains $\sqrt[3]{2}$.

Example 19.1. Let $\mathbb{Q}[\sqrt[3]{2}]$ denote the smallest field in $\mathbb{C}$ that contains $\sqrt[3]{2}$. Clearly, $\mathbb{Q}[\sqrt[3]{2}]$ must also contain $(\sqrt[3]{2})^2 = \sqrt[3]{4}$. I claim that

$$\mathbb{Q}[\sqrt[3]{2}] = \left\{ a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q} \right\}.$$

As in the discussion of $\mathbb{Q}[\sqrt{i}]$, several field properties are immediate: associativity, commutativity, distributivity hold because they hold in $\mathbb{C}$ and the identity elements 0 and 1 are clearly in $\mathbb{Q}[\sqrt[3]{2}]$. The only thing we need to check is that addition and multiplication are indeed operations on $\mathbb{Q}[\sqrt[3]{2}]$ (in other words $\mathbb{Q}[\sqrt[3]{2}]$ is closed under $+$ and $*$) and that $\mathbb{Q}[\sqrt[3]{2}]$ is closed under taking inverses (additive and multiplicative). Closure under addition and taking additive inverses is clear.

$$\begin{aligned}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) + (r + s\sqrt[3]{2} + t\sqrt[3]{4}) &= (a + r) + (b + s)\sqrt[3]{2} + (c + t)\sqrt[3]{4} \\ -(a + b\sqrt[3]{2} + c\sqrt[3]{4}) &= -a + (-b)\sqrt[3]{2} + (-c)\sqrt[3]{4}\end{aligned}$$

Closure under multiplication, and the formula for computing products follows.

$$\begin{aligned}&(a + b\sqrt[3]{2} + c\sqrt[3]{4})(r + s\sqrt[3]{2} + t\sqrt[3]{4}) \\ &\qquad = (ar) + (as + br)\sqrt[3]{2} + (at + bs + cr)\sqrt[3]{4} + (bt + cs)\sqrt[3]{8} + ct\sqrt[3]{16} \\ &\qquad = (ar + 2bt + 2cs) + (as + br + 2ct)\sqrt[3]{2} + (at + bs + cr)\sqrt[3]{4}\end{aligned}$$

To establish closure under the multiplicative inverse, consider a, b, c as given and r, s, t as unkowns in the previous equation. We need to solve

$$(ar + 2bt + 2cs) + (as + br + 2ct)\sqrt[3]{2} + (at + bs + cr)\sqrt[3]{4} = 1 + 0\sqrt[3]{2} + 0\sqrt[3]{4}$$

This gives three equations in the three unkowns.

$$\begin{bmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{bmatrix} \begin{bmatrix} r \\ s \\ t \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

There is a unique solution provided the determinant is nonzero. The determinant is $a^3 + 2b^3 + 4c^3 + 8abc$.

It will be simpler to proceed if we modify the question. It should be clear that if I can invert $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ then I can invert any rational multiple of it. This allows us to reduce to the case $a+b\sqrt[3]{2}+c\sqrt[3]{4}$ for *mutually coprime integers* a, b, c. One of these integers must be odd.

- If a is odd, then $a^3 + 2b^3 + 4c^3 + 8abc$ is odd, and is therefore nonzero.
- If a is even, and b is odd then a^3 is a multiple of 8, and $a^3+2b^3+4c^3+8abc = 2(a^3/2 + b^2 + 2c^2 + 4abc)$ is divisible by 2 but not 4, so it cannot be 0.
- If a and b are both even and c is odd, then $a^3+2b^3+4c^3+8abc$ is a multiple of 4, but not of 8, so it is nonzero.

Thus we have shown that $a+b\sqrt[3]{2}+c\sqrt[3]{4}$ has an inverse in $\mathbb{Q}[\sqrt[3]{2}]$, which completes the proof that $\mathbb{Q}[\sqrt[3]{2}]$ is a field.

Now let's consider automorphisms of $\mathbb{Q}[\sqrt[3]{2}]$. Reflect for a minute to guess how many automorphisms there are.

Let φ be an automorphism of $\mathbb{Q}[\sqrt[3]{2}]$. Since $(\sqrt[3]{2})^3 = 2$, it must be the case that $\left(\varphi(\sqrt[3]{2})\right)^3 = 2$. You can try setting $\varphi(\sqrt[3]{2}) = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, then cubing setting the result equal to 2, and solving for a, b, c. Alternatively, let's think: we are working in the complex numbers, and we know that there are 3 cube roots of 2—the others are $\sqrt[3]{2}\omega$ and $\sqrt[3]{2}\omega^2$ where $\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Since $\mathbb{Q}[\sqrt[3]{2}]$ is contained in $\mathbb{R}$, these other square roots—which are not real—are not in $\mathbb{Q}[\sqrt[3]{2}]$. Thus the only possible value for $\varphi(\sqrt[3]{2})$ is $\sqrt[3]{2}$ and φ must be the identity map.

Finally, we note that there is an isomorphism:

$$\begin{aligned} \mathbb{Q}[x]/(x^3-2) &\longrightarrow \mathbb{Q}[\sqrt[3]{2}] \\ a + bx + cx^2 &\longmapsto a + b\sqrt[3]{2} + c\sqrt[3]{4} \end{aligned}$$

Check that this maps respects addition (easy) and multiplication.

More generally, we have the following.

Proposition 19.2. *Let B be a rational number that is not a perfect cube.*

(1) The set $\left\{a + b\sqrt[3]{B} + c\sqrt[3]{B^2} : a, b, c \in \mathbb{Q}\right\}$ is a field (it is denoted $\mathbb{Q}[\sqrt[3]{B}]$).

(2) The polynomial $x^3 - B$ is irreducible.

(3) The field $\mathbb{Q}[x]/(x^3 - B)$ is isomorphic to $\mathbb{Q}[\sqrt[3]{B}]$.

(4) The field $\mathbb{Q}[\sqrt[3]{B}]$ is isomorphic to $\mathbb{Q}[\sqrt[3]{a}]$ for some cube free integer *a.*

(5) The identity map is the only automorphism of $\mathbb{Q}[\sqrt[3]{B}]$.

The solution of a cubic polynomial

In the 16^{th} and 17^{th} centuries, there was a great deal of interest in deriving formulas, like the one for quadratics, for the solution of arbitrary cubic, quartic and higher degree equations. Several solutions of the cubic equation were discovered. I'm presenting one that is on the Wolfram MathWorld site and attributed to Vieta.

Consider the general cubic equation

$$x^3 + ax^2 + bx + c = 0$$

Substitute $x = y - \frac{a}{3}$, to get

$$\begin{aligned} 0 &= (y - \frac{a}{3})^3 + a(y - \frac{a}{3})^2 + b(y - \frac{a}{3}) + c \\ &= y^3 - ay^2 + \frac{a^2}{3}y - \frac{a^3}{27} + ay^2 - 2a\frac{a}{3}y + a\frac{a^2}{9} + by - b\frac{a}{3} + c \\ &= y^3 + \left(-\frac{a^2}{3} + b\right)y + \frac{2a^3}{27} - \frac{ab}{3} + c \end{aligned}$$

Setting $p = -\frac{a^2}{3} + b$ and $q = \frac{2a^3}{27} - \frac{ab}{3} + c$, we can write the last equation as $y^3 + py + q$. It should be clear that a solution to this equation (call it $\bar{y}(p, q)$, an expression for y in terms of p and q), can be transformed to a solution to the original equation, $\bar{x}$ a function of a, b and c, by a number of substitutions.

$$\bar{x} = \bar{y}(p, q) - \frac{a}{3} = \bar{y}(-\frac{a^2}{3} + b, \frac{2a^3}{27} - \frac{ab}{3} + c) - \frac{a}{3}$$

We proceed now to the solution of

$$y^3 + py + q$$

This is somewhat easier than the general equation since there is no y^2 term. We may assume p and q are both nonzero since $q = 0$ gives solutions $y = 0$ and $y = \pm\sqrt{p}$ and $p = 0$ is the case dealt with in Proposition 19.2.

The clever trick here is to substitute

$$y = z - \frac{p}{3z}$$

This may seem odd, but notice that clearing fractions gives $z^2 - 3yz - p = 0$. Thus for each y the quadratic formula gives two values of z such that $y = z - \frac{p}{3z}$—unless $9y^2 + 4p = 0$ in which case there is a single value of z. Note also that, since we assumed $p \neq 0$, the value of z cannot be zero.

We have

$$y^3 = z^3 - 3z^2\frac{p}{3z} + 3z\frac{p^2}{9z^2} - \frac{p^3}{27z^3}$$

so substituting $y = z - \frac{p}{3z}$ in $y^3 + py + q$ gives

$$\begin{aligned} y^3 + py + q &= z^3 - pz + \frac{p^2}{3z} - \frac{p^3}{27z^3} + pz - p\frac{p}{3z} + q \\ &= z^3 - \frac{p^3}{27z^3} + q \end{aligned}$$

Multiplying by z^3 and setting the expression equal to 0 gives

$$0 = z^6 + qz^3 - \frac{p^3}{27}$$

Now, as if by magic, we can use the quadratic formula to get two solutions for z^3.

$$R = \frac{1}{2}\left(-q + \sqrt{q^2 + \frac{4p^3}{27}}\right) \qquad S = \frac{1}{2}\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)$$

Let's call the discriminant of the quadratic $B = q^2 + \frac{4p^3}{27}$. The solutions for z are now

$$z = R^{\frac{1}{3}}, R^{\frac{1}{3}}\omega, R^{\frac{1}{3}}\omega^2, \quad \text{and} \quad S^{\frac{1}{3}}, S^{\frac{1}{3}}\omega, S^{\frac{1}{3}}\omega^2$$

Let's return to the original problem, finding solutions to $y^3 + py + q = 0$. There is a bit of a puzzle now—we seem to have 6 roots, $y = z - \frac{p}{3z}$ for the 6 different values of z above.

Some observations

- $RS = -p^3/27$ since the product of the roots of a quadratic is the constant term of the quadratic.
- If R is real (and therefore S is also real) then $R^{1/3}$ is unambiguously assigned the value of the unique real cube root of R (and similarly for $S^{1/3}$). Then $R^{\frac{1}{3}}S^{\frac{1}{3}} = -p/3$ the unique real root of $-p^3/27$.
- If R is not real (and therefore S is also not real), there is ambiguity in the notation $R^{\frac{1}{3}}$, there is no obvious way to identify a particular cube root. Fortunately, we can still choose $R^{\frac{1}{3}}$ and $S^{\frac{1}{3}}$ so that their product is $-p/3$. Take a moment to verify this claim.

Let's choose our cube roots $R^{1/3}$ and $S^{1/3}$ so that their product is $-p/3$. Then we get three solutions for y (not six):

$$\begin{aligned} R^{\frac{1}{3}} - \frac{p}{3R^{\frac{1}{3}}} &= R^{\frac{1}{3}} + S^{\frac{1}{3}} &&= S^{\frac{1}{3}} - \frac{p}{3S^{\frac{1}{3}}} \\ R^{\frac{1}{3}}\omega - \frac{p}{3R^{\frac{1}{3}}\omega} &= R^{\frac{1}{3}}\omega + S^{\frac{1}{3}}\omega^2 &&= S^{\frac{1}{3}}\omega^2 - \frac{p}{3S^{\frac{1}{3}}\omega^2} \\ R^{\frac{1}{3}}\omega^2 - \frac{p}{3R^{\frac{1}{3}}\omega^2} &= R^{\frac{1}{3}}\omega^2 + S^{\frac{1}{3}}\omega &&= S^{\frac{1}{3}}\omega - \frac{p}{3S^{\frac{1}{3}}\omega} \end{aligned}$$

The following problems treat each of the possibilities for a cubic polynomial with distinct roots: three rational roots, one rational and two complex roots, one rational and two irrational roots, one irrational and two complex roots, three irrational roots (there are actually two subcases here). Note: by irrational I mean irrational real, and by complex I mean complex nonreal.

Problems 19.3.

(1) Consider $x^3 - 7x + 6 = (x-1)(x-2)(x+3)$. Use the cubic formula to find the roots. Explain why you are surprised.

(2) Find the roots of $x^3 - 15x - 4$ using the cubic formula. [Hint: compute $(2+i)^3$.]

(3) Find the roots of

(4) Consider $m(x) = x^3 - 3x + 1 \in \mathbb{Q}[x]$.

- Show $x^3 - 3x + 1$ is irreducible.
- Find the roots using the cubic formula (they involve 9th roots of unity).
- For α any particular root, conclude that $m(x)$ factors completely in $\mathbb{Q}[\alpha]$. [Hint: For each root α show that $\alpha^2 - 2$ is also a root.]
- If α is one root, $\alpha^2 - 2$ is another. Find the third root in terms of α.

(5) Let $m(x) = x^3 - 6x - 6$.

- Find the roots of $m(x)$ using the cubic formula and show that exactly one root is real.
- Let α be the real root. Show the other roots are *not* contained in $\mathbb{Q}[\alpha]$.
- For this real root α show that $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt[3]{2}]$.

(6) Let $m(x) = x^3 - 15x - 10$.

- Find the roots of $m(x)$ using the cubic formula and show they are all real.
- Let α, β be two roots of $m(x)$. Show that $\beta \notin \mathbb{Q}(\alpha]$.

20 Finite Fields

We have already seen that $\mathbb{Z}/p$ is a field for p a prime. We will write this field as $\mathbb{F}_p$ to emphasize that it is a field. In this section we characterize finite fields completely by proving the following theorem.

Theorem 20.1. *Let K be a field with a finite number of elements.*

1) K has p^n elements where p is a prime.

2) There is an element $\alpha \in K$ whose powers $\alpha^1, \alpha^2, \ldots, \alpha^{p^n-1} = 1$ give all the nonzero elements of K. Consequently, K^* is cyclic of order $p^n - 1$.

3) K is isomorphic to $\mathbb{F}_p[x]/m(x)$ for some irreducible polynomial $m(x)$ of degree n over $\mathbb{F}_p$.

For any prime p and any positive integer n:

4) There exists a field with p^n elements.

5) Any two fields with p^n elements are isomorphic.

We use $\mathbb{F}_{p^n}$ to denote the unique field with p^n elements. The automorphism group of $\mathbb{F}_{p^n}$ satisfies:

(6) $\mathrm{Aut}(\mathbb{F}_{p^n})$ is generated by the Frobenius map, $\varphi(\beta) = \beta^p$.

(7) $\mathrm{Aut}(\mathbb{F}_{p^n}) \cong \mathbb{Z}/n$.

As a first step we prove

Proposition 20.2. *A finite field is a vector space over $\mathbb{F}_p$ for some prime p. Consequently, the number of elements of K is a power of p.*

Proof. Suppose that K is a finite field. Consider the additive subgroup generated by 1, i.e. 1, $1+1$, $1+1+1$. Let m be the smallest positive integer such that the sum of m 1's is 0. If m where composite, $m = ab$, then we would have

$$0 = \underbrace{1+1+1+\cdots+1+1}_{m \text{ terms}} = (\underbrace{1+1+\cdots+1}_{a \text{ terms}})(\underbrace{1+1+\cdots+1}_{b \text{ terms}})$$

The two factors on the right would then be zero-divisors, contradicting the assumption that K is a field. Thus m is in fact a prime, which we will now call p.

The set of elements $\underbrace{1+1+\cdots+1}_{a \text{ terms}}$ for $0 \le a < p$ is a subset of K that is closed under addition and multiplication, and it is routine to check that it is isomorphic to $\mathbb{F}_p$. So, we will think of K as containing $\mathbb{F}_p$.

From the field axioms we see immediately that K satisfies the axioms for a vector space over $\mathbb{F}_p$. For example: if $a \in \mathbb{F}_p$ and $\beta, \gamma \in K$ then $a(\beta+\gamma) = a\beta + a\gamma$ follows from the distributive law, but may be also considered as the property concerning scalar multiplication (by α) of a sum of vectors, $\beta+\gamma$. If the dimension of K over $\mathbb{F}_p$ is n then K has a basis $u_1, \ldots, u_n$ and the elements of K are $a_1u_1 + \ldots, a_nu_n$ for $a_i \in \mathbb{F}_p$. Thus K must have p^n elements. □

Definition 20.3. The prime p in the theorem is called the **characteristic** of the field.

Suppose that $q = p^n$ is the number of elements in K. By the field axioms, the set of nonzero elements of K is a group under multiplication. This group is denoted K^*. Recall that the **order** of an element α in a group G is the smallest positive integer r such that α^r is the identity, or infinity, if no such r exists. As an exercise, review the following properties from Theorem 1.24 and problems immediately following it.

Theorem Let α be an element of order r in a group G.

1) $\alpha^i = \alpha^j$ iff $i \equiv j \mod r$.

2) The order of α^i is r/d where $d = \gcd(i, r)$.

3) Let G be abelian. Let $\beta \in G$ have order s, coprime to $r = \text{ord}(\alpha)$. Then $\text{ord}(\alpha\beta) = rs$.

4) Let G be abelian. If $\alpha_1, \ldots, \alpha_n$ have orders $r_1, \ldots, r_n$ where the r_i are pairwise coprime, then $\text{ord}(\prod_{i=1}^n \alpha_i) = \prod_{i=1}^n r_i$.

Now we can establish item 2) of the Theorem.

Proposition 20.4. *The multiplicative group of a finite field is cyclic.*

Proof. Let K have p^n elements and let the prime factorization of $p^n - 1$ be $\prod_{i=1}^r q_i^{a_i}$. We will show that for each $i = 1 \ldots, r$ there is an element $b_i \in K^*$ of order $q_i^{a_i}$. Since the $q_i^{a_i}$ are coprime to each other, the Theorem above shows that the order of $b = \prod_{i=1}^r b_i$ is $\prod_{i=1}^r q_i^{a_i} = p^n - 1$. Thus b generates the multiplicative group of K.

Let $q^a || (p^n - 1)$. Let $t = (p^n - 1)/q^a$ and consider the set $S = \{\alpha^t : \alpha \in K^*\}$. For any $\beta \in S$ the polynomial $x^t - \beta$ has at most t roots so there can be at most

t elements of K whose tth power is β. Therefore the cardinality of S is at least $(p^n-1)/t = q^a$. On the other hand, everything in S is a root of $x^{q^a}-1$ since

$$(\alpha^t)^{q^a} = \alpha^{p^n-1} = 1$$

There can be only q^a roots of $x^{q^a}-1$, so S has at most q^a elements. This shows $|S| = q^a$. Similarly, at most q^{a-1} of the elements in S can be roots of $x^{q^{a-1}}-1$ so there must be at least $q^a - q^{a-1}$ elements of S whose order in K is q^a. This shows what we wanted: there is some element of K of order q^a.

□

Definition 20.5. An element of a finite field whose powers generate the nonzero elements of the field is called **primitive**.

The theorem says that every finite field has a primitive element. Furthermore, from the lemma, if α is primitive in a field of p^n elements then α^k is also primitive whenever k is coprime to p^n-1. Thus there are $\varphi(p^n-1)$ primitive elements, where φ is the Euler totient function ($\varphi(n)$ is the number of positive integers less than n and coprime to n).

I will state the next result as a corollary, but it is really a more basic result derived from Lagrange's theorem. Since K^* has p^n-1 elements, the order of any given element has to divide p^n-1. Thinking of this in terms of roots of polynomials, we have the following.

Corollary 20.6. *If K is a field with p^n elements then*

$$x^{p^n-1} - 1 = \prod_{\alpha \in K^*} (x-\alpha) \quad \textit{and,}$$
$$x^{p^n} - x = \prod_{\alpha \in K} (x-\alpha)$$

According to the following definition, the corollary shows that a field K of order p^n is a splitting field for $x^{p^n-1}-1$ and for $x^{p^n}-x$ over $\mathbb{F}_p$.

Definition 20.7. Let K be a field and let $f(x) \in K[x]$. A **splitting field** for $f(x)$ is a field K containing K such that

- $f(x)$ factors into linear factors in $K[x]$.
- Every element of K can be written as a polynomial in the roots of $f(x)$.

To prove item 3) of the Theorem we need to use the minimal polynomial of a primitive element (see Definition 15.5).

Proposition 20.8. *Let K be a finite field of p^n elements. Let β be any primitive element of K and let $M(x)$ be its minimal polynomial over $\mathbb{F}_p$. Then K is isomorphic to $\mathbb{F}_p[x]/M(x)$. In particular* $\deg M(x) = n$.

Proof. Let $\beta \in K$ be primitive and let its minimal polynomial be $M(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{F}_p$. We will show that $1, \beta, \ldots, \beta^{r-1}$ is a basis for K over $\mathbb{F}_p$. We first observe that $1, \beta, \ldots, \beta^{r-1}$ must be linearly independent over $\mathbb{F}_p$. Suppose on the contrary that some nontrivial linear combination is 0, $b_{r-1}\beta^{r-1} + \cdots + b_1\beta + b_0 = 0$. Let k be the largest positive integer such that $b_k \neq 0$. Then

$$\beta^k + \frac{b_{k-1}}{b_k} \cdots + \frac{b_1}{b_k}\beta + \frac{b_0}{b_0} = 0$$

This shows that β is a root of a polynomial over $\mathbb{F}_p$ of degree less than $\deg M(x)$, contradicting the minimality of $M(x)$.

Next we show that any power of β can be written as a linear combination of $1, \beta, \beta^2, \ldots, \beta^{r-1}$ with coefficients in $\mathbb{F}_p$. This is true trivially for β^i for $i = 0, \ldots, r-1$. Assume that for some $k \geq r$, each β^i for $i < k$ can be written as a linear combination as stated. Since $M(\beta) = 0$, $\beta^r = -a_{r-1}\beta^{r-1} - \cdots - a_1\beta - a_0$. Multiplying by β^{k-r} we can write β^k as a linear combination of lower powers of β. By the induction hypothesis these are all linear combinations of $1, \beta, \ldots, \beta^{r-1}$, so β^k is also. Since β is primitive, every nonzero element of K is a power of β. Thus we have shown that $1, \beta, \ldots, \beta^{r-1}$ span K as claimed.

Since K has p^n elements $r = n$. Furthermore the arithmetic on K is completely determined by its structure as a vector space and $\beta^n = -a_{n-1}\beta^{n-1} - \cdots - a_1\beta - a_0$. This is exactly the same structure that $\mathbb{F}_p[x]/M(x)$ has. In other words the map from $\mathbb{F}_p[x]/M(x)$ to K taking the class of x to β is an isomorphism. □

We can now prove existence and uniqueness for fields of prime power order. We will need the "Freshman's dream":

Proposition 20.9. *Let α, β be elements of a field of characteristic p. Then* $(\alpha + \beta)^p = \alpha^p + \beta^p$.

Proof. Expand $(\alpha + \beta)^p$ using the binomial theorem and we get terms like

$$\binom{p}{k}\alpha^k\beta^{p-k}$$

The binomial coefficient really means 1 added to itself $\binom{p}{k}$ times. Since p divides the binomial coefficient when $1 < k < p$ the coefficient is 0 unless $k = 0$ or $k = p$. That gives the result. □

Proposition 20.10. *For any prime power there exists a unique field of that order.*

Proof. Uniqueness: Let K and K' be two fields with p^n elements. Let α be a primitive element in K and let $M(x)$ be its minimal polynomial over $\mathbb{F}_p$. Since α is a root of $x^{p^n} - x$, Lemma 15.4 says that $M(x)$ divides $x^{p^n} - x$. By Corollary 20.6, $x^{p^n} - x$ factors into distinct linear factors in both K and K' so there must be a root of $M(x)$ in K'. By Proposition 20.8, both K and K' are isomorphic to $\mathbb{F}_p[x]/M(x)$ so they are isomorphic to each other.

Existence: By successively factoring $x^{p^n} - x$ and adjoining roots of a nonlinear irreducible factor, we can, after a finite number of steps, arrive at a field in which $x^{p^n} - x$ factors completely. I claim that the roots of $x^{p^n} - x$ form a field. Since the derivative of $x^{p^n} - x$ is -1, $x^{p^n} - x$ does not have multiple roots, so by the roots-factors theorem it has exactly p^n roots. Thus we have a field of p^n elements.

We need to show that the sum of two roots is a root, that the additive inverse of a root is a root, that the product of two roots is a root and that the multiplicative inverse of a root is a root. These are all trivial except for the case of the sum of two roots, which can be proved using the "Freshman's dream." □

The following example shows that there are many ways to construct a given field.

Example 20.11. Let $p = 3$. We can construct the field $\mathbb{F}_{3^2}$ by adjoining to $\mathbb{F}_3$ a root α of the irreducible polynomial $x^2 + 2x + 2$. You can check by hand that α is primitive in this field. If we had used $x^2 + 1$, which is also irreducible, we would get still get a field with 9 elements. But the root of $x^2 + 1$ will only have order 4 since $\alpha^2 = -1$ implies $\alpha^4 = 1$.

Definition 20.12. Let K be a finite field and let $p(x)$ be a polynomial over K. If $p(x)$ is irreducible and the class of x is primitive in $K[x]/p(x)$, then we say $p(x)$ is a **primitive polynomial**.

Example 20.13. We can construct $\mathbb{F}_{3^6}$ by adjoining to the field of the previous example a root β of the primitive polynomial (verified using Magma) $x^3 + \alpha x^2 + \alpha x + \alpha^3$ over $\mathbb{F}_{3^2}$. Elements of $\mathbb{F}_{3^6}$ are uniquely represented as polynomials in α and β whose degree in α is at most 1, and whose degree in β is at most 2.

We could also construct $\mathbb{F}_{3^6}$ by first constructing $\mathbb{F}_{3^3}$ by adjoining a root α' of the primitive polynomial $x^3 + 2x + 1$ and then adjoining a root β' of the primitive polynomial (verified using Magma) $x^2 + x + (\alpha')^7$ over $\mathbb{F}_{3^3}$.

Finally we could construct $\mathbb{F}_{3^6}$ directly by adjoining a root of the primitive polynomial $x^6 + 2x^4 + x^2 + 2x + 2$.

In each of these fields you can find a root of any one of the polynomials, and thereby define isomorphisms between the fields.

Now we consider the automorphism group of a finite field. Recall that any automorphism has to take 1 to itself, and must therefore fix the subfield $\mathbb{F}_p$.

Lemma 20.14. *Let $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^n})$. Let $\alpha \in \mathbb{F}_{p^n}$ have minimum polynomial $m(x)$. Then $\sigma(\alpha)$ is also a root of $m(x)$.*

Proof. Let $m(x) = x^d + m_{d-1}x^{d-1} + \cdots + m_0$ be the mimimum polynomial for α. Each $m_i \in \mathbb{F}_p$ so

$$\begin{aligned}\sigma\Big(m(\alpha)\Big) &= \sum_{i=1}^{n} \sigma(m_i\alpha) \\ &= \sum_{i=1}^{n} m_i\sigma(\alpha) \\ &= m(\sigma(\alpha))\end{aligned}$$

Since $m(\alpha) = 0$ we have $m(\sigma(\alpha))$ is also 0. □

Proposition 20.15. *The automorphism group of $\mathbb{F}_{p^n}$ is cyclic of order n, generated by the Frobenius map $\varphi : \alpha \longmapsto \alpha^p$.*

Proof. The Frobenius map respects addition, by the Freshman's dream, and it clearly respects multiplication: $\varphi(\alpha\beta) = (\alpha\beta)^p = \alpha^p\beta^p = \varphi(\alpha)\varphi(\beta)$. Thus φ is a homomorphism of fields. Since a homomorphism of fields must be injective, and since an injective function on a finite set is also surjective, we conclude that φ is an automorphism.

Repeatedly composing the Frobenius with itself gives other automorphims and one can inductively establish the formula: $\varphi^t(\alpha) = \alpha^{p^t}$. Since $\mathbb{F}_{p^n}^*$ has order $p^n - 1$ we have for $\alpha \neq 0$, $\varphi^n(\alpha) = \alpha^{p^n} = \alpha^{p^n-1} * \alpha = \alpha$. Thus φ^n is the identity map. I claim no lower power of φ is the identity map. Suppose that φ^r is the identity automorphism and let η be primitive in $\mathbb{F}_{p^n}$. Then $\eta = \varphi^r(\eta) = \eta^{p^r}$, so $\eta^{p^r-1} = 1$. Since η is primitive it has order $p^n - 1$, so we see $r \geq n$ as claimed.

We need to show that there are no other automorphisms of $\mathbb{F}_{p^n}$. Let η be primitive, and let $m(x) = x^n + m_{n-1}x^{n-1} + \cdots + m_0$ be its mimimum polynomial. The lemma showed that $\varphi^r(\eta) = \eta^{p^r}$ is another root of $m(x)$. Since η is primitive, $\eta, \ldots, \eta^{p^{n-1}}$ are all distinct and they form the complete set of roots of $m(x)$. Any automorphims σ must take η to one of these other roots of $m(x)$. Since the action of σ on η determines σ completely, if $\sigma(\eta) = \eta^{p^r}$ then $\sigma = \varphi^r$.

In conclusion $\mathrm{Aut}(\mathbb{F}_{p^n})$ is cyclic of order n, and is generated by φ. □

Problems 20.16.

(1) Factor $x^{15} - 1$ over $\mathbb{F}_2$. Construct $\mathbb{F}_{16}$ in three ways as a degree 4 extension of $\mathbb{F}_2$ and show isomorphisms between the three representations.

(2) Here is some Sage code to use to study the field $\mathbb{F}_{81}$.

```
F3 = FiniteField(3)
P.<x> = PolynomialRing(F3)
p = x^81 -x
p.factor()
m = x^4+x+2
F81.<a> = FiniteField(81,modulus=x^4+x+2)
```

- The polynomials $x^2 + 2x + 1$ and $x^2 + x + 2$ are both irreducible over $\mathbb{F}_3$. Can you construct $\mathbb{F}_{81}$ by using one of these polynomials and then the other?
- In Sage, use $m(x) = x^4 + x + 2$ and $r(x) = x^4 + 2x + 2$ to construct two versions of $\mathbb{F}_{81}$. Using a brute force search, find a root of $m(x)$ in the second field and a root of $r(x)$ in the first field. These give isomorphisms between the two fields. Check by hand that the composition is the identity.
- Factor $x^{80} - 1$ over $\mathbb{F}_3$. For each irreducible factor $a(x)$, find the roots of $a(x)$ in $\mathbb{F}_3[x]/m(x)$.

(3) The field of 64 elements.

- The polynomials $m(x) = x^6 + x + 1$ and $r(x) = x^6 + x^5 + x^4 + x + 1$ are both irreducible over $\mathbb{F}_2$. In Sage, use $m(x)$ and $r(x)$ to construct two versions of $\mathbb{F}_{64}$. Using a brute force search, find a root of $m(x)$ in the second field and a root of $r(x)$ in the first field. These give isomorphisms between the two fields. Check by hand that the composition is the identity.
- Factor $x^{63} - 1$ over $\mathbb{F}_2$. For each irreducible factor $a(x)$, find the roots of $a(x)$ in $\mathbb{F}_2[x]/m(x)$. Use Sage, but also use your understanding of the theory. Using Sage, use $m(x)$ and $r(x)$ to construct two versions of $\mathbb{F}_{64}$ in Sage. Using a brute force search, find a root of $m(x)$ in the second field and a root of $r(x)$ in the first field. These give isomorphisms between the two fields. Check that the composition is the identity.
- Factor $x^{63} - 1$ over $\mathbb{F}_2$. Find the roots of each of the irreducibles in $\mathbb{F}_2[x]/m(x)$. Use Sage, but also use your understanding of the theory.

```
L= (x^63-1).factor()
[l[0] for l in L if l[0].is_primitive()]
```

- The field $\mathbb{F}_{64}$ can also be constructed as an extension of $\mathbb{F}_4$. Construct $\mathbb{F}_4$, then factor $x^{63}-1$ in $\mathbb{F}_4[x]$. Choose one of the factors of degree 3 to construct $\mathbb{F}_{64}$. The following code will show how Sage treats elements of this new object. It appears that there is no way in Sage to create a "field;" the code below only creates a ring. In particular FF.list() will not work.

```
FF.<b> = F4.extension(x^3+a)
[b^i for i in [1..64] ]
```

- Now create $\mathbb{F}_8$ using an irreducible polynomial of degree 3 over $\mathbb{F}_2$, then factor $x^{63}-1$, then create $\mathbb{F}_{64}$ using an irreducible polynomial of degree 2 in $\mathbb{F}_8[x]$.
- The polynomials $m(x) = x^6 + x + 1$ and $r(x) = x^6 + x^5 + x^4 + x + 1$ are both irreducible over $\mathbb{F}_2$.

(4) Make a table showing the possible orders and the number of elements of each order for $\mathbb{F}_{64}$, $\mathbb{F}_{128}$, and $\mathbb{F}_{256}$.

(5) Prove that if $r|n$ then $\mathbb{F}_{q^r}$ is a subfield of $\mathbb{F}_{q^n}$.

(6) For a given prime p, let $I(d)$ be the set of irreducible polynomials of degree d over $\mathbb{F}_p$. Show that for $n > 0$,

$$\prod_{d|n} \prod_{f \in I(d)} f = x^{p^n} - x$$

(7) Show that for any $\alpha \in \mathbb{F}_q$,

$$1 + \alpha + \alpha^2 + \alpha^3 + \cdots + \alpha^{q-2} = \begin{cases} 1 \text{ if } \alpha = 0 \\ -1 \text{ if } \alpha = 1 \\ 0 \text{ otherwise} \end{cases}$$

21 Problems

Problem 1: The field $\mathbb{F}_{81}$.

(a) In Sage, use $m(x) = x^4 + x + 2$ and $r(x) = x^4 + 2x + 2$ to construct two versions of $\mathbb{F}_{81}$. Using a brute force search, find a root of $m(x)$ in the second field and a root of $r(x)$ in the first field. These give isomorphisms between the two fields. Check by hand that each composition is an automorphism of the appropriate version of $\mathbb{F}_{81}$.

(b) Factor $x^{80} - 1$ over $\mathbb{F}_3$. For each irreducible factor $a(x)$, find the roots of $a(x)$ in $\mathbb{F}_3[x]/m(x)$.

Problem 2: The field of 64 elements.

(a) The polynomials $m(x) = x^6 + x + 1$ and $r(x) = x^6 + x^5 + x^4 + x + 1$ are both irreducible over $\mathbb{F}_2$. In Sage, use $m(x)$ and $r(x)$ to construct two versions of $\mathbb{F}_{64}$. Using a brute force search, find a root of $m(x)$ in the second field and a root of $r(x)$ in the first field. These give isomorphisms between the two fields. Check by hand that each composition of the two isomorphisms is an automorphism of the appropriate version of the field.

(b) Factor $x^{63} - 1$ over $\mathbb{F}_2$. For each irreducible factor $a(x)$, find the roots of $a(x)$ in $\mathbb{F}_2[x]/m(x)$. Use Sage, but also use your understanding of the theory.

(c) The field $\mathbb{F}_{64}$ can also be constructed as an extension of $\mathbb{F}_4$. Construct $\mathbb{F}_4$, then factor $x^{63} - 1$ in $\mathbb{F}_4[x]$. Choose one of the factors of degree 3 to construct $\mathbb{F}_{64}$. The following code will show how Sage treats elements of this new object. It appears that there is no way in Sage to create a "field;" the code below only creates a ring. In particular FF.list() will not work.

```
FF.<b> = F4.extension(x^3+a)
[b^i for i in [1..64] ]
```

(d) Now create $\mathbb{F}_8$ using an irreducible polynomial of degree 3 over $\mathbb{F}_2$, then factor $x^{63} - 1$, then create $\mathbb{F}_{64}$ using an irreducible polynomial of degree 2 in $\mathbb{F}_8[x]$.

Problem 3: Make a table showing the possible multiplicative orders and the number of elements of each order for $\mathbb{F}_{64}$, $\mathbb{F}_{128}$, and $\mathbb{F}_{256}$. Relate this information to subfields.

Problem 4: Let $n > m$ be positive integers and $d = \gcd(n, m)$. Show that the intersection of $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$ is $\mathbb{F}_{p^d}$ as follows.

(a) Show that the remainder $x^n - 1$ divided by $x^m - 1$ is $x^r - 1$ where r is the remainder when n is divided by m.

(b) Show that the gcd of $x^n - 1$ and $x^m - 1$ is $x^d - 1$.

(c) Use the fact that the set of roots of $x^{p^n - 1} - 1$ is exactly the nonzero elements of $\mathbb{F}_{p^n}$.

(d) Conclude that $\mathbb{F}_{p^d}$ is a subfield of $\mathbb{F}_{p^n}$ iff d divides n.

Problem 3: Make a table showing the possible multiplicative orders and the number of elements of each order for $\mathbb{F}_{64}$, $\mathbb{F}_{128}$, and $\mathbb{F}_{256}$. Relate this information to subfields.

Problem 4: Let $n > m$ be positive integers and $d = \gcd(n, m)$. Show that the intersection of $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$ is $\mathbb{F}_{p^d}$ as follows.

(a) Show that the remainder $x^n - 1$ divided by $x^m - 1$ is $x^r - 1$ where r is the remainder when n is divided by m.

(b) Show that the gcd of $x^n - 1$ and $x^m - 1$ is $x^d - 1$.

(c) Use the fact that the set of roots of $x^{p^n-1} - 1$ is exactly the nonzero elements of $\mathbb{F}_{p^n}$.

(d) Conclude that $\mathbb{F}_{p^d}$ is a subfield of $\mathbb{F}_{p^n}$ iff d divides n.

Problem 4: Irreducible polynomials over $\mathbb{F}_p$. Suppose you have formulas for the number of irreducible monic polynomials of degree m over $\mathbb{F}_p$ for each $m < n$. Using some combinatorial arguments you can then compute the number of monic reducible polynomials of degree n. Subtracting this from the number of monic polynomials of degree n yields the number of monic irreducible polynomials of degree n.

(a) Show that the number of monic irreducible quadratics over $\mathbb{F}_p$ is $(p^2 - p)/2$.

(b) Show that the number of monic irreducible cubics over $\mathbb{F}_p$ is $(p^3 - p)/3$.

(c) You might want to guess at a general formula. A different counting method yields the result more easily than the one above. Try this if you want, noting:

- For $a \in \mathbb{F}_{p^n}$, a is in no proper subfield iff the minimal polynomial for a has degree n.
- Each monic irreducible of degree n has n distinct roots in $\mathbb{F}_{p^n}$.

Problem 1: Let F be a field of characteristic $p \neq 0$ and let $a \in F$.

(a) Show that the polynomial $f = x^p - x - a \in F[x]$ is separable.

(b) Show that either f splits or it is irreducible. Break this into two steps:

- If f possesses a root in F then f already splits over F.
- If f is reducible over F then it has a root in F.

(c) Suppose that f is irreducible. What is the Galois group of the splitting field of f over F?

Hint: In **(b)**, suppose α is a root of f in F, and consider the element $\alpha + \gamma$ with $\gamma \in \mathbb{F}_p$ as a further candidate for a root. Then assume a factorization $f = gh$ and look at one of the coefficients of g.

Problem 2: (150 pts.) Finite fields.

(a) Prove, from minimal assumptions, that the Frobenius map $\varphi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ defined by $\varphi(x) = x^p$ is an isomorphism and that its fixed field is $\mathbb{F}_p$.

(b) Prove that the Galois group of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is isomorphic to $\mathbb{Z}_n$.

(c) Show the Galois correspondence between subfields of $\mathbb{F}_{p^{18}}$ and subgroups of $\mathrm{Gal}(\mathbb{F}_{p^{18}}/\mathbb{F}_p)$.

(d) Identify the intersection of the fields $\mathbb{F}_{p^d}$ and $\mathbb{F}_{p^r}$, and the join of these fields, $\mathbb{F}_{p^r}\mathbb{F}_{p^n}$. Briefly justify your answer.

22 Field Extensions: Algebraic and Transcendental

Definition 22.1. Let E be a field and let F be a subset of E such that F is a field using the operations $*_F$ and $+_F$. We say F is a *subfield* of E and E is an *extension field* of F. We will write $F \leq E$.

Observe that if $F \leq K$ then K is a vector space over F. We write $[K : F]$ for the dimension.

Definition 22.2. For $F \leq K$ and $\alpha \in K$, let $F[\alpha]$ be the intersection of all rings containing F and α. Let $F(\alpha)$ be the intersection of all fields containing F and α. Similarly for $S \subseteq K$ let $F[S]$ be the intersection of all rings containing S and $F(S)$ the intersection of all fields containing S.

It is easy to check if we have subfields $F_i \leq K$ for each i in some set I (not necessarily finite) then the intersection $\bigcap_{i \in I} F_i$ is a subfield of K. Similarly we can show that the intersection of a set of subrings R_i of some ring S is a subring of S. Thus $F[S]$ is a ring and $F(S)$ is a field.

Proposition 22.3. *$F[\alpha]$ is the set of all polynomials in α with coefficients from F.*

$$F[\alpha] = \left\{ c_0 + c_1\alpha + \cdots + c_d\alpha^d : c_i \in F, d \in \mathbb{N}_0 \right\}$$

$F(\alpha)$ consists of all quotients of elements in $F[\alpha]$ (with nonzero denominator).

Let $\varphi : F \longrightarrow K$ be a homomorphism of fields. Recall that φ must be injective, so φ is isomorphic to some subfield of K. The following is just a special case of the universal property of polynomial rings.

Proposition 22.4. *The universal property of $F[x]$. Let $\varphi : F \longrightarrow K$ and let α be an element of K. There is a unique homomorphism from $F[x]$ to K taking x to α.*

We will call the map of the proposition "the natural map extending φ taking x to α."

When the map of the proposition is not injective, Proposition 10.4 says that the kernel is generated by a polynomial $m(x)$. We then have an injective homomorphism $F[x]/m(x) \longrightarrow K$. Since K is a field it has no zero divisors, and therefore $F[x]/m(x)$ has no zero divisors. Theorem 9.3 (and Corollay 9.4) imply that $F[x]/m(x)$ must be a field and $m(x)$ must be irreducible.

Definition 22.5. Let F be a subfield of K and let φ be the inclusion map $F \longrightarrow K$. We say that $\alpha \in K$ is *transcendental* over F when the natural map $F[x] \longrightarrow K$ taking x to α is injective. We say α is *algebraic* over F when the natural map

taking x to α is not injective. We call the monic polynomial generating the kernel the *minimal polynomial* of α and we denote it by $m_\alpha(x)$.

We say that K is *an algebraic extension* of F (or simply K is *algebraic* over F) when each element of K is algebraic over F. Otherwise K is transcendental over F.

Proposition 22.6. *For $\beta \in K$ algebraic over F, $F[x]/m_\beta(x) \cong F[\beta] = F(\beta)$.*

Proof. From the discussion before the definition, we know $F[x]/m_\beta(x)$ can have no zero divisors, so it must be a field. There is an injective homomorphism $F[x]/m_\beta(x) \longrightarrow K$. The image is $F[\beta]$, which is therefore isomorphic to Since $F[x]/m_\beta(x)$, and consequently it must also be a subfield of K. Thus $F[\beta] = F(\beta)$. □

Proposition 22.7. *If K contains some transcendental element over F then $[K : F]$ is infinite. Conversely, if K is finite dimensional over F then every element of K is algebraic over F.*

Proof. Let $\alpha \in K$ be transcendental over F. Then $F[\alpha]$ is isomorphic to $F[x]$ and it is already infinite dimensional over F. □

Proposition 22.8. *Let $F \leq D \leq E$ and $\beta \in E$. Let $m(x)$ be the min poly of β over F and $p(x) \in D[x]$ the min poly over D. Then $p(x) \mid m(x)$.*

Proposition 22.9 (Dimension)**.** $[K : E][E : F] = [K : F]$

Corollary 22.10. *If $[E : F] = n$ then each $\beta \in E$ is algebraic of some degree d dividing n.*

Proof. □

Here is how to find the minimum polynomial of $\beta \in K$ over F. Consider powers of β, $1, \beta, \beta^2, \ldots$. Find the smallest d such that they are linearly dependendent over F. The linear dependency gives the minimal polynomial of β (or some constant multiple of it).

Any finite extension is algebraic, so if we take two finite extensions E/F (this is shorthand we will use to say E is an extension of F) and K/E then since dimensions multiply K/F is also finite dimensional and therefore algebraic.

Proposition 22.11 (Transitivity of algebraic extensions)**.** *If $F \leq E$ and $E \leq K$ are both algebraic extensions then so is $F \leq K$. Conversely if $F \leq K$ is algebraic, so are the extensions $F \leq E$ and $E \leq K$.*

Proof. □

23 Splitting Fields

Definition 23.1. We say $f(x)$ splits in F when it factors into linear factors.

Suppose $f(x)$ does not split in F. Let $p(x)$ be an irreducible factor of $f(x)$. We may form the extension of F, $F[x]/p(x)$. In this extension the class of x is a root of $p(x)$. We will call the construction of this new field "adjoining a root of $f(x)$ (or $p(x)$) to F".

Example 23.2. $x^3 - 3x + 1 \in \mathbb{Q}[x]$. Factor, after adjoining a root.

Example 23.3. $x^3 - 2 \in \mathbb{Q}[x]$. Factor, after adjoining a root. Factor the remaining irreducible factor.

Here is a subtle issue. Suppose $F \cong \tilde{F}$ and therefore $F[x] \cong \tilde{F}[x]$. Let $f(x) \in F[x]$ be irreducible and let $\tilde{f}(x)$ be the corresponding irreducible in $\tilde{F}[x]$ under the isomorphism. Then $F[x]/f(x) \cong \tilde{F}[x]/\tilde{f}(x)$. Now supppose that E is an extension of F containing a root α of $f(x)$ and that $\tilde{E}$ is an extension of $\tilde{F}$ containing a root $\tilde{\alpha}$ of $\tilde{f}(x)$. I'm not assuming anything additional about E and $\tilde{E}$ (in particular, no assumed isomorphism between the two). We have $F(\alpha)$ (the subfield of E) is isomorphic to $F[x]/f(x)$ which is isomorphic to $\tilde{F}[x]/\tilde{f}[x]$ and this is isomorphic to $\tilde{F}(\tilde{\alpha})$. So the two subfields $F(\alpha)$ (in E) and $\tilde{F}(\tilde{\alpha})$ (in $\tilde{E}$) are isomorphic.

Definition 23.4. Let $f(x) \in F[x]$. A *splitting field* of $f(x)$ is an extension of F in which $f(x)$ splits and for which $f(x)$ does not split in any proper subfield.

Theorem 23.5 (Splitting Field)**.** *A splitting field of $f(x) \in F[x]$ exists and any two such fields are isomorphic.*

Proof. □

Corollary 23.6. *The splitting field for $f(x) \in F[x]$ of degree n has dimension at most $n!$ over F.*

Proof. □

Think about the formulas for the solution of a cubic relative to the question of computing the splitting field of a cubic.

24 Algebraic Closure

Proposition 24.1. *For a field C the following are equivalent.*

(1) Each $f(x) \in C[x]$ has a root.

(2) Each $f(x) \in C[x]$ splits in $C[x]$

(3) Each irreducible $f(x) \in C[x]$ is linear.

(4) C has no proper algebraic extensions.

Definition 24.2. A field satisfying the properties of the proposition is called *algebraically closed*.

Proposition 24.3. *Let C be an algebraic extension of F such that every polynomial in $F[x]$ splits in C. Then C is algebraically closed.*

Proof. Let $c(x) \in C[x]$ be irreducible and let $D = C[x]/c(x)$. The D is algebraic over C and C is algebraic over F, so by transitivity, D is algebraic over F. Thus α is algebraic over F. Let $f(x) \in F[x]$ be the minimal polynomial of α. Since $f(x)$ splits in $C[x]$, all of its roots are in C, so $\alpha \in C$. Thus $c(x)$ must be linear (so $D = C$). □

Theorem 24.4 (Algebraic Closure)**.** *For any field F there is a field $C \geq F$ that is algebraic over F and is algebraically closed. Any two such fields are isomorphic.*

We will show that the complex field $\mathbb{C}$ is algebraically closed in Theorem **??**.

The algebraic closure of F is usually denoted $\overline{F}$. In Sage QQbar is the algebraic closure of $\mathbb{Q}$.

25 Separable Extensions

Proposition 25.1. *A polynomial $f(x) \in \mathbb{C}[x]$ has repeated roots iff* $\gcd(f, f') \neq 1$.

Proof. If there is some $a \in \mathbb{C}$ such that $f(x) = (x-a)^2 g(x)$ then $(x-a)$ divides $f'(x)$ (check!). On the other hand, if $f(x) = (x-a)g(x)$ and $(x-a)$ does not divide $g(x)$ then $(x-a)$ does not divide $f'(x)$. Consequently, if $f(x)$ has no repeated roots then $gcd(f(x), f'(x)) = 1$. □

We want to extend this to to arbitrary fields.

Definition 25.2. An irreducible polynomial $f(x)$ of degree d in $F[x]$ that has d distinct roots in its splitting field is called *separable*. An arbitrary polynomial is separable when each of its irreducible factors is.

Definition 25.3. Derivative of f

Example 25.4. Over finite field.

Proposition 25.5 (Properties of the derivative)**.**

Proof. □

The repeated roots theorem is valid for any field.

Theorem 25.6. *A polynomial $f(x) \in F[x]$ has repeated roots iff* $\gcd(f, f') \neq 1$.

Proposition 25.7. *For $f(x)$ irreducible: $f(x)$ is separable iff $f' \neq 0$.*

Proof. □

Corollary 25.8. *Every polynomial over a field of characteristic 0 is separable.*

Proof. □

Corollary 25.9. *Every polynomial in $\mathbb{F}_q[x]$ is separable.*

Proof. □

Definition 25.10. separable extension, perfect,

The classic example of an inseparable polynomial.

Example 25.11.

Discussion: Suppose that $\varphi : F \longrightarrow E$ is an embedding of F into C, the algebraic closure of E. Then there is an extension of φ to an embedding of E into C. In particular for $E = F[\alpha]$ we may (and must!) take α to a root of $m_\alpha(x)$, the minimal polynomial of α in $F[x]$.

Theorem 25.12. *Let E/F be an extension of dimension n and let C be an algebraic closure of F. There are at most n distinct embeddings of E into C and there are exactly n embeddings iff E is separable over F.*

Proof. □

Theorem 25.13. *Primitive Element*

Proof. □

26 Normal Field Extensions

Definition 26.1. A field extension $F \leq E$ satisfying the equivalent conditions in the following theorem is called *normal*.

Theorem 26.2 (Normal Extension)**.** *Let $F \leq E \leq C$ be field extensions with E algebraic over F and C the algebraic closure of E. The following are equivalent.*

(1) Each irreducible $m(x) \in F[x]$ that has a root in E splits in E.

(2) E is the splitting field of some set of polynomials.

(3) Every embedding of E into C that fixes F has image E, and is therefore an automorphism of E.

Proof. We prove the theorem just for the case where $[E : F]$ is finite. The infinite dimensional case requires some modification of the final step of this proof, esentially reducing to the case of a finite dimensional extension.

(3) $\implies$ (1). Let $m(x)$ be an irreducible in $F[x]$ having a root α in E. Let $\beta \in C$ be another root of $m(x)$; we will show $\beta \in E$. Since β is arbitrary, $m(x)$ splits in E.

We know $F[\alpha] \cong F[\beta]$, because both are isomorphic to $F[x]/m(x)$. Since E is an algebraic extension of F this isomorphism extends to an embedding of E in C. By assumption, the image is E, so in particular $\beta \in E$. (This proof works for infinite extensions.)

(1) $\implies$ (2). Let $\alpha_1, \ldots \alpha_r$ be such that $E = F[\alpha_1, \ldots, \alpha_r]$. (Here we use finiteness.) Let $m_i(x)$ be the minimal polynomial of α_i over F. By assumption, $m_i(x)$ splits in E, so E contains the splitting field of $m(x) = \prod_{i=1}^{r} m_i(x)$. On the other hand the splitting field of $m(x)$ contains all the α_i, so it contains the field generated by them, $F[\alpha_1, \ldots, \alpha_r] = E$. Thus E is the splitting field of $m(x)$. (Thus in the finite dimensional case, E is the splitting field of a single polynomial.)

(2) $\implies$ (3) (Assuming finite). Suppose that E is the splitting field of $m(x)$, and let $\alpha_1, \ldots, \alpha_r$ be the roots of $m(x)$. Let $\tau : E \longrightarrow C$ be an embedding of E into C that fixes F. We have seen that τ must take roots of $m(x)$ to roots of $m(x)$. The roots generate E, so $\tau(E) \subseteq E$. Since τ is an isomorphism onto its image the dimension of $\tau(E)$ over F is equal to $[E : F]$. Thus $\tau(E) = E$. □

Corollary 26.3. *Let $[E : F] = n$. E/F is normal and separable over F iff $|\mathrm{Aut}(E/F)| = n$*

Proof. $\implies$ By separability, there are exactly n embeddings of E into C fixing F. By normality, these must all be automorphisms of E. Thus $|\mathrm{Aut}(E/F)| = n$.

$\Longleftarrow$ By the the theorem on separability, there are at most n embeddings of E into C that fix F, and the number of embeddings is n iff E is separable over F. Consequently, if $|\mathrm{Aut}(E/F)| = n$, then E must be separable and the automorphisms of E fixing F account for all the embeddings of E into C fixing F. Thus E is normal. □

Definition 26.4. When E is normal and separable over F, the extension E/F is called *Galois*. In this case, it is common to call the automorphism group $\mathrm{Aut}(E/F)$ the *Galois group* and write $\mathrm{Gal}(E/F)$. (Some authors use $\mathrm{Gal}(E/F)$ for arbitrary algebraic extensions.)

Recall that we showed that for separable extensions we have transitivity. In fact, for $F \leq D \leq E$, E/F is separable iff each of E/D and D/F is separable. Neither implication is true for normality, but we do have the following weaker property.

Proposition 26.5. *If E/F is normal then E/D is normal for any $F \leq D \leq E$.*

Proof. Suppose E/F is normal. By the normality theorem, there is some set of polynomials, $S \subseteq F[x]$, for which E is the smallest field containing F in which polynomials in S all split. Since $S \subseteq D[x]$, E is the also the smallest field containing D in which the polynomials in S split. So E is normal over D. □

Here is an immediate consequence.

Corollary 26.6. *Let E/F be Galois. Then E is Galois over any intermediate extension.*

27 Galois main theorem

Let E/F be an algebraic field extension and let $G = \mathrm{Aut}(E/F)$. We now consider the relationship between subfields of E containing F and subgroups of G. Define the *fixed field* functor $\mathcal{F}$ and the *fixing group* functor $\mathcal{G}$ by

$$\mathcal{F}(H) = \{x \in E : \sigma(x) = x \,\forall\, \sigma \in H\}$$
$$\mathcal{G}(D) = \{\sigma \in G : \sigma(x) = x \,\forall\, x \in D\}$$

Please verify that for D a field with $F \leq D \leq E$, $\mathcal{G}(D)$, which we call the fixing group of D, is a subgroup of G (it is closed under the operation of composition and taking inverses). Similarly, $\mathcal{F}(H)$, which we call the fixed field of H, is indeed a field (closure for both addition and multiplication, and both additive and multiplicative inversion). The following proposition characterizes these functors and their relationship to each other.

Theorem 27.1. *Let E/F be an algebraic extension and $\mathcal{F}$ and $\mathcal{G}$ the operations defined above.*

(1) $\mathcal{G}$ and $\mathcal{F}$ are inclusion reversing.

(2) $\mathcal{FG}$ and $\mathcal{GF}$ are increasing.

(3) $\mathcal{FGF} = \mathcal{F}$ and $\mathcal{GFG} = \mathcal{G}$.

Proof. Let $F \leq D \leq D' \leq E$. Any $\sigma \in \mathcal{G}(D')$ fixes everything in D', so it must fix each element of D. Thus $\mathcal{G}(D) \geq \mathcal{G}(D')$. Similarly one shows that for $H \leq H' \leq G$, $\mathcal{F}(H) \geq \mathcal{F}(H')$.

Next we want to show that $\mathcal{FG}(D) \geq D$. This is clear: since everything in $\mathcal{G}(D)$ fixes D, the fixed field of $\mathcal{G}(D)$ contains D. The analogous result for $\mathcal{GF}$ is similar.

Applying $\mathcal{G}$ to the result of the previous paragraph, and using item (1), $\mathcal{G}(\mathcal{FG}(D)) \leq \mathcal{G}(D)$. On the other hand, since $\mathcal{GF}$ is increasing, when it is applied to $\mathcal{G}(D)$ we get $\mathcal{GF}(\mathcal{G}(D)) \geq \mathcal{G}(D)$. Thus $\mathcal{GFG} = \mathcal{G}$, and by analogous argument $\mathcal{FGF} = \mathcal{F}$. □

The most useful approach to studying the relationship between subfields and subgroups of field automorphisms is to restrict to Galois extensions. In fact, this is not a restrictive restriction. If one wants to study the arbitrary extension E/F, one can first tease apart E/F into a separable part E_s/F and purely inseparable part E_i/F. The purely inseparable part has a trivial automorphism group and $\mathrm{Aut}(E/F) \cong \mathrm{Aut}(E_s/F)$. Thus we reduce to separable extensions. Now, assuming E/F is separable, one can form the normal closure E' of E and get information about $\mathrm{Aut}(E/F)$ from $\mathrm{Aut}(E'/F)$. The details may be found in many standard graduate algebra texts.

We will focus on E/F Galois, but first, here is the key result used in establishing the main theorem of Galois theory. I found this proof in Lang's *Algebra* and he atributes it to Artin.

Proposition 27.2. *Let E be any field and let G be a subgroup of* $\mathrm{Aut}(E)$. *Let $F = \{x \in E : \sigma(x) = x \, \forall \, \sigma \in G\}$.*

(1) E/F is Galois.

(2) $\mathrm{Gal}(E/F) = G$.

(3) $[E : F] = |\mathrm{Gal}(E/F)| = |G|$.

Proof. Let $\alpha \in E$ and let $m(x)$ be the minimal polynomial for α. We will show $m(x)$ factors completely over E with distinct roots. Since α is arbitrary, E/F is Galois.

Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$ be the orbit of α under G, so each $\alpha_i \in E$. Let $\sigma_i \in G$ be such that $\sigma_i(\alpha) = \alpha_i$. Each $\sigma \in G$ fixes F, so $\sigma(m(x)) = m(x)$. (Here we are implicitly extending σ to an automorphism of $E[x]$ by applying σ to each coefficient.) Furthermore, we have

$$0 = \sigma(m(\alpha)) = m(\sigma(\alpha))$$

so each α_i is a root of $m(x)$. Consequently, $\prod_{i=1}^{r}(x - \alpha_i)$ divides $m(x)$.

On the other hand, each $\sigma \in G$ permutes the α_i: because $\sigma(\alpha_i) = \sigma(\sigma_i(\alpha)) \in \mathrm{orb}(\alpha) = \{\alpha_1, \ldots, \alpha_r\}$. (Of course $\sigma(\alpha_i) = \sigma(\alpha_j)$ is only true for $i = j$ since σ is injective.) Now we have

$$\sigma\Big(\prod_{i=1}^{r}(x - \alpha_i)\Big) = \prod_{i=1}^{r}\sigma(x - \alpha_i) = \prod_{i=1}^{r}(x - \sigma(\alpha_i)) = \prod_{i=1}^{r}(x - \alpha_i)$$

This shows that $\prod_{i=1}^{r}(x-\alpha_i)$ is fixed under σ for all $\sigma \in G$ and therefore $\prod_{i=1}^{r}(x-\alpha_i) \in F[x]$. Since $m(x)$ is the minimal polynomial of α it must divide $\prod_{i=1}^{r}(x-\alpha_i)$. This shows that $m(x) = \prod_{i=1}^{r}(x - \alpha_i)$ and therefore $m(x)$ has distinct roots and that it splits over E.

Since E/F is separable, the primitive element theorem says that $E = F[\alpha]$ for some α. For this α, and the notation of the previous paragraph,

$$[E : F] = \deg m_\alpha(x) = \deg \prod_{i=1}^{r}(x - \alpha_i) \leq |G|$$

On the other hand, since E/F is separable, $[E : F] = |\mathrm{Gal}(E/F)| \leq G$. The latter inequality is because each $\sigma \in G$ is, by assumption, an automorphism of E and it fixes F by definition of F. Thus we must have $[E : F] = |G|$ and $G = \mathrm{Gal}(E/F)$. □

Now we come to the climax of the theoretical work in this course.

Theorem 27.3 (Galois)**.** *Let E/F be a Galois extension and set $G = \mathrm{Gal}(E/F)$. Let $\mathcal{F}$ and $\mathcal{G}$ be the fixed field and fixing group functors for this extension.*

(1) $\mathcal{F}$ and $\mathcal{G}$ are inverses of each other.

(2) For $H \leq G$, $[E : \mathcal{F}(H)] = |H|$, or equivalently, $[\mathcal{F}(H) : F] = [G : H]$.

(3) $\mathcal{F}$ and $\mathcal{G}$ respect conjugation. For $\sigma \in G$, and $H \leq G$,

$$\mathcal{F}(\sigma H \sigma^{-1}) = \sigma\mathcal{F}(H)$$

(4) $\mathcal{F}$ and $\mathcal{G}$ respect normality in the following sense:

$$H \text{ is normal in } G \iff \mathcal{F}(H)/F \text{ is a normal extension}$$

Furthermore, if H is normal, $\mathrm{Gal}(\mathcal{F}(H)/F) \cong G/H$.

For items (2)-(4) in the proof, I've expressed the result using $\mathcal{F}$. As a quick exercise, find the corresponding result for $\mathcal{G}$, and obtain it directly from the result for $\mathcal{F}$ using item (1).

Proof. Let $H \leq G$. By the proposition, $E/\mathcal{F}(H)$ is Galois, $\mathrm{Gal}(E/\mathcal{F}(H)) = H$, and $[E : \mathcal{F}(H)] = |H|$. This shows that $\mathcal{G}\mathcal{F}$ is the identity. It also establishes item (2). We derive $[\mathcal{F}(H) : F] = [G : H]$ from

$$[E : \mathcal{F}(H)][\mathcal{F}(H) : F] = [E : F] = |G| = |H|[G : H]$$

Now let $F \leq D \leq E$. By Corollary 26.6, E is Galois over both D and $\mathcal{F}(\mathcal{G}(D))$ and by the proposition,

$$[E : D] = |\mathrm{Gal}(E/D)| = |\mathcal{G}(D)|$$
$$[E : \mathcal{F}\mathcal{G}(D)] = |\mathrm{Gal}(E/\mathcal{F}\mathcal{G}(D))| = |\mathcal{G}\mathcal{F}\mathcal{G}(D)|$$

Since $\mathcal{G}\mathcal{F}\mathcal{G} = \mathcal{G}$ and $D \leq \mathcal{F}\mathcal{G}(D)$, we get $D = \mathcal{F}\mathcal{G}(D)$. Thus $\mathcal{F}$ and $\mathcal{G}$ are inverses of each other.

Now we consider conjugation by $\sigma \in G$. Let $H \leq G$ and let θ be an arbitrary element of H. An element of $\sigma\mathcal{F}(H)$ may be written $\sigma(x)$ with $x \in \mathcal{F}(H)$. We have

$$\sigma\theta\sigma^{-1}(\sigma(x)) = \sigma(x) \in \mathcal{F}(H)$$

So $\sigma\mathcal{F}(H) \subseteq \mathcal{F}(\sigma H\sigma^{-1})$. Applying this result again we have

$$\mathcal{F}(\sigma H\sigma^{-1}) = \sigma(\sigma^{-1}\mathcal{F}(\sigma H\sigma^{-1})) = \sigma(\mathcal{F}(\sigma^{-1}\sigma H\sigma^{-1}\sigma)) = \sigma\mathcal{F}(H)$$

This establishes item (3).

If H is normal, item (3) gives $\sigma\mathcal{F}(H) = \mathcal{F}(H)$ for all $\sigma \in G$. Any embedding of $\mathcal{F}(H)$ into the algebraic closure of E that fixes F can be extended to E. Since E/F is normal, the only embedddings of E fixing F are automorphisms of F. Consequently, the only embeddings of $\mathcal{F}(H)$ are restrictions of elements of G to $\mathcal{F}(H)$. We have just shown that these all have image $\mathcal{F}(H)$, so $\mathcal{F}(H)$ must be normal.

Conversely, if $\mathcal{F}(H)/F$ is normal, then every embedding of $\mathcal{F}(H)$ into its algebraic closure has image $\mathcal{F}(H)$. Thus for any $\sigma \in G$, $\mathcal{F}(\sigma H\sigma^{-1}) = \sigma\mathcal{F}(H) = \mathcal{F}(H)$. Now apply $\mathcal{G}$, to get $\sigma H\sigma^{-1} = H$.

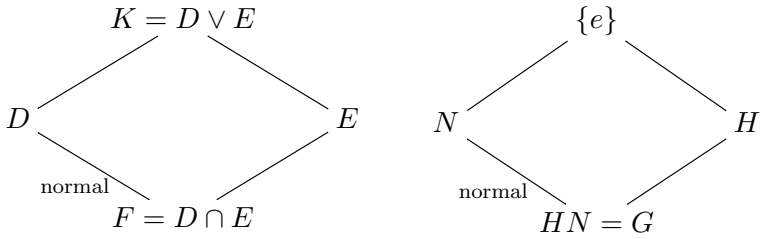

Figure 1: Illustration of Corollary 27.4: $G = \mathrm{Gal}(K/F)$, $N = \mathrm{Gal}(K/D)$ is normal in G, $H = \mathrm{Gal}(K/E)$

For any field $D \leq E$ we get a homomorphism $G \longrightarrow \mathrm{Aut}(D/F)$ just by restricting the domain of $\sigma \in G$ to D. For the field $\mathcal{F}(H)$ with H normal the previous result shows that H is in the kernel of $G \longrightarrow \mathrm{Aut}(\mathcal{F}(H)/F) = \mathrm{Gal}(\mathcal{F}(H)/F)$. By the factor theorem we have $G/H \longrightarrow \mathrm{Gal}(\mathcal{F}(H)/F)$. By item (2), and Proposition 27.2,

$$|\mathrm{Gal}(\mathcal{F}(H)/F)| = [\mathcal{F}(H) : F] = [G : H] = |G/H|$$

so in fact $G/H \cong \mathrm{Gal}(\mathcal{F}(H)/F)$. □

Corollary 27.4. *Let K be a Galois extension of F and let D and E be intermediate fields such that $F = D \cap E$ and $K = D \vee E$. Suppose in addition that D is a normal extension of F. Then the Galois group of K over F is a semidirect product:*

$$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(K/D) \rtimes \mathrm{Gal}(K/E)$$

If both E and F are normal extensions of F then $\mathrm{Gal}(K/F)$ *is the direct product of* $\mathrm{Gal}(K/D)$ *and* $\mathrm{Gal}(K/E)$*.*

Proof. By the Galois correspondence $\mathrm{Gal}(K/D)$ is a normal subgroup of $\mathrm{Gal}(K/F)$. Since $D \cap E = F$, $\mathrm{Gal}(K/D) \vee \mathrm{Gal}(K/E) = \mathrm{Gal}(K/F)$. Since $D \vee E = K$, $\mathrm{Gal}(K/D) \cap \mathrm{Gal}(K/E) = \mathrm{Gal}(K/K)$, the identity element of $\mathrm{Gal}(K/F)$. This shows that $\mathrm{Gal}(K/F)$ is the semidirect product of its normal subgroup $\mathrm{Gal}(K/D)$ and the subgroup $\mathrm{Gal}(K/E)$. □

Proposition 27.5 (Diamond)**.** *Let D and E be two subfields of K. If D is a finite Galois extension of $D \cap E$ then $D \vee E$ is Galois over E and* $\mathrm{Gal}(D \vee E/E) \cong \mathrm{Gal}(D/D \cap E)$*.*

Proof. Let D be a finite Galois extension of $D \cap E$. By the Primitive Element Theorem, $D = D \cap E(\alpha)$ for some $\alpha \in D$. The minimal polynomial of α over $D \cap E$ is separable and splits in D.

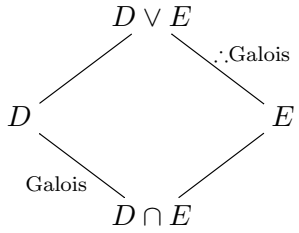

Figure 2:

I claim $D \vee E = E(\alpha)$. Since $E(\alpha)$ contains $D \cap E$ and α it must contain D. Clearly $E(\alpha)$ contains E so it contains $E \vee D$. The reverse inclusion is immediate since $D \vee E$ contains E and α. Now, since the minimum polynomial of α over E divides $m(x)$, it has distinct roots, and all these roots lie in $D \vee E$ (since they lie in D). Thus $D \vee E$ is Galois over E.

We now show there is a homomorphism

$$\mathrm{Gal}(D \vee E/E) \longrightarrow \mathrm{Gal}\, D/(D \cap E)$$

and that it is injective and surjective.

Let $\sigma \in \mathrm{Gal}(D \vee E/E)$. We may restrict σ to D and get an embedding of D into $D \vee E$ that fixes $D \cap E$, which we write $\sigma|_D$. Since $D/D \cap E$ is normal, any such embedding is actually an automorphism of D. Since it also fixes $D \cap E$, we have $\sigma|_D \in \mathrm{Gal}\, D/(D \cap E)$. Since the group operation in both $\mathrm{Gal}(D \vee E/E)$ and $\mathrm{Gal}(D/D \cap E)$ is composition the map $\sigma \longmapsto \sigma|_D$ is a homomorphism.

To show injectivity, suppose $\sigma|_D$ is the identity map on D. Then σ fixes D and E and therefore fixes $D \vee E$ since elements of $D \vee E$ are algebraically expressible using elements of D and E. This proves injectivity.

To show surjectivity, let $H = \{\sigma|_D : \sigma \in \mathrm{Gal}(D \vee E/E)\}$. We will show that $\mathcal{F}(H) = D \cap E$. Then the fact that D is Galois over $D \cap E$ implies that $H = \mathrm{Gal}(D/D \cap E)$. Each $\sigma \in \mathrm{Gal}(D \vee E/E)$ fixes $\mathcal{F}(H)$ and E so it fixes $\mathcal{F}(H) \vee E$. Since $D \vee E/E$ is Galois, the fixed field of $\mathrm{Gal}(D \vee E/E)$ is E, so $\mathcal{F}(H) \vee E = E$ and therefore $\mathcal{F}(H) \subseteq E$. We also have $D \cap E\mathcal{F}(H) \subseteq D$, so $D \cap E = \mathcal{F}(H)$. $\square$

If both D and E are Galois over their intersection $D \cap E$, then the proposition says that $D \vee E$ is Galois over both D and E. The following corollary is a stronger statement.

Corollary 27.6. *Suppose that both D and E are Galois over $D \cap E$. Then $D \vee E$ is Galois over $D \cap E$ and*

$$\mathrm{Gal}(D \vee E)/D \cap E) \cong \mathrm{Gal}(D/D \cap E) \times \mathrm{Gal}(E)/D \cap E)$$

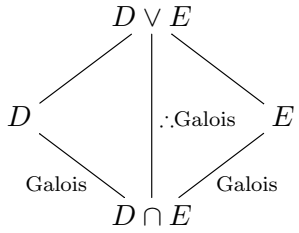

Figure 3:

Proof. We have $D = D \cap E(\alpha)$ and $E = D \cap E(\beta)$ for some $\alpha \in D$ and $\beta \in E$. Let $m_\alpha(x)$ and $m_\beta(x)$ be the associated minimal polynomials in $D \cap E[x]$. Then $D \vee E = D \cap E(\alpha, \beta)$ and $D \vee E$ is the splitting field of $m_\alpha(x) m_\beta(x)$ over $D \cap E$. $\square$

28 Problems

Problem 3: Let E be the splitting field of $x^6 - 2$.

(a) Show that $x^6 - 2$ is irreducible over $\mathbb{Q}$.

(b) Explain why the Galois group is isomorphic to D_6, the dihedral group on 6 elements.

(c) Find the Galois group and map out the relationship between subfields and subgroups for $E/\mathbb{Q}$.

Problem 1: Minimal polynomials for elements of $\mathbb{Q}(\sqrt[3]{2})$ (see [A] 3.1#4,5).

(a) Find the minimum polynomial of $\sqrt[3]{2} + 1$ over $\mathbb{Q}$. [There is a clever way that involves little computation, but don't feel obliged to use it!]

(b) Find the minimum polynomial of $\sqrt[3]{2} + \sqrt[3]{4}$ over $\mathbb{Q}$.

Problem 2: Let $E = \mathbb{Q}(i + \sqrt{2})$.

(a) Show that i and $\sqrt{2}$ are both in E.

(b) Find the minimum polynomial of $i + \sqrt{2}$.

(c) Show this polynomial splits in E.

(d) Find the Galois group and map out the relationship between subfields and subgroups for $E/\mathbb{Q}$.

Problem 3: Sixth roots of unity.

(a) Factor $x^6 - 1$ completely over $\mathbb{Q}$.

(b) Show that the splitting field of $x^6 - 1$ is of degree 2 over $\mathbb{Q}$.

Problem 4: Map out the Galois correspondence for $\mathbb{Q}(\zeta_n)$ for $n = 7, 9, 10, 11$.

Problem 5: Infinite algebraic extensions.

(a) Find a sequence of fields $\mathbb{Q} \leq F_1 \leq F_2 \leq \cdots$ such that each F_i is a normal extension of $\mathbb{Q}$. Justify your answer. [See 6.3#5 for inspiration.]

(b) Find a sequence of fields $\mathbb{Q} \leq F_1 \leq F_2 \leq \cdots$ such that each F_{i+1} is a normal extension of F_i but not of F_{i-1}. [See 6.3#9 for inspiration.]

Problem 6: Irreducible polynomials over $\mathbb{F}_p$. Suppose you have formulas for the number of irreducible monic polynomials of degree m over $\mathbb{F}_p$ for each $m < n$. Using some combinatorial arguments you can then compute the number of monic reducible polynomials of degree n. Subtracting this from the number of monic polynomials of degree n yields the number of monic irreducible polynomials of degree n.

(a) Show that the number of monic irreducible quadratics over $\mathbb{F}_p$ is $(p^2 - p)/2$.

(b) Show that the number of monic irreducible cubics over $\mathbb{F}_p$ is $(p^3 - p)/3$.

(c) You might want to guess at a general formula. A different counting method yields the result more easily than the one above. Try this if you want, noting:

- For $a \in \mathbb{F}_{p^n}$, a is in no proper subfield iff the minimal polynomial for a has degree n.
- Each monic irreducible of degree n has n distinct roots in $\mathbb{F}_{p^n}$.

Problem 1: Infinite algebraic extensions.

(a) Find a sequence of fields $\mathbb{Q} \leq F_1 \leq F_2 \leq \cdots$ such that each F_i is a normal extension of $\mathbb{Q}$. Justify your answer. [See 6.3#5 for inspiration.]

(b) Find a sequence of fields $\mathbb{Q} \leq F_1 \leq F_2 \leq \cdots$ such that each F_{i+1} is a normal extension of F_i but not of F_{i-1}. [See 6.3#9 for inspiration.]

Problem 2: Let E be a Galois extension of F. Let E_1 and E_2 be two intermediate fields and let $H_i = \mathrm{Gal}(E/E_i)$ for $i = 1, 2$. Let $E_1 \vee E_2$ be the compositum of E_1 and E_2—the smallest field containing them both. Let $H_1 \vee H_2$ be the smallest group containing H_1 and H_2.

(a) Explain why $\mathrm{Gal}(E/E_1 \vee E_2) = H_1 \cap H_2$. [One direction is easy, the other just requires an understanding of the elements of $E_1 \vee E_2$.]

(b) Explain why $\mathrm{Fix}(H_1 \vee H_2) = E_2 \cap E_2$. [Again, one direction is easy, the other just requires an understanding of the elements of $H_1 \vee H_2$.]

(c) Now use Galois' main theorem to show that $E_1 \vee E_2 = \mathrm{Fix}(H_1 \cap H_2)$ and $H_1 \vee H_2 = \mathrm{Gal}(E_1 \cap E_2)$.

Problem 3: Let $E = \mathbb{Q}(i + \sqrt{2})$.

(a) Show that i and $\sqrt{2}$ are both in E.

(b) Find the minimum polynomial of $i + \sqrt{2}$.

(c) Show this polynomial splits in E.

(d) Find the Galois group and map out the relationship between subfields and subgroups for $E/\mathbb{Q}$.

Problem 4: Let E be the splitting field of $x^6 - 2$

(a) Explain why the Galois group is isomorphic to D_{12}, the dihedral group on 6 elements.

(b) Find the Galois group and map out the relationship between subfields and subgroups for $E/\mathbb{Q}$.

1. Let the group G act on X.

(a) Let $y \in \mathrm{orb}(x)$. Show that the stabilizer of x and the stabilizer of y are conjugate subgroups of G.

(b) Suppose that the action of G is transitive—for any $x \in X$, $\mathrm{orb}(x) = X$. Show there is a bijection $G/\mathrm{stab}(x) \longrightarrow X$.

2. Let H be a subgroup of G and let G act on left cosets of H by left multiplication. Show that the kernel of the action is

$$N = \bigcap_{g \in G} gHg^{-1}$$

3. For both the quaternions, Q, and the dihedral group with 8 elements, D_8, the center is isomorphic to $\mathbb{Z}_2$ and the quotient to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Note that $\mathbb{Z}_2 \times \mathbb{Z}_2$ has 3 nontrivial proper subgroups.

(a) Using $D_8/Z(D_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, find the subgroups of D_8 corresponding to the 3 proper nontrivial subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$. Find the isomorphism class of each of these subgroups ($\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$.).

(b) Do the same thing for Q.

4. Let P be a p-Sylow subgroup of G. Let N be a normal subgroup of G. Show that

(a) $P \cap N$ is a p-Sylow subgroup of N.

(b) Show that PN/N is a p-Sylow subgroup of G/N.

Problem 1: Minimal polynomials for elements of $\mathbb{Q}(\sqrt[3]{2})$ (see [A] 3.1#4,5).

(a) Find the minimum polynomial of $\sqrt[3]{2}+1$ over $\mathbb{Q}$. [There is a clever way that involves little computation, but don't feel obliged to use it!]

(b) Find the minimum polynomial of $\sqrt[3]{2} + \sqrt[3]{4}$ over $\mathbb{Q}$.

Problem 2: Sixth roots of unity.

(a) Factor $x^6 - 1$ completely over $\mathbb{Q}$.

(b) Show that the splitting field of $x^6 - 1$ is of degree 2 over $\mathbb{Q}$.

Problem 2: Show that each of the following extensions is a Galois extension of $\mathbb{Q}$. Find the according Galois group.

(a) $\mathbb{Q}(i + \sqrt{2})$

(b) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

Problem 3: Show that $\mathbb{Q}(i\sqrt{5})/\mathbb{Q}$ and $\mathbb{Q}((1+i)\sqrt[4]{5})/\mathbb{Q}(i\sqrt{5})$ are normal, but $\mathbb{Q}((1+i)\sqrt[4]{5})/\mathbb{Q}$ is not normal.
(See also Rothman Ex. 88)

Problem 4: Prove: If H is an intermediate field of the finite Galois extension G/F then H/F is normal if and only if $\sigma(H) \subseteq H$ for all $\sigma \in \mathrm{Aut}(G/F)$.

Problem 16: Let F be the splitting field of $x^3 - 7 \in \mathbb{Q}[x]$ and let G be the splitting field of $(x^3 - 7)(x^2 - 3) \in \mathbb{Q}[x]$.

(a) Show that $F \neq G$.

(b) Show that $\mathrm{Aut}(G : \mathbb{Q})$ is the product of two normal subgroups, which have trivial intersection.

Problem 11: In the Euclidean plane there is given a line segment of length 1 and the parabola T described by the equation $y = x^2$. Assume that we allow for the usual compass and straight-edge constructions, and in addition we allow for intersections of constructible sets with T.

(a) Determine those integers $m \in \mathbb{N}$ for which $\sqrt[m]{2}$ can be constructed.

(b) Describe a construction of the number $\sqrt[3]{2}$.

Problem 1: Suppose that the polynomial $f = x^4 + ax^2 + b$ in $\mathbb{Q}[x]$ is irreducible. Let E be the splitting field of f and let the roots of f be $\pm\alpha$ and $\pm\beta$. We treated the case where $\alpha\beta \in \mathbb{Q}$ in class. Consider the extension of $\mathbb{Q}$ by a root γ of $y^2 + ax + b$.

(a) Show that when $\alpha\beta \in \mathbb{Q}[\gamma]$, the Galios group of E is $\mathbb{Z}/4$. The polynomial $x^2 + 4x + 2$ is an example.

(b) If $\alpha, \beta \notin \mathbb{Q}[\gamma]$ then the Galois group is D_4 the symmetry group for the square. The polynomial $x^4 - 2$ is an example. Identify the lattice of subgroups of D_4 and the corresponding lattice of intermediate fields between E and $\mathbb{Q}$.

Problem 2: In the Euclidean plane there is given a line segment of length 1 and the parabola T described by the equation $y = x^2$. Assume that we allow for the usual compass and straight-edge constructions, and in addition we allow for intersections of circles and lines with T.

(a) Investigate intersections of T with lines and circles.

(b) Describe a construction of the number $\sqrt[3]{2}$.

(c) Determine those integers $m \in \mathbb{Z}$ for which $\sqrt[m]{2}$ can be constructed.

(d) Can you determine other constructions that were not possible with ruler and compass?

Problem 3: Let $\varphi_n(x)$ be the irreducible polynomial for a primitive nth root of unity. We found cyclotomic polynomials over the rationals $\varphi_p(x)$ for p prime.

(a) What is the degree of the cyclotomic polynomial $\varphi_n(x) \in \mathbb{Q}[x]$ for arbitrary n? Can you find a formula for it?

(b) Find $\varphi_n(x)$ for $n \leq 16$.

(c) What happens over a prime field? Are the polynomials $\varphi_n(x)$ still irreducible?

(d) How do roots of unity and subfields of finite fields interact?

Problem 3: (100 pts.) Roots of equations.

(a) Compute the Galois group of the splitting field of $x^4 - 2x^2 - 3$.

(b) Identify the subgroups of the Galois group and the corresponding subfields of E.

Problem 4: (200 pts.) Cyclotomic extensions of $\mathbb{Q}$.

(a) Prove that if a field contains the nth roots of unity for n odd then it also contains the $2n$th roots of unity.

(b) Show that for n odd the cylcotomic polynomial $\Psi_{2n}(x)$ is $\Psi_n(-x)$. (We saw this for $n = 6$.)

(c) Compute $\Psi_9(x)$ the 9th cyclotomic polynomial.

(d) Identify $\mathrm{Gal}(\mathbb{Q}_9/\mathbb{Q})$ and all of its subgroups.

(e) For each subgroup choose a generator. Show how the generator acts on the 9th roots of unity with a diagram of these roots in the complex plane.

(f) Identify the corresponding subfields of $\mathbb{Q}_9$. [Hint, one is $\mathbb{Q}_3$].