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

August 20, 2012

The principle objects of study in algebra are groups, rings and fields. This course will focus on Galois theory, which involves the interplay between field theory and group theory. We will need a small amount of ring theory.

In the first part of the course, I'm going to define all three algebraic structures, and briefly discuss their most basic properties. The presentation will start abstract, but we will develop lots of examples to illustrate the core concepts. The purpose is to set the context for this course, and to establish some fundamental terminology. My goal is that at the end of five weeks I can explain in some depth several core problems that Galois theory solves.

For each type of algebraic structure, we study subsets that have the same algebraic structure: subgroups, subrings, subfields. We are also interested in functions that "respect the operations" for that structure. Such functions are called homomorphisms.

The first five weeks are therefore devoted to developing fluency with groups, subgroups and group homomorphisms, and fields, subfields and field homomorphisms. We will also discuss polynomial rings over a field since these are used to construct new fields. I would like you to review Sections 6 and 8 which concern the divisibility and factorization in the integers and in polynomial rings over a field. Please also review Sections 7 and 9, which concern congruence in the integers and in polynomial rings. I will only spend a little time on these results in class. You needn't worry about memorizing the proofs, mainly we need to be able to use the results with some depth of understanding.

The second part of the course will be a thorough treatment of group theory, primarily following Ash's Algebra Chapters 1 and 5. I suggest having a good undergraduate text to supplement the graduate text by Ash, such as those by Hungerford or Gallian, or the free text by Judson (updated by Beezer) `http://abstract.ups.edu/`. The core topics are normal subgroups and quotient groups, the isomorphism and correspondence theorems, classification of abelian groups, groups actions and the orbit-stabilizer theorem, the Sylow theorems.

The third part of the course will focus on field theory and lead to climax of the course, Galois's main theorem: Chapters 3 and 6 of Ash. We will then apply Galois theory to as many examples as we have time to cover. In particular: solution of equations by radicals, cyclotomic extensions, finite fields, and constructible numbers.

Part I

An Introduction to Groups

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.

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 $h \in H$, $e_h *_G h = h$. Proposition 1.3 (item 4) shows that it must be $e_H = e_G$, since $h \in G$. Each $h \in H$ must have an inverse, but the inverse in G is uniquely determined. Thus we must have $h^{-1} \in H$. Finally $*_G$ must be an operation on H, so for $h, h' \in H$, we must have $h *_G h' \in H$.

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 $*_G$, $h *_G h^{-1} = e_G \in H$.

To prove the second statement, suppose $h \in H$. Letting $h' = h$ in the assumed property gives $h *_G h^{-1} = e_G \in H$. 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. □

Definition 1.6. 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.*

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 1.7. *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 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.

If φ is an isomorphism, then the inverse function φ^{-1} is also an isomorphism.

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

Example 1.8. 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 $\mathbb{Z}, +$ to emphasize that we are are ignoring multiplication, and are just considering the additive properties of $\mathbb{Z}$.

Exercises 1.9.

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

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

Example 1.10. 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 $\mathbb{Z}_n$).

Exercises 1.11.

(a) 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 $\varphi_a(1) = a$.

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

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

Example 1.12. 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 1.13.

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

(2) 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 1.14. 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. 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 $\varphi^{-1} \circ \varphi = \mathrm{id}_S$. Finally, the composition of two bijections is also a bijection.

The most important special case is the *symmetric group on n elements*, written S_n, which is the set of bijections on $\{1, \dots, n\}$. The next section is devoted to an extensive study of the symmetric group and subgroups of it.

The following result is a straightforward exercise, but well worth doing carefully.

Proposition 1.15. *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 1.16.

(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 1.17. 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 1.18. 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).

Exercises 1.19.

(a) Check that the above definition does, indeed, make $G \times H$ a group.

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

(c) The construction can be generalized to the direct product of any set of groups $\{G_i : i \in I\}$ indexed by some set I.

(d) If A and B are abelian groups show that $A \times B$ is also abelian.

(e) If G' is a subgroup of G and H' is a subgroup of H then $G' \times H'$ is a subgroup of $G \times H$.

(f) 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 1.20. 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 $\mathrm{ord}(g)$ for the order of g.

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

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 others may a different order. For any finite group there is a well defined exponent, but an infinite group may not have one.

If $g \in G$ has order n then the set of powers of g is $\{g^0 = e_G, g, g^2, \ldots, g^{n-1}\}$ (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 1.21.

(1) If g has order m and 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 $\operatorname{ord}(a)$ and $\operatorname{ord}(b)$ are coprime find the order of ab.

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

(4) Show by brute force that S_4 has no element with order equal to $\exp(S_4)$.

Theorem 1.22 (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) $\operatorname{ord}(g^r) = \frac{n}{\gcd r,n}$.

(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. □

Exercises 1.23.

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

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

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 $\operatorname{ord}(g)$.

Exercises 1.24.

(a) 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 1.25. *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.*

Definition 1.26. 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 1.27. *Let $\varphi : G \longrightarrow H$ be a homomorphism of groups. The kernel of φ is trivial (just $\{e_G\}$) iff φ is injective.*

Proof. Suppoe φ is injective. Then only one element of G has image e_H, but we already know that $\varphi(e_G) = e_H$, so $\ker(\varphi) = \{e_G\}$.

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 1.25 is a subgroup of H. Thus $\varphi : G \longrightarrow G$ is an isomorphism. We will often call an injective homomorphism an *embedding* since the image is a "copy" of G inside of H.

Proposition 1.28. *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.

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 1.29. 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.

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 $G = \left\{a^i : i \in \mathbb{Z}\right\}$ 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 $\{1,\dots,n\}$. These are also called permutations of $\{1,\dots,n\}$. The number of elements in S_n is $n!$. Informally, we may justify this 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 $\{1,\dots,n\}$ to itself. We can give a more formal inductive proof later.

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.

Exercises 2.1.

(a) Here are two elements of S_5:

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

(b) Compute the inverse of each.

(c) 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

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

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 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.

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

Exercises 2.4.

(a) A t-cycle has order t.

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

Proposition 2.5. *Every permutation has a unique cycle decomposition.*

Definition 2.6. 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 $3, 2, 1$.

Exercises 2.7.

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

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

There is a another factorization that is important.

Proposition 2.8. *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

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

□

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 2.9.

(1) Show that S_n is generated by the $n-1$ elements $(1, k)$ for $k = 2, \dots, n$. [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 $(1, 2, 3, \dots, n-1, n)$. [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 parity of the factorization is.

Proposition 2.10. *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.

Suppose that π is the product of transpositions in two ways: $\pi = \sigma_1\sigma_2 \dots \sigma_m = \theta_1\theta_2 \dots \theta_k$. Then $\mathrm{id} = \sigma_1\sigma_2 \dots \sigma_m\theta_1^{-1}\theta_2^{-1} \dots \theta_k^{-1}$. 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 2.11. *The set of even parity permutations forms a subgroup of S_n. This is called the* alternating group *and is denoted A_n.*

Problems 2.12.

(1) Show that there is a homomorphism from S_n to $\mathbb{Z}_2$. The preimage of $0 \in \mathbb{Z}_2$ is A_n.

(2) Find all subgroups of A_4.

(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.

The first use of this notation is to define a coset of a group H in a group G containing H.

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 $|G|/|H|$. It is an integer by the previous proposition.

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

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

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

(4) Show that $\{\varphi_a : a \in G\}$ is a subgroup of $\operatorname{Aut}(G)$. It is called $\operatorname{Inn}(G)$, the group of *inner automorphisms* of G.

Proposition 3.11. *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 exercise.

Problems 3.12.

(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."

Problems 3.13.

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

(2) Now 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.

Part II

Just a bit on Rings, Particularly Polynomial Rings

4 Rings and Homomorphisms

Definition 4.1. A *ring* is a set R, with two operations $+$ and $*$ satisfying the properties

(1) Associativity of $+$ and $*$.

(2) Commutativity of $+$.

(3) Identities for $+$ and $*$: Usually denoted 0 and 1, respectively.

(4) Inverses for $+$: The inverse of $r \in R$ is usually written $-r$.

(5) Distributivity of $*$ over $+$: For all $a, b, c \in R$, $a * (b + c) = a * b + a * c$.

[Strictly speaking this is a ring with identity; among those who study such rings it is usual to just call them rings.]

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 $+$.

Definition 4.2. 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 4.3.

(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.

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

(1) $\varphi(r + s) = \varphi(r) + \varphi(s)$

(2) $\varphi(r * s) = \varphi(r) * \varphi(s)$

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

Notice that the operations $+$, $*$ on the left-hand side are in R and the operations $+, *$ on the right-hand side are in S. If we want to be careful we specify the ring: we write $+_S$ for the addition in S. We say φ *respects addition, multiplication and* *the identity element.* That is, it respects the ring structure. There are a several little results to establish for homomorphisms: e.g. $\varphi(-s) = -\varphi(s)$. See [**?**, §3.3].

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

Theorem 4.4 (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 4.5. The *kernel of a homomorphism* $\varphi : R \longrightarrow S$ is the preimage of 0_S: that is $\{r \in R : \varphi(r) = 0_S\}$. It is an exercise to show that φ is injective (one-to-one) iff the kernel is trivial (just 0_R). A homomorphism that is also a bijection (injective and surjective) is called an *isomorphism.*

5 Rings and Unit Groups

Proposition 5.1. *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 associativite, and has an identity element, 1. By the definition of $U(R)$, each element of $U(R)$ has an inverse, and the previous exercise shows that the inverse of a unit is also in $U(R)$. □

Definition 5.2. A *division ring* is a ring in which each nonzero element is a unit. A *field* is a commutative division ring.

Exercises 5.3.

(a) Let D be a division ring. Show that $D \setminus \{0\}$, which we denote D^*, is a group under $*$.

(b) Show that a division ring has no zero divisors. That is: if $ar = 0$ for some $a, r \in R$

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 is a group under multiplication. We denote it with a $*$, for example: $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$. In addition we have the subgroups $\mathbb{Q}^{**}$ and $\mathbb{R}^{**}$ consisting of the positive field elements.
- 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 $\mathrm{Gl}(n, F)$.

There are many interesting subgroups of the general linear group.

Exercises 5.4.

(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 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 5.5. 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 5.6.

(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 5.7.

(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.

6 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 6.1 (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 6.2 (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 $r_{-1} = a$ and $r_0 = b$, and define inductively (while $r_k \neq 0$)

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

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 result 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 $Q_k = \begin{bmatrix} -q_k & 1 \\ 1 & 0 \end{bmatrix}$ and $R_k = \begin{bmatrix} r_k \\ r_{k-1} \end{bmatrix}$ 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 6.3 (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
```

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

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

Theorem 6.5 (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*

$$a = up_1^{e_1} \cdots p_t^{e_t}$$

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 6.6.

(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 $S = \{ax+by : x, y \in \{-N, \dots, N\}\}$. 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?

7 Integers modulo n

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

Theorem 7.1. *Congruence modulo n is an eqivalence relation. The set* $\{0, 1, \dots, n-1\}$ *is a system of representatives for congruence modulo n; each integer is congruent modulo n to exactly one element of* $\{0, 1, \dots, n-1\}$.

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 7.2 (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 $0, 1, \dots, n-1$ (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 7.3 (Units, Zero Divisors)**.** *Let $n > 2$ 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 7.4. *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 rest of this section is mainly of interest next semester.

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 $m|(b-a)$ 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 7.5 (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 CRT 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 7.6 (Chinese Remainder Theorem)**.** *Let m, n be coprime. There is an isomorphism $\mathbb{Z}/mn \longrightarrow \mathbb{Z}/m \times \mathbb{Z}/n$.*

Recall that $a \in \mathbb{Z}/n$ is a *zero-divisor* when $a \neq 0$ and there is some nonzero $b \in \mathbb{Z}/n$ such that $a * b = 0$ (in $\mathbb{Z}/n$). We also say a is a *unit* when there is some $b \in \mathbb{Z}/n$ such that $ab = 1$ (in $\mathbb{Z}/n$).

8 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 for polynomial rings as well.

We can think of the polynomial ring as a vector space over F with an infinite basis $1, x, x^2, \dots$, 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 8.1 (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 sometimes omit the (x) to simplify notation. 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 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 8.2 (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 Euclidian 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 8.3 (Prime-Irreducible)**.** *Any nonconstant element of $F[x]$ is irreducible iff it is prime.*

Theorem 8.4 (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. 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. Show furthermore that the remainder $f \,\%\, (x - c) = f(c)$.

Theorem 8.5. *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 8.6.

(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?

9 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 9.1. *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 9.2 (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 9.3 (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 9.4. *Let $p(x)$ be irreducible. Then $\mathbb{Z}/p(x)$ is a field; every nonzero element has an inverse.*

The rest of this section is mainly of interest next semester.

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 9.5 (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 9.6 (Chinese Remainder Theorem)**.** *Let $m(x), n(x) \in F[x]$ be coprime. There is an isomorphism $F[x]/(m(x)n(x)) \longrightarrow F[x]/m(x) \times F[x]/n(x)$.*

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

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

Notation 10.1. 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 **??** for the integers.

Theorem 10.2 (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

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

To show this function is 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.

Proposition 10.3. *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 1.22), following the general theme that many properties for $\mathbb{Z}$ extend to polynomial rings over a field.

Proposition 10.4. *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 10.5. 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.

11 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 11.1. *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 11.2. *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 11.3. *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 11.4. 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 11.5. *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 11.6. *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 10.2 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 11.7. *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 11.8 (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 11.9.

(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. Use the isomorphism $x \longmapsto (x+1)$ and Eisenstein's criterion.

(2) Test whether the following polynomials are irreducible.

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

(3) Show that $x^4 - 10x + 1$ is irreducible 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.

Part III

An Introduction to Fields

12 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 12.1. 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 1.7, $\varphi : F \longrightarrow K$ 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 disctinction! 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 12.2. *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 12.3.

(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 12.4. 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 12.5. *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,

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

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, $\varphi(1/b) = 1/b$ 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.

13 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 the following proposition that is analogous to the result that $\mathbb{Z}/p$ is a field.

Proposition 13.1. *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 13.2. 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 $\text{Aut}(\mathbb{Q}[i])$ 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 13.3. 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 13.4. *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 isomorphic 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 $-\sqrt{D}$.

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 isomorphic to $\mathbb{Q}[\sqrt{D}]$ and by Proposition 13.4 that $\mathbb{Q}[\sqrt{D}]$ is isomorphic 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.

14 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 14.1. 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 $a^3 + 2b^3 + 4c^3 + 8abc$.

We need to 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 $\big(\varphi(\sqrt[3]{2})\big)^3 = 2$. 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 14.2. *Let B be a rational number that is not a perfect cube.*

(1) The set $\left\{a + b\sqrt[3]{} + c\sqrt[3]{B^2} : a, b, c \in \mathbb{Q}\right\}$ 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) identity map is the only automorphism of $\mathbb{Q}[\sqrt[3]{B}]$.

The solution of a cubic polynomial

In the 16$^{\text{th}}$ and 17$^{\text{th}}$ 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 ($\bar{y}(p, q)$ an expression for y in terms of p and q), can be transformed to a solution to the original equation by a number of substitutions.

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

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 14.2. The 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 that this value of z cannot be zero since $p \neq 0$.

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

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

Returning to the original question, 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

- There is ambiguity in the notation $R^{\frac{1}{3}}$. If R is real then this means the real cubic root, but if R is not real then there is not clear way to identify a particular cube root.
- $RS = -p^3/27$ 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 $R^{\frac{1}{3}}S^{\frac{1}{3}} = -p/3$ the unique real root of $-p^3/27$.
- If R is not real then we can still choose $R^{\frac{1}{3}}$ and $S^{\frac{1}{3}}$ so that their product is $-p/3$.

Then we get three solutions for y

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

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 14.3.

(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 $m(x)$ splits 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.

15 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 15.1. *Let F be a field with a finite number of elements.*

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

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

3) F 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 15.2. *A finite field is a vector space over $\mathbb{F}_p$ for some prime p. Consequently, the number of elements of F is a power of p.*

Proof. Suppose that F 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 F 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 $0 \leq a < p$ is a subset of F 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 F as containing $\mathbb{F}_p$.

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

Definition 15.3. The prime p in the theorem is called the *characteristic* of the field.

Suppose that $q = p^n$ is the number of elements in F. By the field axioms, the set of nonzero elements of F is a group under multiplication. This group is denoted F^*. 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:

Lemma 15.4. *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 $r = \operatorname{ord}(\alpha)$. Then $\operatorname{ord}(\alpha\beta) = rs$.

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 $\operatorname{ord}(\prod_{i=1}^n \alpha_i) = \prod_{i=1}^n r_i$.

Now we can establish item 2) of the Theorem.

Proposition 15.5. *The multiplicative group of a finite field is cyclic.*

Proof. Let F 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 $b_i \in F^*$ of order $q_i^{a_i}$. Since the $q_i^{a_i}$ are Lemma 15.4 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 F.

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

t elements of F 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 F is q^a. This shows what we wanted: there is some element of F of order q^a.

□

Definition 15.6. 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. F^* 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 15.7. *If F is a field with p^n elements then*

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

According to the following definition, the corollary shows that a field F 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 15.8. Let F be a field and let $f(x) \in F[x]$. A *splitting field* for $f(x)$ is a field K containing F 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 10.5).

Proposition 15.9. *Let F be a finite field of p^n elements. Let β be any primitive element of F and let $M(x)$ be its minimal polynomial over $\mathbb{F}_p$. Then F is isomorphic to $\mathbb{F}_p[x]/M(x)$. In particular* $\deg M(x) = n$.

Proof. Let $M(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1 x + a_0$ with $a_i \in \mathbb{F}_p$. We will show that $1, \beta, \ldots, \beta^{r-1}$ is a basis for F 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 $1, \beta, \beta^2, \ldots, \beta^{r-1}$. This is true trivially for β^i for $i = 0, \ldots, r-1$. Assume that for some $k \geq r$, each a^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 every nonzero element of F is a power of β, we have shown that $1, \beta, \ldots, \beta^{r-1}$ span F as claimed.

Since F has p^n elements $r = n$. Furthermore the arithmetic on F 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 F 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 15.10. *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 15.11. *For any prime power there exists a unique field of that order.*

Proof. Uniqueness: Let F and F' be two fields with p^n elements. Let α be a primitive element in F and let $M(x)$ be its minimal polynomial over $\mathbb{F}_p$. Since α is a root of $x^{p^n} - x$, Lemma 10.4 says that $M(x)$ divides $x^{p^n} - x$. By Corollary 15.7, $x^{p^n} - x$ factors into distinct linear factors in both F and F' so there must be a root of $M(x)$ in F'. By Proposition 15.9, both F and F' 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 15.12. 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 15.13. Let F be a finite field and let $p(x)$ be a polynomial over F. If $p(x)$ is irreducible and the class of x is primitive in $F[x]/p(x)$, then we say $p(x)$ is a *primitive polynomial.*

Example 15.14. 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 15.15. *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 15.16. *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 15.17.

(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 $\alpha \in \mathbb{F}_q$,

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