Constructing Finite Fields From Quotient Rings

Summary

1 What are these notes?

These are some personal notes that hopefully provide some intuition on how to construct a finite field from a quotient ring.

This starts from scratch (defining a group), and builds up with only relevant information. As a result, lots of concepts taught in a standard abstract algebra course are left out. An understanding of cosets may be useful, but not really necessary.

Most of these notes are definitions and examples. There are only really a few theorems needed to actually construct a finite field from a quotient ring. The proofs of the theorems mentioned are not included.

2 Groups

Definition 1 *A group is a set G, along with a binary operation ❇, that satisfies the following conditions:*

1. *G is closed under ❊. That is, for all $a, b \in G$,*

   a❊$b \in G$.

2. *G satisfies associativity under ❊. That is, for all $a, b, c \in G$,*

   (a❊b)❊c = a❊(b❊c)

3. *There exists an identity element in G. That is, there exists an element $e \in G$ such that, for all $a \in G$,*

   a❊e = e❊a = a

4. *Every element $a \in G$ has an inverse $a' \in G$. That is,*

   a❊a' = a'❊a = e

We denote a group by the tuple (G, ❊).

Examples of groups:

- The integers under addition: $(\mathbf{Z}, +)$
- The rationals under multiplication: $(\mathbf{Q}, *)$

Definition 2 *An abelian group (G,❊) is a group that also satisfies the commutative property. That is, for all $a, b \in G$,*

a❊b = b❊a

Examples of abelian groups

- $(\mathbf{R}, +)$
- $(Z_5, +)$

3 Rings

Every ring is an abelian group, along with some additional requirements. Some authors define a ring differently from others. For these notes, we're going to use the following definition:

Definition 3 *A ring is a set R, along with two distinct binary operations, addition (+) and multiplication ($*$), that satisfies the following:*

1. *R is an abelian group under $+$ with the additive identity* 0
2. *R is associative under $*$*
3. *$*$ distributes over $+$ in R. That is, for all $a, b, c \in R$,*

$$a * (b + c) = (a * b + a * c)$$

$$(a * b) * c = (a * c + b * c)$$

Technically, the binary operations can be whatever you want, like with rings. But for simplicity, we will use addition and multiplication.

Note that there is no requirement for every element in a ring R to have a multiplicative inverse. Those elements with multiplicative inverses are called *units* of R.

Similar to the notation for groups, we can reference a ring by the tuple (set name, +, *). So for example, $(R, +, *)$. But since we are only considering addition and multiplication, we can just refer to the ring by its name.

Examples of rings:

- Z_n for some $n \in \mathbf{Z}$
- $\mathbf{Q} = \{\frac{a}{b} : a, b \in \mathbf{Z}\}$
- $\mathbf{Q}[x] = \{a_0 + a_1(x) + a_2(x^2) + \ldots : a_i \in \mathbf{Q}\}$

The last example, $\mathbf{Q}[x]$, is the set of polynomials with rational coefficients. Polynomial rings are VERY important for the construction of finite fields. Just keep that in mind for now.

Just like abelian groups, there exist abelian (commutative) rings. The only additional requirement is that the ring satisfies commutativity under multiplication.

Definition 4 *A subring S of a ring R is a subset of R and satisfies the following:*

1. *S is itself a ring under the same operations as R.*

Example of a subring:

- $2\mathbf{Z} = \{2x : x \in \mathbf{Z}\}$ is a subring of $\mathbf{Z}$

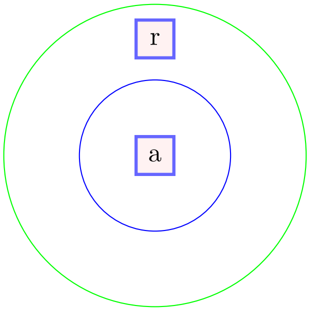
$\mathbf{Z}_{10}$ has completely different binary operations than $\mathbf{Z}$. Specifically, the additive and multiplication operations $\mathbf{Z}_{10}$ are addition mod 10, and multiplication mod 10, respectively, which is different from normal addition and multiplication.

4 Ideals

Definition 5 *A (two-sided) ideal A of a ring R is a subring of R that satisfies the following:*

1. *For all $a \in A$, $r \in R$, $a * r, r * a \in A$*

The second requirement is known as an "absorbing" property. Consider the figure below. Suppose the outer-green circle is a ring R with an arbitrary element $r \in R - A$, and the inner-blue circle is an ideal of R, namely A, with an arbitrary element a. The absorbing property really means that if you multiply r and a (either $r * a$ or $a * r$), then the result must be an element of A; the ideal A absorbs elements in $R - A$.



Some ideals of a ring R can be "generated" by element(s) of R. More formally, an ideal A of a ring R generated by an element $a \in R$ is the set

$$< a >= \{a * r : r \in R\}.$$

These will be useful when discussing irreducible polynomials.

We now introduce a special type of ideal, a maximal ideal.

Definition 6 *A maximal ideal A of a ring R is an ideal that satisfies the following:*

1. *For any ideal B of R where $A \subset B$, either $A = B$ or $B = R$.*

This definition is basically saying that for an ideal A to be a maximal ideal of a ring R, A cannot be contained within any proper subset of R. This along with the following definition are VERY important for setting up the construction of finite fields.

Definition 7 *Let A be an ideal of a ring R. The set*

$$R/A = \{r + A | r \in A\}$$

is known as a quotient ring. Its binary operations addition and multiplication are defined by:

- *For all $(r_m + A), (r_n + A) \in R/A$,*
  1. $(r_m + A) + (r_n + A) = (r_m + r_n + A)$
  2. $(r_m + A) * (r_n + A) = (r_m * r_n + A)$

For now, just know that specific quotient rings are closely related to fields.

5 Fields

Just like how every ring is a (special type of) group, every field is a (special type of) ring.

Definition 8 *A field F is a commutative ring where every non-zero element has a multiplicative inverse. That is, F must be a commutative ring with the following additional properties:*

- *For all $a, b \in F$,*
$$a * b = b * a$$
- *For every $0 \neq a \in F$, there exists an element a' such that*
$$a * a' = a' * a = 1$$
.

Fields are essentially a structure where you can add, subtract, and multiply all numbers, WHILE being able to divide all non-zero numbers. For that reason, fields are sometimes referred to as ”division rings”.

We are interested in one particular type of ring, the polynomial ring $F[x]$. This is the set of all polynomials with coefficients in the field F. More formally,

$$F[x] = \{a_0 + a_1(x) + a_2(x^2) + \ldots + a_n(x^n) : a_i \in F.$$

Note that the polynomials only consider non-negative powers of x. So why is $F[x]$ a ring, but not a field? Although the constants (degree 0 polynomials) are units (have multiplicative inverses), the polynomials with degree ≥ 1 are not. For example, what would be the multiplicative inverse of x? The element $\frac{1}{x}$ doesn't work because we only consider non-negative powers of x in $F[x]$.

6 Irreducible polynomials

Definition 9 *Let F be a field. An irreducible polynomial $p(x) \in F[x]$ is a polynomial that has the following properties:*

- *The degree of $p(x) \geq 2$*
- *If $p(x) = f(x)h(x)$ for some polynomials $f(x), h(x) \in F[x]$, then either the degree of $f(x) = 0$ or the degree of $h(x) = 0$*

Basically, an irreducible polynomial $p(x)$ cannot be broken into smaller, non-unit parts. The first property guarantees we can't factor a constant out of $p(x)$, like $4x+4 = 4(x+1)$, since a constant is a unit. The second property guarantees that if we can reduce $p(x)$ into two smaller parts, then one of the smaller parts must be a unit.

7 Constructing a finite field from a quotient ring

The following theorems are all we need to finally prove that a (finite) field can be constructed from a quotient ring

Theorem 1 *The ideal generated by an irreducible polynomial is maximal.*

Theorem 2 *Let A be a maximal ideal of a ring R. Then R/A is a field.*

And there we have it. The first theorem states that if we have an irreducible element $p(x)$ in some polynomial ring $F[x]$, then $< p(x) >$ is an ideal of $F[x]$. Specifically, $< p(x) >$ is a maximal ideal. Thus, by the second theorem, we obtain the main result of these notes.

Result 1 *When $p(x)$ is an irreducible polynomial over F, $F[x]/ < p(x) >$ is a field.*

7.1 Irreducibility tests

While the result may seem powerful, we need to actually find irreducible polynomials to construct anything.

Luckily, there are lots of irreducibility tests, which often depend on the field of coefficients. We will only cover one that's simple, but still very useful.

Theorem 3 *Let $p(x)$ be a polynomial over some field F with the degree of $p(x)$ being 2 or 3. If $p(x)$ has no roots (zeros) in F, then $p(x)$ is irreducible.*

A root (or zero) of a polynomial is an element a such that $p(a) = 0$. For example, $x + 2 \in \mathbf{Q}[x]$ has a root of -2 (in $\mathbf{Q}$), since $(-2) + 2 = 0$.

On the other hand, $x^2 - 2$ has no roots in $\mathbf{Q}$, since no element a in $\mathbf{Q}$ satisfies $(a)^2 - 2 = 0$.

So we only need to find a degree 2 (or 3) polynomial $p(x)$, and make sure it doesn't have any roots; then we are certain that $p(x)$ is irreducible. But what approach can we take to check that every single possible element in the field of coefficients is not a root? With "small" fields, we can exhaustively check all options.

Consider $p(x) = x^2 + x + 1$ over the field $\mathbf{Z}_2$. Since $\mathbf{Z}_2$ only has 3 elements $(0, 1)$, we only need to make sure none of the elements are roots of $p(x)$.

- $(0)^2 + (0) + 1 = 1$
- $(1)^2 + (1) + 1 = 1$

Note the arithmetic is done modulo 3. Since none of these equations equal 0, we know $x^2 + x + 1$ is irreducible over $\mathbf{Z}_2$. Thus, by the main result of this paper, $\mathbf{Z}_2[x]/ < x^2 + x + 1 >$ is a field. But is this a finite field? Yes! But how do we know?

7.2 Elements of a quotient ring

What do elements look like in $\mathbf{Z}_2[x]/ < x^2 + x + 1 >$?

By definition,

$$\mathbf{Z}_2[x]/ < x^2 + x + 1 >= \{a+ < x^2 + x + 1 >: a \in Z_3\}.$$

Which means the following are some elements of $\mathbf{Z}_2[x]/ < x^2 + x + 1 >$:

1. $0+ < x^2 + x + 1 >=< x^2 + x + 1 >$
2. $1+ < x^2 + x + 1 >$
3. $x + 0+ < x^2 + x + 1 >= x+ < x^2 + x + 1 >$
4. $x + 1+ < x^2 + x + 1 >$

Why did I stop at $x + 1+ < x^2 + x + 1 >$? Notice that $< x^2 + x + 1 >$ acts as the additive identity (0) of the field $\mathbf{Z}_2[x]/ < x^2 + x + 1 >$. Also notes that $x^2 + x + 1$ and 0 are BOTH elements of $< x^2 + x + 1 >$. Thus, $x^2 + x + 1+ < x^2 + x + 1 >= 0+ < x^2 + x + 1 >$ (for more information, look up cosets). It then follows that $x^2+x+1 = 0$, which implies that $x^2 = -x-1 = x+1$ (since we are in modulo 2).

Therefore, $x^2+ < x^2 + x + 1 >= x + 1+ < x^2 + x + 1 >$, which is already a defined element above. In fact, it is the case that all polynomials of degree 2 or more will reduce to one of the above defined elements of $\mathbf{Z}_2[x]/ < x^2 + x + 1 >$. So this field is in fact finite (with exactly the 4 elements above). Finally, we have constructed a finite field of 4 elements. And this cannot be isomorphic to $\mathbf{Z}_4$, because $\mathbf{Z}_4$ is not even a field (consider $2 \neq 0$, which has no multiplicative inverse). This is just one of many different examples for constructing a finite field.