

CDM

Finite Fields

Klaus Sutner
Carnegie Mellon University

Fall 2011

Outline

- 1 Rings and Fields
- 2 Finite Fields
- 3 Ideals
- 4 The Structure theorem

Rings and Field

Definition

A **ring** is an algebraic structure of the form

$$\mathcal{R} = \langle R, +, \cdot, 0, 1 \rangle$$

where

- $\langle R, +, 0 \rangle$ is a commutative group (additive group),
- $\langle R^*, \cdot, 1 \rangle$ is a monoid where $R^* = R - \{0\}$ (multiplicative monoid),
- multiplication distributes over addition:

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

$$(y + z) \cdot x = y \cdot x + z \cdot x$$

Commutative Rings

Note that we need two distributive laws since multiplication is not assumed to be commutative. If multiplication is commutative the ring itself is called **commutative**.

A ring element is called a **unit** if it has an inverse in the multiplicative monoid.

One can relax the conditions a bit and deal with rings without a 1: one has a multiplicative semigroup rather than a monoid, but for our purposes there is no need for this.

Examples: Rings

Example (Standard Rings)

The integers \mathbb{Z} , the rationals \mathbb{Q} , the reals \mathbb{R} , the complex numbers \mathbb{C} .

Example (Univariate Polynomials)

Given a ring R we can construct new rings by considering all polynomials with coefficients in R , written $R[x]$ where x indicates the “unknown” or “variable”.

For example, $\mathbb{Z}[x]$ is the ring of all polynomials with integer coefficients.

Example (Matrix Rings)

Another important way to construct rings is to consider square matrices with coefficients in a ground ring R .

For example, $\mathbb{R}^{n,n}$ denotes the ring of all n by n matrices with real coefficients. Note that this ring is not commutative unless $n = 1$.

The Annihilator

Proposition

In any ring, $a0 = 0a = 0$.

Proof. Note that $a0 = a(0 + 0) = a0 + a0$, done by cancellation in the additive group. □

We are interested in rings that have lots of units. One obstruction to having a multiplicative inverse is described in the next definition.

Definition

A ring element $a \neq 0$ is a **zero divisor** if there exist $b, c \neq 0$ such that $ab = ca = 0$. A commutative ring is an **integral domain** if it has no zero-divisors.

Note that a zero divisor cannot have an inverse: otherwise $ab = 0$ implies $0 = a^{-1}ab = b$, a contradiction.

Examples: Integral Domains

Example (Standard Integral Domains)

The integers \mathbb{Z} , the rationals \mathbb{Q} , the reals \mathbb{R} , the complex numbers \mathbb{C} are all integral domains.

Example (Modular Numbers)

Quotient rings \mathbb{Z}_m are integral domains iff m is prime.

Example (Non-ID)

The ring of 2×2 real matrices is not an integral domain:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

A Strange Ring

Arithmetic structures provide the standard examples for rings, but the axioms are much more general than that. Here is an example. Let A be an arbitrary set and let $P = \mathfrak{P}(A)$ be its powerset. For $x, y \in P$ define

$$x + y = (x - y) \cup (y - x)$$

$$x * y = x \cap y$$

Thus addition is symmetric difference and multiplication is plain set-theoretic intersection. In terms of logic, addition is “exclusive or,” and multiplication is “and.”

Proposition

$\langle \mathfrak{P}(A), +, *, \emptyset, A \rangle$ is a commutative ring.

Exercise

Prove the proposition.

Fields

Definition

A **field** \mathbb{F} is a ring in which the multiplicative monoid $\langle F^*, \cdot, 1 \rangle$ forms a commutative group.

In other words, every non-zero element is already a unit. As a consequence, in a field we can always solve linear equations

$$a \cdot x + b = 0$$

provided that $a \neq 0$: the solution is $x_0 = -a^{-1}b$. In an arbitrary ring the inverse of a may or may not exist.

As we will see, this additional condition makes fields much more constrained than arbitrary rings. By the same token, they are also much more manageable.

Axiomatization

We have seen how to axiomatize monoids and groups in a purely equational fashion, using a unary function symbol $^{-1}$ to denote the inverse function.

Note, though, that this does not work for fields: the inverse operation is partial and we need to guard against argument 0:

$$x \neq 0 \Rightarrow x * x^{-1} = 1$$

One can try to pretend that inverse is total and explore the corresponding axiomatization; this yields a structure called a “meadow.”

Finite Integral Domains

Of course, every field is an integral domain. In the finite case the opposite implication also holds.

First note that in every integral domain we have multiplicative cancellation: $ab = ac$ implies $b = c$ whenever $a \neq 0$.

Theorem

Every finite integral domain is already a field.

Proof. Let $a \neq 0 \in R$ and consider our old friend, the multiplicative map $\hat{a} : R^* \rightarrow R^*$, $\hat{a}(x) = ax$.

From the comment above \hat{a} is injective and hence surjective on R^* . But then every non-zero element is a unit: $ab = 1$ for some b . □

Examples: Fields

Example

In calculus one always deals with the following fields: the rationals \mathbb{Q} , the reals \mathbb{R} , the complex numbers \mathbb{C} .

Example

The modular numbers \mathbb{Z}_m form a field iff m is prime. We can use the Extended Euclidean algorithm to compute multiplicative inverses: obtain two cofactors x and y such that $xa + ym = 1$. Then x is the multiplicative inverse of a modulo m .

Note that we can actually compute quite well in this type of finite field: the elements are trivial to implement and there is a reasonably efficient way to realize the field operations.

Is that It?

So far we have a few infinite fields from calculus ($\mathbb{Q}, \mathbb{R}, \mathbb{C}$) and a family of finite fields from number theory (\mathbb{Z}_m for m prime).

Question:

- Is that already it, or are there other fields?
- In particular, are there other finite fields?

It turns out to be rather surprisingly difficult to come up with more examples of finite fields: none of the obvious construction methods seem to apply here.

Products Fail

One standard method in algebra that produces more complicated structures from simpler one is to form a product (operations are performed componentwise).

This works fine for semigroups, groups, and rings (which all have an equational axiomatization).

Unfortunately, for fields this approach fails. For let

$$F = F_1 \times F_2$$

where F_1 and F_2 are two fields. Then F is a ring, but never a field: the element $(0, 1) \in F$ is not $(0, 0)$, and so would have to have an inverse (a, b) .

But $(0, 1)(a, b) = (0, b) \neq (1, 1)$, so this does not work.

Quotient Fields

Here is one fairly general construction that turns a well-behaved ring into a field. It is often used to construct the rationals from the integers.

Suppose R is an integral domain. Define an equivalence relation \approx on $R \times R^*$ by

$$(r, s) \approx (r', s') \iff rs' = r's.$$

One usually writes the equivalence classes of $R \times R^*$ in fractional notation:

$$\frac{r}{s} \quad \text{for } (r, s) \in R \times R^*.$$

Note that for example $\frac{12345}{6789} = \frac{4115}{2263}$.

Operations

Now define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Lemma

$\langle R \times R^*, +, \cdot, 0, 1 \rangle$ is a field, the so-called *quotient field* of R . Here 0 is short-hand for $0/1$ and 1 for $1/1$.

Exercise

Prove the lemma. Check that this is really the way the rationals are constructed from the integers. Why is it important that the original ring is an integral domain?

Computing in a Quotient Field

How hard is it to implement the arithmetic in the quotient structure?

Not terribly, we can just use the old ring operations. For example, using the best known algorithm (for integer multiplication) we can multiply two rationals in $O(n \log n \log \log n)$ steps.

But there is a significant twist: since we are really dealing with equivalence classes there is the eternal problem of picking canonical representatives.

For example, in the field of rationals $12345/6789$ is the same as $4115/2263$ though the two representations are definitely different.

The second one in lowest common terms is preferred – but requires extra computation: we need to compute and divide by the GCD.

The Truth

Rational arithmetic can be used to approximate real arithmetic, but for really large applications it is actually not necessarily such a great choice:

- Addition of rationals requires 3 integer multiplications, 1 addition plus one normalization (GCD followed by division).
- Multiplication of rationals requires 2 integer multiplications, plus one normalization (GCD followed by division).

This is bad enough, in particular for addition, for people to have developed alternatives, for example p -adic arithmetic. We won't pursue this.

Rational Function Fields

A particularly interesting case of the quotient construction starts with a polynomial ring $R[x]$. Let us assume that $R[x]$ is an integral domain. If we apply the fraction construction to $R[x]$ we obtain the so-called **rational function field** $R(x)$:

$$R(x) = \left\{ \frac{p(x)}{q(x)} \mid p, q \in R[x], q \neq 0 \right\}$$

or, more precisely, the corresponding equivalence classes.

Performing arithmetic operations in $R(x)$ requires no more than standard polynomial arithmetic.

Incidentally, fields used to be called rational domains, this construction is really a classic.

The Classical Example

$R(x)$ is, in a sense, the smallest field containing both R and x .

Alarm: What on earth is the “unknown” x ?

It doesn't actually exist, right?

Here is an example that is a bit easier to deal with. Consider the rational polynomial

$$f(x) = x^2 - 2 \in \mathbb{Q}[x]$$

Clearly, this polynomial has no roots over \mathbb{Q} , we cannot solve the equation $f(x) = 0$ in the rationals.

The real challenge is to construct a field (field of dreams?) that has enough elements to solve this equation. For motivation, let's cheat and exploit the fact that we already know about the reals $\mathbb{R} \supseteq \mathbb{Q}$.

Adjoining a Root

Over the reals there is, of course, no problem: we can take the root $\sqrt{2} \in \mathbb{R}$ and work in

$$\mathbb{Q}(\sqrt{2}) = \text{least subfield of } \mathbb{R} \text{ containing } \mathbb{Q}, \sqrt{2}$$

Terminology: We **adjoin** $\sqrt{2}$ to \mathbb{Q} .

- So what is the structure of $\mathbb{Q}(\sqrt{2})$?
- How do we actually compute in this field?

Adjoining Root of 2

First note that since a subfield is closed under addition and multiplication we must have $p(\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$ for any polynomial $p \in \mathbb{Q}[x]$.

But $\sqrt{2}^2 = 2$, so any polynomial expression $p(\sqrt{2})$ actually simplifies to $a + b\sqrt{2}$:

$$P = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{Q}(\sqrt{2})$$

Clearly, P is closed under addition, subtraction and multiplication.

But can we divide in P ? We need coefficients c and d such that

$$(a + b\sqrt{2})(c + d\sqrt{2}) = 1$$

provided that $ab \neq 0$. Since $\sqrt{2}$ is irrational this means

$$ac + 2bd = 1$$

$$ad + bc = 0$$

Field Operations

Solving the system for c and d we get

$$c = \frac{a}{a^2 - 2b^2} \quad d = \frac{-b}{a^2 - 2b^2}$$

Note that the denominators are not 0 since $ab \neq 0$ and $\sqrt{2}$ is irrational.

Hence $P = \mathbb{Q}(\sqrt{2})$ and we really obtain a field just from polynomials.

Moreover, we can implement the field operations entirely based on the field operations of \mathbb{Q} : we just need a few multiplications and divisions of rationals.

Getting Rid of Numerators

Now consider $\mathbb{Q}(\sqrt{2})$: at $\sqrt{2}$ all polynomials over \mathbb{Q} evaluate to an expression of the form $a + b\sqrt{2}$.

But we don't need the denominators since

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} = r + s\sqrt{2}$$

for rational r and s .

From the algorithmic point of view this means that we only need polynomial arithmetic, nothing else (not even the modest complication introduced by the quotient field construction).

Adjoining Roots

More generally, suppose we have two fields $\mathbb{F} \subseteq \mathbb{K}$ and a polynomial $f(x)$ over \mathbb{F} that has a root α in \mathbb{K} .

Theorem

The least field containing \mathbb{F} and a root α of $f(x)$ is

$$\mathbb{F}(\alpha) = \{ g(\alpha) \mid g \in \mathbb{F}[x] \}$$

Again: What's surprising here is that polynomials are enough. If we let g range over all rational functions with coefficients in \mathbb{F} the result would be trivial – and much less useful.

We won't give a full proof; always think about adjoining $\sqrt{2}$ as an example.

- Rings and Fields

2 Finite Fields

- Ideals
- The Structure theorem

Finite Fields

As we have seen, the ring of modular numbers \mathbb{Z}_p is a field whenever p is a prime.

The question arises whether there are any other finite models for the field axioms.

*AMS Subject Classification: 11Txx,
together with Number Theory.*

There are, and they are the basis for GPS, a good part of coding theory and many efficient pseudo-random number generators. Alas, it takes a bit of work to construct them.

One way to explain these finite fields is to go back to the roots (no pun intended) of field theory: solving polynomial equations.

Classification

Is there any kind of neat classification scheme for (finite) fields, a way to organize them into a nice taxonomy? For infinite fields this is rather difficult, but for finite fields we can carry out a complete classification relatively easily. Here is the first distinguishing criterion.

Definition

The **characteristic** of a ring R is defined by

$$\text{char}(R) = \begin{cases} \min(k > 0 \mid \overbrace{1 + \dots + 1}^k = 0) & \text{if } k \text{ exists,} \\ 0 & \text{otherwise.} \end{cases}$$

In calculus characteristic 0 is the standard case: $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ all have characteristic 0. But in computer science rings of positive characteristic are very important.

Positive Characteristic

Note that characteristic 0 implies that the ring is infinite: there are infinitely many elements of the form $1 + 1 + \dots + 1$.

But the converse is quite false: the powerset ring from above has characteristic 2 and is wildly infinite if the ground set is infinite.

At any rate, we will consider rings with positive characteristic from now on.

The classical example is \mathbb{Z}_m , a ring with characteristic m .

To get an integral domain we need m to be a prime, so prime characteristic will be important to us.

Structure Theorem

We will see that all finite fields have a simple, uniform description (unlike, say, all finite groups which are horrendously complicated).

Theorem

Every finite field \mathbb{F} has cardinality p^k where p is prime and the characteristic of \mathbb{F} , and $k \geq 1$.

Moreover, for every p prime and $k \geq 1$ there is a finite field of cardinality p^k and all fields of cardinality p^k are isomorphic.

From the computational angle it turns out that we can perform the field operations very effectively, in particular in some cases that are important for applications.

We will not prove the whole theorem, but we will make a few dents in it – dents that are also computationally relevant.

The Prime Subfield

Suppose \mathbb{F} is an arbitrary finite field and let $p > 0$ be the characteristic of \mathbb{F} .

Consider

$$P = \left\{ \sum_k 1 \mid k \geq 0 \right\} \subseteq \mathbb{F}.$$

Claim

P is the smallest subfield of \mathbb{F} .

Proof.

P has cardinality p since $\sum_k 1 = \sum_{k \bmod p} 1$.

Moreover, P is closed under addition and multiplication and thus forms a subring. Since \mathbb{F} is an integral domain P must also be an integral domain. But then P is actually a subfield and p must be prime. \square

In other words, every finite field contains a subfield of the form \mathbb{Z}_p where p is prime and p is the characteristic of the field. So the real problem is to determine the rest of the structure.

The Linear Algebra Angle

Given the prime subfield $\mathbb{Z}_p = \mathbb{K} \subseteq \mathbb{F}$, the trick is to think of \mathbb{F} as a **vector space** over \mathbb{K} :

$$\mathbb{F} \cong \mathbb{Z}_p^k = \mathbb{Z}_p \times \mathbb{Z}_p \times \dots \times \mathbb{Z}_p.$$

Addition on these vectors (the addition in \mathbb{F}) comes down addition in \mathbb{Z}_p and thus to modular arithmetic: vector addition is pointwise.

So addition is trivial in a sense. Alas, multiplication is a bit harder to explain.

At any rate, it follows from linear algebra that the cardinality of \mathbb{F} must be p^k for some k .

Cyclic Multiplicative Group

Lemma

The multiplicative subgroup of any finite field is cyclic.

To see this, recall that the **order** of a group element was defined as

$$\text{ord}(a) = \min(e > 0 \mid a^e = 1).$$

For finite groups e always exists.

A group $\langle G, \cdot, 1 \rangle$ is **cyclic** if it has a generator: for some element a :
 $G = \{ a^i \mid i \in \mathbb{Z} \}.$

In the finite case this means $G = \{ a^i \mid 0 \leq i < \alpha \}$ where α is the order of a .

Proposition (Lagrange)

For finite G and every element $a \in G$: $\text{ord}(a)$ divides $|G|$.

Proof of lemma

Let m be the maximal order in \mathbb{F}^* , n the size of \mathbb{F}^* , so $m \leq n$. We need to show that $m = n$.

First assume that every element of \mathbb{F}^* has order dividing m . Then the polynomial $z^m - 1 \in \mathbb{F}[z]$ has n roots in \mathbb{F} since letting p be the order of an element and $m = pq$ we have

$$z^{pq} - 1 = (z^{p(q-1)} + z^{p(q-2)} + \dots + 1)(z^p - 1)$$

But then $n \leq m$ since a degree m polynomial can have at most m roots. Hence $m = n$.

Odious Second Case

Otherwise we can pick $a \in \mathbb{F}^*$ of order m and $b \in \mathbb{F}^*$ of order l not dividing m . Then by basic arithmetic there is a prime q such that

$$m = q^s m_0 \quad l = q^r l_0 \quad s < r$$

where q is coprime to l_0 and m_0 .

Set

$$a' = a^{q^s} \quad b' = b^{l_0}$$

Then a' has order m_0 , and b' has order q^r .

But then $a'b'$ has order $q^r m_0 > m$, contradiction. □

Who Cares?

Given the fact that \mathbb{F}^* is cyclic, there is an easy way to generate the field (let's ignore 0).

- Find a generator g of \mathbb{F}^* .
- Compute all powers of g .

Of course, this assumes that we can get our hands on a generator g . Note that multiplication is trivialized in the sense that $g^i * g^j = g^{i+j \bmod n}$.

Of course, we need be able to rewrite the field elements as powers of g . This is known as the discrete logarithm problem and quite difficult.

Implementation Woes

As far as a real implementation is concerned we are a bit stuck at this point: we can represent a finite field as a vector space which makes addition easy.

Or we can use powers of a generator to get easy multiplication.

Nice, but we need to be able to freely mix both operations. Alas, it is not clear what

$$g^i + g^j$$

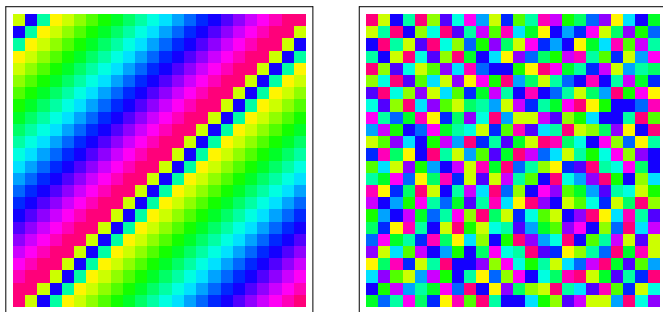
or

$$(a_1, \dots, a_k) * (b_1, \dots, b_k)$$

should be.

Frivolous Picture

A little color: two pictures of the multiplication table for \mathbb{F}_{25} .



On the left, elements are ordered as powers of the generator (so the picture proves that the group is cyclic), on the right we have lexicographic ordering. It's important to look at the right picture.

- Rings and Fields

- Finite Fields

- ③ Ideals

- The Structure theorem

Back to the Roots

Time to get serious about constructing a finite field.

Recall the construction of $\mathbb{Q}(\sqrt{2})$ from above, adding a solution to $x^2 - 2 = 0$ to the rationals. It turned out that we need to consider only polynomials, rather than the rational functions one might expect.

$$\begin{aligned}\mathbb{Q}(\sqrt{2}) &= \{ p(\sqrt{2}) \mid p \in \mathbb{Q}[x] \} \\ &= \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}\end{aligned}$$

One way of thinking about this is that we used a simplification rule:

$$x^2 \rightsquigarrow 2$$

on $\mathbb{Q}[x]$ to produce $\mathbb{Q}(\sqrt{2})$.

The critical point here is that rational polynomials, together with this rule, produce the right set of elements and the algebraic operations. Note that x does not simplify. In fact, in this new structure, x is the root we are looking for (yes, that sounds wacky).

Generalizing $\sqrt{2}$

Is there a way we can use a similar approach to adjoin a root of some polynomial to \mathbb{F}_2 to get a larger finite field?

Lets consider the polynomial

$$f = x^2 + x + 1 \in \mathbb{F}_2[x]$$

Clearly, f has no root over \mathbb{F}_2 .

Unlike the $\sqrt{2}$ example it is absolutely unclear what a solution to the equation $f = 0$ should be.

So how do we adjoin a root for f ?

The Rewrite Rule

We would like $x^2 + x + 1 = 0$, so we use the simplification rule

$$x^2 \rightsquigarrow x + 1$$

(we are dealing with characteristic 2 so plus is minus). What happens to $\mathbb{F}_2[x]$ if we apply this rule systematically?

$$\begin{aligned}x^6 + x^3 + x + 1 &\rightsquigarrow (x + 1)^3 + x(x + 1) + x + 1 \\ &\rightsquigarrow (x^3 + x^2 + x + 1) + (x^2 + x) + x + 1 \\ &\rightsquigarrow x(x + 1) + (x + 1) + 1 \\ &\rightsquigarrow x + 1\end{aligned}$$

Applying the rule systematically to any polynomial will ultimately produce a polynomial of degree at most 1: any higher order term could be further reduced.

The Crucial Point

In general, if we start with a polynomial of degree d we can reduce everything down to polynomials of degree at most $d - 1$.

Since the coefficients come from a finite field there are only finitely many such polynomials; in fact there are q^d where q is the size of the field.

But we don't just get a bunch a of polynomials, we also get the operations that turn them into a field:

- Addition is addition of polynomials in $\mathbb{F}[x]$.
- Multiplication is multiplication of polynomials in $\mathbb{F}[x]$ followed by a reduction: we have to apply the simplification rule until we get back to a polynomial of degree less than d .

Here is a more algebraic description of this process.

Taking Simplification Seriously

The simplification rule $x^2 \rightsquigarrow x + 1$ has lots of algebraic consequences. For example, for any polynomial $P \in \mathbb{F}_2[x]$ we must have

$$P + x^2 \rightsquigarrow P + (x + 1)$$

$$P \cdot x^2 \rightsquigarrow P \cdot (x + 1)$$

If we consider all these consequences we obtain an equivalence relation on polynomials that is compatible with the structure of the ring of polynomials.

The quotient ring then turns out to be the field we are looking for.

Ideals

Let's make this notion of an equivalence relation more precise.

Definition

Let R be a commutative ring. An **ideal** $I \subseteq R$ is a subset that is closed under addition and under multiplication by arbitrary ring elements: $a \in I, b \in R$ implies $ab \in I$.

So an ideal is more constrained than a subring: it has to be closed by multiplication from the outside. Ideals are hugely important since they allow us to form a quotient structure:

$$a = b \pmod{I} \quad \text{iff} \quad a - b \in I.$$

Arithmetic in this quotient structure is well-behaved since I is an ideal. E.g.

$$a = b, c = d \pmod{I} \quad \Rightarrow \quad ac = bd \pmod{I}$$

Generating Ideals

What is the smallest ideal containing a particular element $r \in R$?

All we need is the multiples of r :

$$(r) = \{xr \mid x \in R\}$$

the ideal **generated** by r .

Exercise

Show that $(r) \subseteq R$ is indeed closed under addition and multiplication by ring elements.

This should sound eminently familiar.

Modular Arithmetic Revisited

Familiar example: to describe modular arithmetic we have $R = \mathbb{Z}$ as ground ring and use the ideal $I = (m) = m\mathbb{Z}$.

$$a = b \pmod{I} \quad \text{iff} \quad m \mid (a - b).$$

The ideal I is generated by the modulus m and the quotient ring $\mathbb{Z}/(m)$ is finite in this case.

Moreover, the quotient ring is a field iff m is prime.

Irreducible Polynomials

Ideals provide the right type of equivalence relation for the construction of a finite field from a polynomial ring. Alas, the ideals cannot be chosen arbitrarily, we need to start from special polynomials, in analogy to m being prime in the integer case.

Definition

A polynomial is **irreducible** if it is not the product of polynomials of smaller degree.

Irreducibility is necessary when we try to construct a field $\mathbb{F}[x]/(f)$: otherwise we do not even get an integral domain.

For suppose $f(x) = f_1(x)f_2(x)$ where both f_1 and f_2 have degree at least 1. Then $1 \leq \deg(f_i) < \deg(f)$, so neither f_1 or f_2 can be simplified in $\mathbb{F}[x]/(f)$. In particular both elements in $\mathbb{F}[x]/(f)$ are non-zero, but their product is zero.

Existence

How many irreducible polynomials are there?

Lemma

Suppose \mathbb{F} is a finite field of cardinality q . Then the number of irreducible polynomials in $\mathbb{F}[x]$ of degree d is

$$N_d^q = \frac{1}{d} \sum_{k|d} \mu(d/k) \cdot q^k$$

Here μ is the Möbius function. At any rate, there are quite a few irreducible polynomials.

$$\begin{array}{c|cccccccccc}
 d & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
 N_d^2 & 2 & 1 & 2 & 3 & 6 & 9 & 18 & 30 & 56 & 99
 \end{array}$$

Of course, there is another problem: how do we construct them? Factorization of polynomials is the natural approach (much like prime decomposition), let's not get involved at this point.

Modular Arithmetic for Polynomials

Suppose \mathbb{F} is a field and consider an irreducible polynomial $f(x)$ and the ideal $(f(x)) = f(x)\mathbb{F}[x]$ that it generates.

What does modular arithmetic look like with respect to I ?

We identify two polynomials when their difference is divisible by f :

$$h(x) = g(x) \pmod{f(x)} \iff f(x) \mid (h(x) - g(x))$$

Let d be the degree of f .

Note that any polynomial h is equivalent to a polynomial g of degree less than d : write $h(x) = q(x)f(x) + g(x)$ by polynomial division.

A Harder Example

Over \mathbb{F}_2 , the polynomial

$$f(x) = x^3 + x + 1$$

is irreducible.

Note that unlike with the earlier square root example it is absolutely not clear what a root of $f(x) = 0$ should look like.

In order to manufacture a root, we want to compute in the polynomial ring $\mathbb{F}_2[x]$ modulo the ideal $I = (f(x))$ generated by f .

There are two steps:

- Find a good representation for $\mathbb{F}_2[x]/I$.
Comes down to picking a representative in each equivalence class.
- Determine how to perform addition, multiplication and division on these representatives.

Representatives

Note that

$$x^3 = x + 1 \pmod{I}$$

(we have characteristic 2, so minus is plus) so we can eliminate all monomials of degree at least 3:

$$x^{3k+r} \rightarrow (x+1)^k x^r.$$

If necessary, apply this substitution repeatedly.

In the end, we are left with 8 polynomials modulo I , namely all the polynomials of degree at most 2:

$$\mathbb{K} = \{0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2\}$$

The Root

We write α for (the equivalence class of) x for emphasis.

Then $\alpha \in \mathbb{K}$ really is a root of $f(x) = 0$ in the extension field \mathbb{K} .

For

$$f(\alpha) = x^3 + x + 1 = 0 \pmod{I}$$

Yes, this is a bit of comedown.

But, it's really no different from the $\sqrt{2}$ example, just less familiar.

Representatives II

The representatives are just all polynomial of degree less than 3.

$$c_2x^2 + c_1x + c_0$$

where $c_i \in \mathbb{F}_2$.

Algebraically, it is usually best to think of the extension field $\mathbb{F}_2 \subseteq \mathbb{K}$ as a quotient structure, as the polynomials modulo f :

$$\mathbb{K} = \mathbb{F}_2[x]/(f(x))$$

Addition

But we can also think about the coefficient lists of these polynomials. Since the representatives are of degree at most 2 we are dealing with triples of elements of \mathbb{F}_2 .

In this setting the additive structure is trivial: it's just componentwise addition of these triples mod 2.

$$(c_2, c_1, c_0) + (c'_2, c'_1, c'_0) = (c_2 + c'_2, c_1 + c'_1, c_0 + c'_0)$$

So the additive group of these fields is just a Boolean group.

Note that this operation is trivial to implement (xor on bit-vectors, can even be done in 32 or 64 bit blocks).

Multiplication

How about multiplication? Since multiplication increases the degree, we can't just multiply out, but we have to simplify using our rule $x^3 \rightarrow x + 1$ afterwards.

The product

$$(c_2, c_1, c_0) \cdot (c'_2, c'_1, c'_0)$$

is given by the triple

$$\begin{aligned} & c_2 c'_0 + c_1 c'_1 + c_0 c'_2 + c_2 c'_2 \\ & c_1 c'_0 + c_0 c'_1 + c_2 c'_1 + c_1 c'_2 + c_2 c'_2 \\ & c_0 c'_0 + c_2 c'_1 + c_1 c'_2 \end{aligned}$$

This is a bit messy. And it gets more messy when we deal with larger degree polynomials.

Multiplicative Structure

Recall that α is the equivalence class of x . Then the powers of α are:

$$\alpha^0 = 1 \qquad = (0, 0, 1)$$

$$\alpha^1 = \alpha \qquad = (0, 1, 0)$$

$$\alpha^2 = \alpha^2 \qquad = (1, 0, 0)$$

$$\alpha^3 = \alpha + 1 \qquad = (0, 1, 1)$$

$$\alpha^4 = \alpha^2 + \alpha \qquad = (1, 1, 0)$$

$$\alpha^5 = \alpha^2 + \alpha + 1 \qquad = (1, 1, 1)$$

$$\alpha^6 = \alpha^2 + 1 \qquad = (1, 0, 1)$$

$$\alpha^7 = 1$$

Note: this table determines the multiplicative structure completely.

Table of Inverses

We really obtain a field this way, not just a ring (recall that f is irreducible).

	h	h^{-1}
1	1	1
2	α	$1 + \alpha^2$
3	α^2	$1 + \alpha + \alpha^2$
4	$1 + \alpha$	$\alpha + \alpha^2$
5	$1 + \alpha^2$	α
6	$\alpha + \alpha^2$	$1 + \alpha$
7	$1 + \alpha + \alpha^2$	α^2

Note that this table defines an involution: $(h^{-1})^{-1} = h$.

- Rings and Fields
- Finite Fields
- Ideals
- ④ The Structure theorem

The Structure of Finite Fields

Recall our big theorem:

Theorem

Every finite field \mathbb{F} has cardinality p^k where p is prime and the characteristic of \mathbb{F} , and $k \geq 1$. Moreover, for every p prime and $k \geq 1$ there is a finite field of cardinality p^k and all fields of cardinality p^k are isomorphic.

So there are three assertions to prove:

- Every finite field \mathbb{F} has cardinality p^k where p prime is the characteristic of \mathbb{F} .
- There is a field of cardinality p^k .
- All fields of cardinality p^k are isomorphic.

Proof Sketch

We have already taken care of parts 1 and 2:

- 1 Since \mathbb{F} is finite vector space over \mathbb{Z}_p where p is the characteristic of \mathbb{F} it must have size p^k , p prime, $k \geq 1$.
- 2 Since there are irreducible polynomials over \mathbb{Z}_p of degree k for any k we can always construct a finite field of the form $\mathbb{Z}_p[x]/(f)$ of size p^k .

What is absolutely unclear is they all should be the same (isomorphic).

For example, suppose we pick two irreducible polynomials f and g of degree k .

Since multiplication is determined by f and g there is no obvious reason that we should have

$$\mathbb{Z}_p[x]/(f) \cong \mathbb{Z}_p[x]/(g)$$

Homomorphisms and Kernels

Let's collect some tools to compare rings and fields.

Definition

Let R and S be two rings and $f : R \rightarrow S$. f is a **ring homomorphism** if

$$f(g + h) = f(g) + f(h) \quad \text{and} \quad f(gh) = f(g)f(h).$$

If f is in addition injective/surjective/bijective we speak about monomorphisms, epimorphism and isomorphisms, respectively. The **kernel** of a ring homomorphism is the set of elements that map to 0.

Notation: **$\ker(f)$** .

Note that $f(0) = 0$.

It is easy to see that the kernel of any ring homomorphism $f : R \rightarrow S$ is an ideal in R .

Since $f(x) = f(y)$ iff $x - y \in \ker(f)$ a ring homomorphism is a monomorphism iff its kernel is trivial: $\ker(f) = \{0\}$.

Rings with 1

When the rings in question have a multiplicative unit one also requires

$$f(1) = 1$$

(unital ring homomorphisms). This is in particular the case when dealing with fields.

Lemma

If $f : \mathbb{F} \rightarrow \mathbb{K}$ is a field homomorphism then f is injective.

Proof.

$\ker(f) \subseteq \mathbb{F}$ is an ideal. But in a field there are only two ideals: $\{0\}$ and the whole field. Since $f(1) = 1$, 1 is not in the kernel, so the kernel must be $\{0\}$ and f is injective.

□

The Frobenius Homomorphism

Here is a somewhat surprising example of a homomorphism.

Definition

Let R be a ring of characteristic $p > 0$. The **Frobenius homomorphism** is defined by the map $R \rightarrow R$, $x \mapsto x^p$.

The Frobenius map is indeed a ring homomorphism since R has characteristic p :

$$(a + b)^p = a^p + b^p.$$

Over a finite field we even get an automorphism. The orbits of a non-zero element look like

$$a, a^p, a^{p^2}, \dots, a^{p^{k-1}}$$

Exercise

Use the binomial theorem to prove the the Frobenius map is a homomorphism.

Establishing Isomorphisms

The following fact is often useful to establish an isomorphism. Suppose $f : R \rightarrow S$ is an epimorphism (no major constraint, otherwise replace S by the range of f). Then $R/\ker(f)$ is isomorphic to S .

For example, we can use this technique can be used to prove our old theorem that give a polynomial characterization for field extensions by adjoining roots.

More precisely, let $\mathbb{F}(\alpha)$ be the smallest field $\mathbb{F} \subseteq \mathbb{F}(\alpha) \subseteq \mathbb{K}$ that contains a root $\alpha \in \mathbb{K}$ of some polynomial $f \in \mathbb{F}[x]$. Then

$$\mathbb{F}(\alpha) = \{ g(\alpha) \mid g \in \mathbb{F}[x] \}$$

rather than, say, the collection of rational functions over \mathbb{F} evaluated at α .

Adjoining a Root, contd.

To see why, note that the right hand side is the range of the evaluation map

$$\begin{aligned}\nu: \mathbb{F}[x] &\longrightarrow \mathbb{K} \\ \nu(g) &\mapsto g(\alpha)\end{aligned}$$

that evaluates g at α , producing a value in \mathbb{K} . It is easy to check that ν is a ring homomorphism and clearly $(f) \subseteq \ker(\nu)$.

We may safely assume that f is monic and has minimal degree in $\mathbb{F}[x]$ of all polynomials with root α . Then f is irreducible and we have

$$\ker(\nu) = \{p \in \mathbb{F}[x] \mid f \text{ divides } p\} = (f)$$

This shows that the range of ν is isomorphic to $\mathbb{F}[x]/(f)$ and hence a field.

Irreducibility is essential here, otherwise $f(x) = (x^2 - 2)(x^2 - 3) = x^4 - 5x^2 + 6$ with $\alpha = \sqrt{2}$ over $\mathbb{F} = \mathbb{Q} \subseteq \mathbb{C} = \mathbb{K}$ would produce a non-integral domain.

Kernels, The Idea

Note that this is the third time we encounter kernels.

- For a general function $f : A \rightarrow B$ the kernel relation is given by $f(x) = f(y)$.
- For a group homomorphism $f : A \rightarrow B$ the kernel is given by $\{x \in A \mid f(x) = 1\}$.
- For a ring homomorphism $f : A \rightarrow B$ the kernel is given by $\{x \in A \mid f(x) = 0\}$.

In the last two cases we can easily recover the classical kernel relation and the definition as stated turns out to be more useful.

Still, there is really just one idea.

Uniqueness

Back to the problem of showing that there is only “one” finite field \mathbb{F}_{p^k} of size p^k . To understand finite fields completely we need just one more idea.

Definition

Let $f \in \mathbb{F}[x]$ monic, $\mathbb{F} \subseteq \mathbb{K}$. Field \mathbb{K} is a **splitting field** of f if

- $f(x) = (x - \alpha_1) \dots (x - \alpha_d)$ in $\mathbb{K}[x]$, and
- $\mathbb{K} = \mathbb{F}(\alpha_1, \dots, \alpha_d)$.

Needless to say, the $\alpha_i \in \mathbb{K}$ are exactly the roots of f . Thus, in a splitting field we can decompose the polynomial into linear factors.

Moreover, there are no more elements in \mathbb{K} , by adjoining all the roots of f we get all of \mathbb{K} .

Examples

Example

\mathbb{C} is the splitting field of $x^2 + 1 \in \mathbb{R}[x]$.

It is more than surprising that over \mathbb{C} any non-constant real polynomial can already be decomposed into linear factors, everybody splits already.

Example

Consider $f(x) = x^8 + x \in \mathbb{F}_2[x]$. Then

$$f(x) = x(x+1)(x^3+x^2+1)(x^3+x+1)$$

Adjoining one root of $g(x) = x^3 + x + 1$ already produces the splitting field of f : the other irreducible factor of degree 3 also splits.

Example contd.

$$x^8 + x = x(x+1)(x^3 + x^2 + 1)(x^3 + x + 1)$$

element	root of
0	x
α^0	$x + 1$
α^1	$x^3 + x + 1$
α^2	$x^3 + x + 1$
α^3	$x^3 + x^2 + 1$
α^4	$x^3 + x + 1$
α^5	$x^3 + x^2 + 1$
α^6	$x^3 + x^2 + 1$

Splitting Field theorem

Theorem (Splitting Field Theorem)

For any irreducible polynomial there exists a splitting field, and any two such splitting fields are isomorphic.

We have all the tools to construct a splitting field, so existence is not very hard.

But the uniqueness proof is quite involved.

Basic problem: what would happen in the last example if we had chosen $x^3 + x + 1$ rather than $x^3 + x^2 + 1$? We get isomorphic vector spaces, but why should the multiplicative structure be the same?

The Bible:

R. Lidl, H. Niederreiter

Introduction to Finite Fields and their Applications

Cambridge University Press, 1986.

Finite Fields Explained

Now we can pin down the structure of all finite fields.

Theorem

There is a unique (up to isomorphism) finite field of size p^k .

Proof.

Let $n = p^k$ and consider $f(x) = x^n - x \in \mathbb{F}_p[x]$.

Has n roots, which form a field. For let a and b two roots, then:

$$f(a + b) = (a + b)^n - (a + b) = a^n - a + b^n - b = 0$$

$$f(ab) = (ab)^n - (ab) = a^n b^n - ab = 0$$

Hence the roots form the splitting field of f . By the Splitting Field theorem this field is unique up to isomorphism. □

Example: The Field \mathbb{F}_{5^2}

Consider characteristic $p = 5$ and $k = 2$.

$$\begin{aligned}x^{25} - x &= x(1+x)(2+x)(3+x)(4+x) \\ &(2+x^2)(3+x^2)(1+x+x^2)(2+x+x^2)(3+2x+x^2)(4+2x+x^2) \\ &\quad (3+3x+x^2)(4+3x+x^2)(1+4x+x^2)(2+4x+x^2)\end{aligned}$$

There are 10 irreducible quadratic polynomials to choose from.

Which one should we pick?

Primitive Polynomials

Definition

Let \mathbb{F} be a field of characteristic $p > 0$ and $f \in \mathbb{F}[x]$ irreducible of degree k . f is **primitive** if $x \bmod f$ is a generator of the multiplicative subgroup in the extension field $\mathbb{F}[x]/(f)$. The roots of a primitive polynomial are also called primitive.

Since the size of the multiplicative subgroup is $p^k - 1$ there must be $\Phi(p^k - 1)$ generators (where Φ is Euler's totient function).

Since any of the roots of a corresponding primitive polynomial is a generator the number of primitive polynomials of degree k is

$$\frac{\Phi(p^k - 1)}{k}$$

For example, in the case $p = 5$, $k = 2$ there are 8 primitive elements and 4 polynomials.

The Order of a Polynomial

There is an alternative way to describe primitive polynomials that avoid references to the extension field construction.

Definition

Let $f \in \mathbb{F}[x]$ such that $f(0) \neq 0$. The **order** of f is the least exponent e such that f divides $x^e - 1$.

In other words, $x^e = 1 \pmod{f}$.

So an irreducible f is primitive iff it has order $p^k - 1$ where p is the characteristic and k the degree of f .

The Field \mathbb{F}_{5^2} , contd.

For example, $f = 2 + 4x + x^2$ is primitive.

α	x	α^{13}	$4x$
α^2	$3 + x$	α^{14}	$2 + 4x$
α^3	$3 + 4x$	α^{15}	$2 + x$
α^4	$2 + 2x$	α^{16}	$3 + 3x$
α^5	$1 + 4x$	α^{17}	$4 + x$
α^6	2	α^{18}	3
α^7	$2x$	α^{19}	$3x$
α^8	$1 + 2x$	α^{20}	$4 + 3x$
α^9	$1 + 3x$	α^{21}	$4 + 2x$
α^{10}	$4 + 4x$	α^{22}	$1 + x$
α^{11}	$2 + 3x$	α^{23}	$3 + 2x$
α^{12}	4	α^{24}	1

So $\mathbb{F}_{5^2}^*$ is indeed cyclic with generator α , and \mathbb{F}_{5^2} has dimension 2 as a vector space over \mathbb{F}_5 , as required.

Galois Fields

“The” finite field of size p^k is often called the **Galois field** of size p^k in honor of Evariste Galois (1811-1832).

Written \mathbb{F}_{p^k} or $\text{GF}(p^k)$.



Summary

- Finite fields have a very rich theory (unlike rings where it is much harder to prove sweeping theorems).
- FFs can be used in cryptographic schemes.
- FFs are important for the design of codes (and more generally for many combinatorial design problems).
- FFs are important for efficient pseudo-random number generation.
- Implementation leads to lots of interesting algorithmic problems.