# CDM

# Finite Fields

Klaus Sutner
Carnegie Mellon University

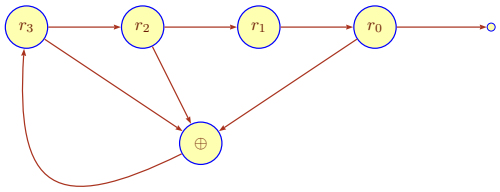
40-ffields 2017/12/15 23:16





## Where Are We? 3

We have empirical evidence that feedback shift registers can be used to produce bit-sequences with very long periods.




But, we need proof: running experiments is unrealistic, even if the FSR is implemented in hardware. We'll need a bit of finite field theory for this.

## Rings and Field 4

### 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 (not necessarily commutative),
- 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 5

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.

One can relax the conditions a bit and deal with rings without a 1: for example, $2\mathbb{Z}$ is a ring without 1. Instead of a multiplicative monoid one has a semigroup.

For our purposes there is no need for this, we will always assume that we have ring elements $0 \neq 1$.

## Examples: Rings 6

### 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 a new ring 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 $n = 1$.

## Annihilators, Inverses and Units



### Definition

A ring element $a$ is an annihilator if for all $x$: $xa = ax = a$.

An inverse $u'$ of a ring element $u$ is any element such that $uu' = u'u = 1$.

A ring element $u$ is called a unit if it has an inverse $u'$.

### Proposition

*$0$ is an annihilator in any ring.*

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

## Inverses



Note that an annihilator cannot be a unit.

For suppose $aa' = 1$. But then $a = 1$, contradiction.

The multiplicative $1$ in a ring is uniquely determined: $1 = 1 \cdot 1' = 1'$.

### Proposition

*If $u$ is a unit, then its inverse is uniquely determined*

*Proof.*

Suppose $uu' = u'u = 1$ and $uu'' = u''u = 1$. Then

$$u' = u'1 = u'uu'' = 1u'' = u''.$$

□

As usual, lots of equational reasoning. And we can write the inverse as $u^{-1}$.

## Integral Domains



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.

Consider $R^\star = R - \{0\}$, so all units are located in $R^\star$.

Then $\langle\, R^\star, \cdot, 1 \,\rangle$ is a monoid in any integral domain.

### Proposition (Multiplicative Cancellation)

*In an integral domain we have $ab = ac$ where $a \neq 0$ implies $b = c$.*

*Proof.* $ab = ac$ iff $a(b - c) = 0$, done. □

## 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)

The ring of modular numbers $\mathbb{Z}_m$ is an integral domain iff $m$ is prime.

### Example (Non-ID)

The ring of $2 \times 2$ real matrices is not an integral domain:

$$\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$$

## A Strange Ring



Arithmetic structures provide the standard examples for rings, but the axioms are much more general than that. Here is a warning not to over-interpret the ring axioms.

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 fact, we can solve systems of linear equations using the standard machinery from linear algebra.

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.

## Examples: Fields



### Example

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

### Example

The modular numbers $\mathbb{Z}_m$ form a field for $m$ 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.

## Axiomatization



Note that one can axiomatize monoids and groups in a purely equational fashion, using a unary function symbol $^{-1}$ to denote an inverse function when necessary.

Alas, 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" which does not quite have the right properties.

## 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 structures with an equational axiomatization: semigroups, monoids, groups, and rings.

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.



## Fractions



The first field one typically encounters in kindergarten is the field of rationals $\mathbb{Q}$.

$\mathbb{Q}$ can be built from the ring of integers by introducing fractions. There is a fairly general and intuitive construction hiding behind this familiar idea.

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

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

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

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

Note that for example

$$\frac{12345}{6789} = \frac{4115}{2263}$$

## Operations



Now define arithmetic operations

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

### Lemma

*$\langle R \times R^\star, +, \cdot, 0, 1 \rangle$ 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 is in lowest common terms and 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 $R(x)$:

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

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. It will be very useful in a moment.

## Fields and Numbers



We are ultimately interested in finite fields, but let's start with the classical number fields

$$\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

where everybody has pretty good intuition.

- $\mathbb{Q}$ is effective: the objects are finite and all operations are easily computable. Alas, upper bounds and limits typically fail to exist.
- $\mathbb{R}$ fixes this problem, but at the cost of losing effectiveness: the carrier set is uncountable, only generalized models of computation apply. Finding reasonable models of actual computability for the reals is a wide open problem.
- $\mathbb{C}$ is quite similar, except that all polynomials there have roots (at the cost of losing order).

## A Challenge



Suppose we want to preserve computability as in $\mathbb{Q}$, but we need to use other reals such as $\sqrt{2} \in \mathbb{R}$. This is completely standard in geometry, and thus in engineering.

### Definition

A complex number $\alpha$ is algebraic if it is the root of a non-zero polynomial $p(x)$ with integer coefficients. $\alpha$ is transcendental otherwise.

$\overline{\mathbb{Q}}$ is the collection of all algebraic numbers.

### Theorem

$\overline{\mathbb{Q}} \subseteq \mathbb{C}$ *forms an effective field.*

Note that transcendental numbers may or may not be computable in some sense; e.g., $\pi$ and $e$ certainly are computable in the right setting. BTW, proving that a number is transcendental is often very difficult.

## A Field?



Note that it is absolutely not clear that the sums and products of algebraic numbers are again algebraic: all we have to define these numbers are rational polynomials, and we cannot simply add and multiply these polynomials.

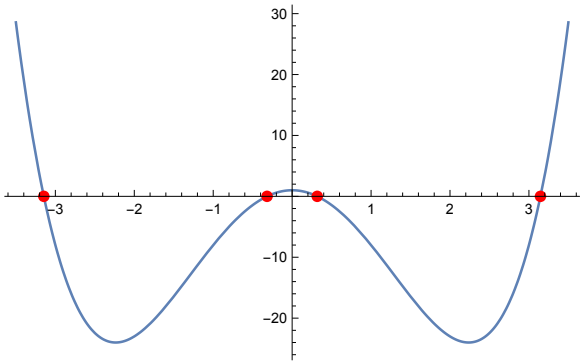
For example, the polynomial for $\sqrt{2} + \sqrt{3}$ is

$$1 - 10x^2 + x^4$$

The polynomial for $1 + \sqrt{2}\sqrt{3}$ is

$$-5 - 2x + x^2$$

The polynomial $1 - 10x^2 + x^4$ has the following 4 real roots:




$$-\sqrt{5+2\sqrt{6}} \qquad \sqrt{2}-\sqrt{3} \qquad \sqrt{5-2\sqrt{6}} \qquad \sqrt{2}+\sqrt{3}$$

## Adjoining a Root



Here is a closer look. We want to use a root of the polynomial

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

commonly known as $\sqrt{2} \in \mathbb{R}$.

We need to somehow "adjoin" a new element $\alpha$ to $\mathbb{Q}$ so that we get a new field

$$\mathbb{Q}(\alpha)$$

in which

- $\alpha$ behaves just like $\sqrt{2}$
- the extended field is fully effective.

Ideally, all computations should easily reduce to $\mathbb{Q}$.

## Easy



In this case, there is a trick: we already know the reals $\mathbb{R}$ and we know that $f$ has a root in $\mathbb{R}$, usually written $\sqrt{2}$.

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

In the standard impredicative definition this looks like

$$\mathbb{Q}(\sqrt{2}) = \bigcap \{\, K \subseteq \mathbb{R} \mid \mathbb{Q}, \sqrt{2} \subseteq K \text{ subfield of } \mathbb{R} \,\}$$

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

## Quoi?



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

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 $a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$.

## Adjoining Root of 2



We claim that

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

Clearly, $P$ is closed under addition, subtraction and multiplication, so we definitely have a ring.

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 $a \neq 0 \vee b \neq 0$. Since $\sqrt{2}$ is irrational this means

$$\begin{aligned} ac + 2bd &= 1 \\ ad + bc &= 0 \end{aligned}$$

## Field Operations



Solving the system for $c$ and $d$ we get

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

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

Hence $P$ is actually a field and indeed $P = \mathbb{Q}(\sqrt{2})$. The surprise is that we obtain a field just from polynomials, not rational functions.

Moreover, we can implement the field operations in $\mathbb{Q}(\sqrt{2})$ rather easily based on the field operations of $\mathbb{Q}$: we just need a few multiplications and divisions of rationals.

## Again: Killing Denominators



Division of field elements comes down to plain polynomial arithmetic over the rationals. There is no need for rational functions.

$$\frac{a+b\sqrt{2}}{r+s\sqrt{2}} = \frac{1}{r^2-2s^2}(a+b\sqrt{2})(r-s\sqrt{2})$$

## Adjoining Roots in General



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

### Theorem

*The least field containing $\mathbb{F}$ and a root $\alpha$ 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.

### Exercise

*Prove the theorem.*



## Is that It?



So far we have a few infinite fields from calculus $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and variants such as $\mathbb{Q}(\sqrt{2})$ or $\overline{\mathbb{Q}}$, plus 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?

We will avoid infinite fields beyond this point.

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.

## Finite Integral Domains



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

### Theorem

*Every finite integral domain is already a field.*

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

By multiplicative cancellation, $\widehat{a}$ is injective and hence surjective on $R^\star$. But then every non-zero element is a unit: $ab = \widehat{a}(b) = 1$ for some $b$. □

## Finite Fields



The AMS has an entry for finite fields in its classification:

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

So we can safely assume that there must be quite a few finite fields. 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.

As usual, we distinguish by characteristic.

### Definition

The characteristic of a ring $R$ is defined by

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

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 $1 + 1 + \ldots + 1$.

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 only examples of finite fields so far are $\mathbb{Z}_p$, a ring with characteristic $p$ where $p$ is prime.

As we will see, this is no coincidence.

## Structure Theorem



Here is the surprising theorem that pins down finite fields completely (this compares quite favorably to, say, the class of finite groups).

### 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 quite 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 the subring generated by $1$:

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

### 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. □

## Vector Spaces



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.

### Definition

A vector space over a field $\mathbb{F}$ is a two-sorted structure $\langle V, +, \cdot, \mathbf{0} \rangle$ where

- $\langle V, +, \mathbf{0} \rangle$ is an Abelian group,
- $\cdot : \mathbb{F} \times V \to V$ is scalar multiplication subject to
  - $a \cdot (x + y) = a \cdot x + a \cdot y$,
  - $(a + b) \cdot x = a \cdot x + b \cdot x$,
  - $(ab) \cdot x = a \cdot (b \cdot x)$,
  - $1 \cdot x = x$.

In this context, the elements of $V$ are vectors, the elements of $\mathbb{F}$ are scalars.

## Examples of Vector Spaces



### Example

$\mathbb{F}$ is a vector space over $\mathbb{F}$ via $a \cdot x = ax$.

### Example

$\mathbb{F}^n$ is a vector space over $\mathbb{F}$ using componentwise operations.

### Example

$\coprod_I \mathbb{F}$ and $\prod_I \mathbb{F}$ are vector spaces over $\mathbb{F}$ for arbitrary index sets $I$.

### Example

The set of functions $\mathbb{F} \to \mathbb{F}$ using pointwise addition and multiplication is a vector space over $\mathbb{F}$.

## Independence



A linear combination in a vector space is a finite sum

$$a_1 \cdot v_1 + a_2 \cdot v_2 + \ldots + a_n \cdot v_n$$

where the $a_i$ are scalars and the $v_i$ vectors, $n \geq 1$. The linear combination is trivial if $a_i = 0$ for all $i$.

### Definition

A set $X \subseteq V$ of vectors is linearly independent if every linear combination $\sum a_i v_i = 0$, $v_i \in X$, is already trivial.

In other words, we cannot express any vector in $X$ as a linear combination of others. In some sense, $X$ is not redundant.

## Bases



### Definition

A set $X \subseteq V$ of vectors is spanning if all vectors in $V$ are linear combinations of vectors in $X$.

A set $X \subseteq V$ of vectors is a basis (for $V$) if it is independent and spanning.

Note that independent/spanning sets trivially exist if we don't mind them being small/large. The problem is to combine both properties.

### Theorem

*Every vector space has a basis. Moreover, the cardinality of any basis is the same.*

Correspondingly, one speaks of the dimension of the vector space.

## Digression: Proof



For vector spaces of the form $V = \coprod_I \mathbb{F}$ this is fairly easy to see: let $e_i \in V$ be the $i$th unit vector: $e_i(j) = 1$ if $i = j$, $e_i(j) = 0$, otherwise.

Then $B = \{ e_i \mid i \in I \}$ is a basis for $V$.

But how about $\prod_{\mathbb{N}} \mathbb{F}$? $B$ from above is still independent, but no longer spanning: we miss e.g. the vector $(1, 1, 1, 1, \ldots)$.

We could try to add this vector to $B$, but then we would still miss $(1, 0, 1, 0, 1, \ldots)$.

Add that vector and miss another. And so on and so on.

This sounds utterly non-constructive; how are we supposed to pick the next vector? And will the process ever end?

## (AC) to the Rescue



As it turns out, one needs a fairly powerful principle from axiomatic set theory: the Axiom of Choice.

Write $\mathfrak{P}_+(X)$ for $\mathfrak{P}(X) - \{\emptyset\}$, the set of all non-empty subsets of $X$. (AC) guarantees that for any set $X$ there is a choice function $C$

$$C : \mathfrak{P}_+(X) \to X$$

such that $C(x) \in x$.

With choice, we can build a basis in any vector space by transfinite induction: repeatedly choose a vector that is not a linear combination of the vectors already collected.

$$B_0 = \emptyset$$
$$B_{\alpha+1} = C\left(V - \sum B_\alpha\right)$$
$$B_\lambda = \bigcup_{\alpha<\lambda} B_\alpha$$

## (AC) to the Rescue, II



An easy (if transfinite) induction shows that all the $B_\alpha$ are independent.

For cardinality reasons, the process must stop at some point. But then the corresponding $B_\alpha$ must be spanning and we have a basis.

With more work one can show that this process always produces a basis of the same cardinality, no matter which choice function we use.

### Exercise

*Show the uniqueness of dimension when there is a finite basis: demonstrate that any independent set has cardinality at most the cardinality of any spanning set (both finite).*

## Coordinates



The importance of bases comes from the fact that they make it possible to focus on the underlying field and, in a sense, avoid arbitrary vectors.

To see why, suppose $V$ has finite dimension and let $B = \{b_1, b_2, \ldots, b_d\}$ be a basis for $V$.

Then there is a natural vector space isomorphism

$$V \longleftrightarrow \mathbb{F}^d$$

that associates every linear combination $\sum c_i b_i$ with the coefficient vector $(c_1, \ldots, c_d) \in \mathbb{F}^d$. Since $B$ is a basis this really produces an isomorphism.

So, we only need to deal with $d$-tuples of field elements. For characteristic 2 this means: bit-vectors.

## The Linear Algebra Angle



Back to finite fields. Given the prime subfield $\mathbb{Z}_p \cong \mathbb{K} \subseteq \mathbb{F}$ we have just seen that we can think of $\mathbb{F}$ as a finite dimensional vector space over $\mathbb{K}$. Hence we can identify the field elements with fixed-length vectors of elements in the prime field.

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

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

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

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 $\alpha$ is the order of $a$.

### Proposition (Lagrange)

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

## Proof of lemma



Let $m$ be the maximal order in $\mathbb{F}^\star$, $n$ the size of $\mathbb{F}^*$, so $m \leq n$.

We need to show that $m = n$.

**Case 1:** 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 $\mathbb{F}$: letting $p$ be the order of an element and $m = pq$ we have

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

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

## Odious Second Case



**Case 2:** Otherwise.

Then we can pick $a \in \mathbb{F}^\star$ of order $m$ and $b \in \mathbb{F}^\star$ of order $l$ not dividing $m$.

Then by basic arithmetic there is a prime $q$ such that

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

where $q$ is coprime to $l_0$ and $m_0$.

Set

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

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

- Find a generator $g$ of $\mathbb{F}^\star$, and
- 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 $g^i * g^j = g^{i+j \bmod |\mathbb{F}^*|}$.

Hence it is most interesting to be able to rewrite the field elements as powers of $g$. This is known as the discrete logarithm problem and quite difficult (but useful for cryptography).

## Representation 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:

| | | |
|---|---|---|
| addition | $\mathbb{F} \cong (\mathbb{Z}_p)^k$ | $(a_1, \ldots, a_k)$ |
| multiplication | $\mathbb{F}^* \cong \mathbb{Z}_{p^k - 1}$ | $g^i$ |

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

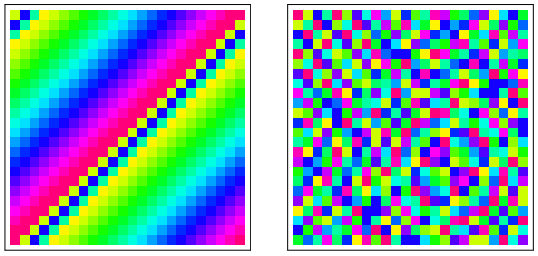
$$g^i + g^j \qquad \text{or} \qquad (a_1, \ldots, a_k) * (b_1, \ldots, b_k)$$

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.



## Back to the Roots



Time to get serious about building a finite field.

We would like to follow the construction of $\mathbb{Q}(\sqrt{2})$ from above, adjoining a root of $x^2 - 2 = 0$ to the rationals. So let's consider the polynomial

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

Note that one can easily check that $f$ has no root over $\mathbb{F}_2$.

So how do we expand $\mathbb{F}_2$ to a field $\mathbb{F}$ where $f$ has a root?

## Obstructions



This time:

- We do not know a convenient big field like $\mathbb{R}$ that we can use as a safe sandbox, and
- we have no intuitive idea what a root of $f$ looks like.

So, we can't just do

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

**But:** we can interpret this construction as the result of applying the simplification rule

$$x^2 \rightsquigarrow 2$$

to polynomials over $\mathbb{Q}$. In this setting, the "unknown" $x$ works just like the root we are after.

## Generalizing $\sqrt{2}$



So the hope is that we can generalize this idea by starting with $\mathbb{F}_2[x]$ and we use the simplification rule

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

Recall, we are dealing with characteristic 2, so plus is minus.

By systematically applying this rule, plus standard field arithmetic, we might be able to construct a finite field that has a root for $f$.

## The Rewrite Rule



So what happens to $\mathbb{F}_2[x]$ if we apply this rule systematically? Here is a (characteristic) example.

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

It is easy to see that any polynomial will similarly ultimately produce a polynomial of degree at most 1: any higher order term could be further reduced.

## Simplification, Algorithmically



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 simply 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.

## Simplification, Algebraically



Obviously, the simplification rule $x^2 \rightsquigarrow x+1$ has lots of algebraic consequences.

In order to really get a grip on these, we need to determine all equational consequences of the identity $x^2 = x+1$. It is not hard to see that we obtain an equivalence relation on polynomials in $\mathbb{F}_2[x]$ that is nicely compatible with the structure of the ring (a congruence).

Given a congruence, we can form a quotient ring, which turns out to be exactly the field we are looking for.

Here is a more algebraic description of this congruence.

## Ideals



### 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 much more constrained than a subring: it has to be closed by multiplication from the outside. Ideals are hugely important since they produce congruences and thus allow us to form a quotient structure:

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

As a consequence, arithmetic in this quotient structure is well-behaved: E.g.

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

## Generating Ideals



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

All we need is the multiples of $r$:

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

This is the ideal generated by $r$, aka principal ideal.

### Exercise

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

## 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.

## Digression: Proper Substructures



In algebra it is important to come up with the right notion of substructure: just picking a subset that is closed under the algebraic operations is often not enough.

- For groups, normal subgroups are arguably more important than plain subgroups.
- For rings, ideals are arguably more important than subrings.
- But a sub-vector-space is just right.

## 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 $\mu$ is the Möbius function. At any rate, there are quite a few irreducible polynomials.

| $d$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $N_d^2$ | 2 | 1 | 2 | 3 | 6 | 9 | 18 | 30 | 56 | 99 |

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.

Again, 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:

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

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 $\alpha$ 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 lame. One would have hoped for some kind of fireworks.

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, Algorithmically



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 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, Algorithmically



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

The product

$$(c_2, c_1, c_0) \cdot (c'_2, c'_1, c'_0) = (d_2, d_1, d_0)$$

is given by the coefficient triple

$$\begin{aligned} d_2 &= c_2\,c'_0 + c_1\,c'_1 + c_0\,c'_2 + c_2\,c'_2 \\ d_1 &= c_1\,c'_0 + c_0\,c'_1 + c_2\,c'_1 + c_1\,c'_2 + c_2\,c'_2 \\ d_0 &= c_0\,c'_0 + c_2\,c'_1 + c_1\,c'_2 \end{aligned}$$

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

## Multiplicative Structure



Recall that $\alpha$ is the equivalence class of $x$. Then the powers of $\alpha$ are:

$$\begin{aligned} \alpha^0 &= 1 && = (0,0,1) \\ \alpha^1 &= \alpha && = (0,1,0) \\ \alpha^2 &= \alpha^2 && = (1,0,0) \\ \alpha^3 &= \alpha + 1 && = (0,1,1) \\ \alpha^4 &= \alpha^2 + \alpha && = (1,1,0) \\ \alpha^5 &= \alpha^2 + \alpha + 1 && = (1,1,1) \\ \alpha^6 &= \alpha^2 + 1 && = (1,0,1) \\ \alpha^7 &= 1 \end{aligned}$$

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 | $\alpha$ | $1 + \alpha^2$ |
| 3 | $\alpha^2$ | $1 + \alpha + \alpha^2$ |
| 4 | $1 + \alpha$ | $\alpha + \alpha^2$ |
| 5 | $1 + \alpha^2$ | $\alpha$ |
| 6 | $\alpha + \alpha^2$ | $1 + \alpha$ |
| 7 | $1 + \alpha + \alpha^2$ | $\alpha^2$ |

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

## Reciprocal Polynomials



### Definition

The reciprocal of a polynomial $f(x)$ of degree $k$ is the polynomial $f^\star(x) = x^k f(1/x)$.

In other words: we reverse the coefficient vector:

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots a_1 x + a_0$$

produces the reciprocal

$$f^\star(x) = a_0 x^m + a_1 x^{m-1} + \ldots a_{m-1} x + a_m$$

## Properties? 79

The map $f \mapsto f^\star$ is not very well behaved, in particular it fails to be a homomorphism.

Still, we have the following properties.

### Proposition

*Let $f$ and $g$ be two polynomials.*

- *If $f(0) \neq 0$ then $(f^\star)^\star = f$.*
- $(f \cdot g)^\star = f^\star \cdot g^\star$.

### Exercise

*Prove the last proposition.*

## MinPol for Inverse 80

If we have a field extension $\mathbb{F}[\alpha]$ where $\alpha$ is a root of $f(x)$, then it is easy to determine the minimal polynomial for $1/\alpha$: given

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots a_1 x + a_0$$

it is none other than the reciprocal

$$f^\star(x) = a_0 x^m + a_1 x^{m-1} + \ldots a_{m-1} x + a_m$$

## Example 81

Consider the field extension $\mathbb{F}_2[\alpha]$ where $\alpha$ is a root of $f(x) = x^3 + x + 1$.

Then $f^\star = x^3 + x^2 + 1$ and the field elements have associated minimal polynomials as follows.

| | |
|---|---|
| $0$ | $x$ |
| $1$ | $x+1$ |
| $\alpha, \alpha^2, \alpha^4$ | $x^3 + x + 1$ |
| $\alpha^3, \alpha^5, \alpha^6$ | $x^3 + x^2 + 1$ |



## The Structure of Finite Fields 83

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 $p$ is the characteristic of $\mathbb{F}$ and therefore prime.
- There is a field of cardinality $p^k$.
- All fields of cardinality $p^k$ are isomorphic.

## Proof Sketch 84

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 $f : R \to S$. $f$ 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 $f : R \to S$ 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 $f : \mathbb{F} \to \mathbb{K}$ 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 $R \to R$, $x \mapsto x^p$.

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

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

### Exercise

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

## Aside: Frobenius and Galois



For algebra lovers: the Frobenius homomorphism $F$ is the key to understanding the Galois group of the algebraic closure $K$ of a finite field $\mathbb{F}_p$.

Recall that the Galois group is the collection of all automorphisms of $K$ that leave the prime field invariant. By Fermat's little theorem, $\mathbb{F}_p$ is certainly invariant under $F$.

Algebraically closed fields are perfect, so $F$ is indeed an automorphism of $K$. The group generated by $F$ is a subgroup of the Galois group, the so-called Weil group. In fact, the whole Galois group is a kind of completion of the Weil group.

## Establishing Isomorphisms



The following fact is often useful to establish an isomorphism. Suppose $f : R \to S$ 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 $\alpha$.

## Adjoining a Root, contd.



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

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

that evaluates $g$ at $\alpha$, producing a value in $\mathbb{K}$. It is easy to check that $\nu$ 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 $\alpha$. 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 $\nu$ 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 $f : A \to B$ the kernel relation is given by $f(x) = f(y)$.
- For a group homomorphism $f : A \to B$ the kernel is given by $\{ x \in A \mid f(x) = 1 \}$.
- For a ring homomorphism $f : A \to B$ 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 |
|---|---|
| $0$ | $x$ |
| $\alpha^0$ | $x + 1$ |
| $\alpha^1$ | $x^3 + x + 1$ |
| $\alpha^2$ | $x^3 + x + 1$ |
| $\alpha^3$ | $x^3 + x^2 + 1$ |
| $\alpha^4$ | $x^3 + x + 1$ |
| $\alpha^5$ | $x^3 + x^2 + 1$ |
| $\alpha^6$ | $x^3 + x^2 + 1$ |

## 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?

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 $k = 2$.

$$x^{25} - x = x\,(1+x)\,(2+x)\,(3+x)\,(4+x)$$
$$(2+x^2)\,(3+x^2)\,(1+x+x^2)\,(2+x+x^2)\,(3+2\,x+x^2)\,(4+2\,x+x^2)$$
$$(3+3\,x+x^2)\,(4+3\,x+x^2)\,(1+4\,x+x^2)\,(2+4\,x+x^2)$$

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 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 $\Phi$ 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 avoids references to the extension field construction.

### Definition

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

In other words, $x^e = 1 \bmod f$.

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

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

So $\mathbb{F}_{5^2}^*$ is indeed cyclic with generator $\alpha$, 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 GF($p^k$).