PhD course: Finite Fields Some slides for 1st Lecture

Diego Ruano

Department of Mathematical Sciences Aalborg University Denmark

10-12-2012

Groups

A composition on a set G is a map

 $\begin{array}{cccc} \circ: G \times G & \to & G \\ (g,h) & \mapsto & \circ(g,h) = g \circ h \end{array}$

A pair (G, \circ) consisting of a set *G* and a composition $\circ : G \times G \rightarrow G$ is a group if it satisfies:

① The composition is associative: for every $s_1, s_2, s_3 \in G$

$$s_1 \circ (s_2 \circ s_3) = (s_1 \circ s_2) \circ s_3$$

- 2 There is a neutral element $e \in G$: for every $s \in G$ $e \circ s = s \circ e = s$
- For every $s \in G$ there is an inverse element $t \in G$ such that

$$s \circ t = t \circ s = e$$

A group is called abelian or commutative if for every $g, h \in G$:

 $g \circ h = h \circ g$

A ring is an abelian group (R, +) (the neutral element is 0) with an additional composition \cdot called multiplication which satisfies (for every $x, y, z \in R$:

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

2 There exists an element $1 \in R$ s.t. $1 \cdot x = x \cdot 1 = x$

3 $x \cdot (y+z) = x \cdot y + x \cdot z$ and $(y+z) \cdot x = y \cdot x + z \cdot x$.

R is called commutative if xy = yx for every $x, y \in R$.

An element $x \in R$ is called a **unit** if there exists $y \in R$ s.t. xy = yx = 1. In this case we say $x^{-1} = y$ is the inverse of x. The set of units in R is denoted R^* .

Field

A ring R with $R^* = R \setminus \{0\}$ is called a field.

Another way to say it:

A field $(F, +, \cdot)$ is a set *F* with two compositions $+, \cdot$ which satisfies (for every *x*, *y*, *z* \in *R*):

- The + is associative: x + (y + z) = (x + y) + z.
- **2** There exits $0 \in R$, s.t. 0 + x = x + 0 = x
- **3** There exists $-x \in R$, s.t. x + (-x) = (-x) + x = 0
- The + is abelian: x + y = y + x.
- $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- There exists $1 \in R$ s.t. $1 \cdot x = x \cdot 1 = x$
- $x \cdot (y+z) = x \cdot y + x \cdot z$ and $(y+z) \cdot x = y \cdot x + z \cdot x$.
- There exists $y \in R$ s.t. $x \cdot y = y \cdot x = 1$. In this case we say $x^{-1} = y$ is the inverse of x.

Some finite fields

A finite field $(F, +, \cdot)$ is a field such that $|F| < \infty$.

Some fields that we already know: Fields with |F| = p, with p prime.

 $(\mathbb{F}_{p} = \mathbb{Z}/p\mathbb{Z}, +, \cdot), \text{ where}$ $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \cdots, \overline{p-1}\}$ $\overline{x} = \overline{y} \Leftrightarrow p \mid x - y \Leftrightarrow x \text{ rem } p = y \text{ rem } p \Leftrightarrow x \equiv y \pmod{p}$ $\overline{x} + \overline{y} = \overline{x+y}$ $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$

Are the compositions well defined?

- How do we guarantee that every element has an inverse?
- Even better: How do find the inverse of every element?

Answer: Extended Euclidean algorithm Since gcd(x, p) = 1, for $x \in \{1, ..., p-1\}$, there exist $\lambda, \mu \in \mathbb{Z}$ such that

$$\lambda x + \mu p = 1$$

Then $x^{-1} = \lambda$.

Is $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ a field?

Let n = ab with $a, b \neq 1, n$. Is $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ a field?

Proposition

Let *F* be a field. Then *F* is a domain (a ring $R \neq \{0\}$ with no zero divisors).

Proof:

- Suppose $x, y \in F, x \neq 0$ and xy = 0. Is y = 0???
- Since $x \neq 0$, there exists x^{-1} .
- Hence, $0 = x^{-1}0 = x^{-1}(xy) = y$

What about the Extended Euclidean Algorithm?

Computing the gcd: The Euclidean algorithm

Proposition

Let $m, n, \in \mathbb{Z}$. Then,

- gcd(m, 0) = m if $m \in \mathbb{N}$
- gcd(m, n) = gcd(m qn, n), for every $q \in \mathbb{Z}$.

Let $m \ge n \ge 0$

•
$$r_{-1} = m$$
 and $r_0 = n$

• If $r_0 = 0$ then $gcd(r_{-1}, r_0) = r_1$. Otherwise define remainder r_1 :

$$r_{-1} = q_1 r_0 + r_1$$

• We have $gcd(r_{-1}, r_0) = gcd(r_0, r_1)$ and $r_{-1} > r_0 > r_1$ We iterate this process

Computing the gcd: The Euclidean algorithm

Let $m \ge n \ge 0$

• $r_{-1} = m$ and $r_0 = n$

• If $r_0 = 0$ then $gcd(r_{-1}, r_0) = r_1$. Otherwise define remainder r_1 :

$$r_{-1} = q_1 r_0 + r_1$$

• We have $gcd(r_{-1}, r_0) = gcd(r_0, r_1)$ and $r_{-1} > r_0 > r_1$ We iterate this process if $(r_1 \neq 0)$:

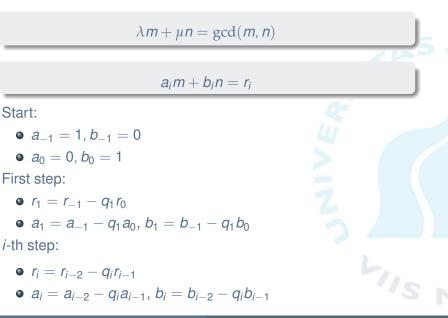
• Define remainder *r*₂:

$$r_0 = q_1 r_1 + r_2$$

• We have $gcd(r_0, r_1) = gcd(r_1, r_2)$ and $r_{-1} > r_0 > r_1 > r_2$

We will get $r_N = 0$ for some step N. Why???

Extended Euclidean algorithm



How to compute the remainder of 12¹¹ divided by 21?

- Exercise 1.3: [xy] = [[x][y]]
- $a^b a^c = a^{b+c}$
- $(a^b)^c = a^{bc}$

Allow us to have the repeated squared algorithm:

$$\left[a^{2^{n}}\right] = \left[(a^{2^{n-1}})^{2}\right] = \left[\left[a^{2^{n-1}}\right]\left[a^{2^{n-1}}\right]\right]$$

Multiplicative group

Proposition

 $\mathbb{F}_{p}^{*} = \mathbb{F}_{p} \setminus \{0\}$ is a cyclic group (with the multiplication), i.e. there exists $g \in \mathbb{F}_{p} \setminus \{0\}$ (primitive element) such that

$$\mathbb{F}_{p} = \{g^{0}, g^{1}, \ldots, g^{p-2}\} \cup \{0\}$$

Notation:
$$\langle g \rangle = \{g^0, g^1, \dots, g^{p-2}\} = \{g^i : i \in \mathbb{Z}\}$$

Proposition

There are $\varphi(p-1)$ generators of $\mathbb{F}_p \setminus \{0\}$ (but the proof is not constructive).

How to find such a *g*?, there is no efficient algorithm. Try random element. What is the probability of picking a generator?

But if you find one generator, you can computed the others easily.

The characteristic of a field *F* is the is the least positive integer n such that nx = 0 for every xinF. If no such positive integer exists then we say that the characteristic of the field is 0.

The finite field \mathbb{F}_p has characteristic *p*.

Proposition

A finite field has prime characteristic

Proposition: Freshman's dream

Let R be a ring of prime characteristic, then

$$(a+b)^{p^n}=a^{p^n}+b^{p^n}$$

Polynomials

Let F be a field, a polynomial over F is

$$a_0 + a_1 X + \cdots + a_n X^n \in F[X]$$

 $X \in F$ and it is consider an indeterminate over F

$$F[X] = \{\sum_{i \ge 0} a_i X^i : a_i = 0 \text{ excepting a finite number of them} \}$$

F[X] is a ring:

$$\sum a_i X^i + \sum b_i X^i = \sum (a_i + b_i) X^i$$
$$\sum a_i X^i \cdot \sum b_i X^i = \sum c_i X^i,$$

 $c_i = \sum_{j+k=i} a_j b_k$

where

- 0 is the neutral element for the sum.
- $1 = X^0$ is the neutral element for multiplication.
- *F*[*X*] is a domain (it has no zero divisors).

F[X] is a ring but it is not a field: X^{-1} ? $a \in F[X]^* \iff a \in F \setminus \{0\}$

Concepts: Term, coefficient, degree, leading term, leading coefficient, monic polynomial.

Proposition

Let $f, g \in R[X] \setminus \{0\}$ then

 $\deg(\mathit{fg}) = \deg(\mathit{f}) + \deg(\mathit{g})$

Let *d* be a non-zero polynomial in R[X]. Given $f \in R[X]$, there exist unique polynomials $q, r \in R[X]$ such that

f = qd + r

and either r = 0 or deg(r) < deg(d). *r* is called the **remainder** of *f* divided by *d*.

Having division we can extend:

- gcd(*f*, *g*)
- Extended Euclidean Algorithm.
- We say that *F*[*X*] is an Euclidean domain. We used prime numbers for dividing, what shall we use here?

Irreducible polynomials

A polynomial $f \in F[X]$ is said to be irreducible in F[X] if p has positive degree and if f = gh implies that g or h are in F.

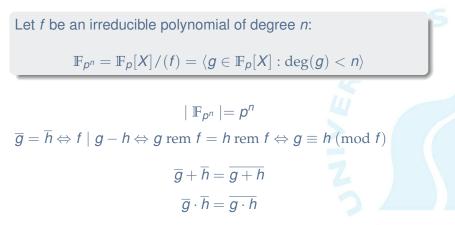
prime \longleftrightarrow irreducible

- *F*[X] is a UFD (Unique Factorization Domain).
- Let f irreducible, $f \mid gh$ then $f \mid g$ or $f \mid h$.

How do we know that a polynomial is irreducible?

- If deg(f) = 1 then *f* is irreducible.
- If f is irreducible and deg(f) > 1 then f does not have any roots.
- If deg(f) is 2 or 3 then f is irreducible if and only if f has no roots.

X⁴ + X² + 1 ∈ 𝔽₂ does not have any roots but it is not irreducible.



Are the compositions well defined?, Do we have a field?

Multiplicative representation

Let α be root of an irreducible polynomial $f = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{F}_p$ of degree *n*.

 $\alpha \notin \mathbb{F}_p$

 $\alpha \in F \supset \mathbb{F}_p$

Actually, $\alpha \in \mathbb{F}_{p^n}$, since " α is like x":

$$a_0 + a_1 \alpha + \cdots + a_n \alpha^n = 0$$

and

$$\mathbb{F}_{p^n} \setminus \{\mathbf{0}\} = \{\alpha^0, \ldots, \alpha^{p^n-2}\},\$$

if we consider some particular irreducible polynomials (primitive) that we will see in lecture 2.