

**Announcements:** Today we'll discuss material from chapter 2 of text-book. The preamble gives basic facts from field and Galois theory and we'll try to fill in the gaps in the coming lectures. Qing Luo's Office Hours: F 2-4 SAL 317.

**Topics for today:**

1. Field
2. Finite Fields
3. Vector Spaces
4. Finite Field Construction

## 1. Field

**Definition.** A *field* is a set  $\mathbf{k}$  with binary operations  $+_{\mathbf{k}}$  and  $*_{\mathbf{k}}$  such that

1.  $(\mathbf{k}, +_{\mathbf{k}}, 0_{\mathbf{k}})$  is an abelian group with  $0_{\mathbf{k}}$  being the identity wrt  $+_{\mathbf{k}}$
2.  $(\mathbf{k} - \{0_{\mathbf{k}}\}, *_{\mathbf{k}}, 1_{\mathbf{k}})$  is an abelian group with  $1_{\mathbf{k}}$  being the identity wrt  $*_{\mathbf{k}}$
3.  $a *_{\mathbf{k}} (b +_{\mathbf{k}} c) = a *_{\mathbf{k}} b +_{\mathbf{k}} a *_{\mathbf{k}} c$

If  $(\mathbf{k} - \{0_{\mathbf{k}}\}, *_{\mathbf{k}}, 1_{\mathbf{k}})$  is not an abelian group we end up with a skew field. We'll usually drop with subscript  $\mathbf{k}$  Examples of infinite fields are  $(\mathbf{Q}, +, *)$ ,  $(\mathbf{R}, +, *)$ ,  $(\mathbf{C}, +, *)$ . An example of a finite field is  $(\mathbf{Z}/p\mathbf{Z}, +, *)$  for prime  $p$ .

If  $f(x) = \sum_{i=0}^m a_i x^i$  with  $a_i \in \mathbf{k}$ , we say  $f(x) \in \mathbf{k}[x]$

**Division Thm.** Given  $f(x), g(x) \in \mathbf{k}[x]$  there exist unique polynomials  $h(x), r(x) \in \mathbf{k}[x]$  such that  $f(x) = h(x)g(x) + r(x)$  with  $0 \leq \deg r(x) < \deg g(x)$ .

**Proof Sketch.** The existence of the polynomials can be proved inductively. To prove uniqueness suppose in addition to  $h(x), r(x)$  there exists polynomials  $h'(x), r'(x)$  such that  $f(x) = h'(x)g(x) + r'(x)$  with  $\deg r' < \deg g$ . Then  $h'g + r = hg + r \Rightarrow (h' - h)g = r - r'$ . As  $\deg r < \deg g$  and  $\deg r' < \deg g$  we have  $\deg (r - r') < \deg g$ . But then  $\deg (h' - h)g < \deg g$  which is a contradiction unless  $h' - h = 0 \Rightarrow r - r' = 0 \quad \diamond$

Analogous to numbers decomposing into primes, polynomials over fields decompose into irreducible polynomials.

**Definition.** Say  $g, f \in \mathbf{k}[x]$ . We write  $g|f$  iff  $f = hg$  for some  $h \in \mathbf{k}[x]$ .  $g|f$  is read as  $g$  divides  $f$ .

**Definition.**  $f$  is *irreducible* over  $\mathbf{k}$  iff there doesn't exist  $g \in \mathbf{k}[x]$  with  $0 < \deg g < \deg f$  such that  $g|f$

*Remark.* Irreducibility is field sensitive. Consider the polynomial  $x^2 + 1$  with real coefficients, it is irreducible over the reals but not irreducible over the complex.

Constants are polynomials of degree 0. Next come the linear polynomials which have degree 1 and they are obviously irreducible. Polynomials with degrees greater than 1 may or may not be irreducible. Decomposition of polynomials into irreducible polynomials is unique upto constants (since you can play around with constants  $x + 1 = \frac{1}{2}(2x + 2)$ ). But if we restrict our attention to **monic** polynomials (polynomials with 1 as the leading coefficient) then polynomial decomposition is unique. Let's study roots of polynomials.

**Definition.**  $\alpha \in \mathbf{k}$  is a root of  $f(x) = \sum_{i=0}^m a_i x^i$  with  $a_i \in \mathbf{k}$  if  $f(\alpha) = \sum_{i=0}^m a_i \alpha^i = 0$ .

**Lemma.** Let  $f \in \mathbf{k}[x]$  be of degree  $m$  then  $f$  has  $\leq m$  roots in  $\mathbf{k}$ .

**Proof.** Induction on  $n$ .  $n = 1$  case is clear as a linear polynomial has exactly one root. Now suppose  $\deg f = n$ . If  $f$  has no roots in  $\mathbf{k}$  then we are done as  $0 \leq n$ . On the other hand suppose  $\alpha \in \mathbf{k}$  is a root of  $f$  then the Division Thm says that  $f(x) = (x - \alpha)h + r$  for some  $h \in \mathbf{k}[x]$  with  $r \in \mathbf{k}$  since  $\deg (x - \alpha) = 1$ . And  $0 = f(\alpha) = 0 + r \Rightarrow r = 0$ . Hence  $f(x) = (x - \alpha)h$ .  $\deg h = n - 1$  and by induction  $h$  has  $\leq n - 1$  roots. So the number of roots of  $f$  in  $\mathbf{k} \leq 1 + \deg h = n. \quad \diamond$

## 2. Finite Fields

We next turn our attention to finite fields.

**Definition.** A field  $\mathbf{k}$  is *finite* if  $|\mathbf{k}| < \infty$ .

We adopt a short hand to denote adding  $1_{\mathbf{k}}$  (the identity with respect to  $*$ ) to itself  $m$  times.  $m.1_{\mathbf{k}} := 1_{\mathbf{k}} +_{\mathbf{k}} 1_{\mathbf{k}} +_{\mathbf{k}} \dots m \text{ times} \dots 1_{\mathbf{k}}$ .

**Lemma.** A field has no zero-divisors, that is if  $u \neq 0, v \neq 0$  then  $u.v \neq 0$ .

**Proof.** Suppose  $u.v = 0$ . Since  $u \neq 0$ ,  $u^{-1}$  exists. So  $u^{-1}(u.v) = 0 \Rightarrow v = 0$ . Contradiction.  $\diamond$

**Thm.** For a finite field  $\mathbf{k}$  there exists a prime  $p$  such that  $p.1_{\mathbf{k}} = 0$

**Proof.** Since  $\mathbf{k}$  is finite, the pigeon hole principle tells us that there exist integers  $q, q'$  with  $q < q'$  such that  $q.1_{\mathbf{k}} = q'.1_{\mathbf{k}} \Rightarrow (q' - q).1_{\mathbf{k}} = 0$ . Let  $p \in \mathbf{Z}_{>0}$  be the smallest number such that  $p.1_{\mathbf{k}} = 0$ . Suppose  $p = lm$  where  $1 < l, m$ . Now consider

$$\begin{aligned} & (l.1_{\mathbf{k}}).(m.1_{\mathbf{k}}) \\ &= (1_{\mathbf{k}} +_{\mathbf{k}} 1_{\mathbf{k}} +_{\mathbf{k}} \dots m \text{ times} \dots 1_{\mathbf{k}}).(1_{\mathbf{k}} +_{\mathbf{k}} 1_{\mathbf{k}} +_{\mathbf{k}} \dots l \text{ times} \dots 1_{\mathbf{k}}) \\ &= lm.1_{\mathbf{k}} \text{ since } 1_{\mathbf{k}} *_k 1_{\mathbf{k}} = 1_{\mathbf{k}} \text{ and the distributive law} \\ &= p.1_{\mathbf{k}} \\ &= 0 \end{aligned}$$

As a field has no zero divisors either  $l < p$  with  $l.1_{\mathbf{k}} = 0$  or  $m < p$  with  $m.1_{\mathbf{k}} = 0$  contradicting the minimality of  $p$ . So  $p$  is prime.  $\diamond$

We call the number  $p$  the characteristic of the field.  $char \mathbf{k} := p$ . If no such prime exists as in the case of infinite fields then  $char \mathbf{k} = 0$ . And we've seen if the field is finite then  $char \mathbf{k} = p$ , a prime

*Remark.* Also observe that  $p$  kills all elements in the field as  $p.1_{\mathbf{k}} = 0 \Rightarrow p.x = (p.1_{\mathbf{k}}) = 0$  for all  $x \in \mathbf{k}$ .

Recall that  $\mathbf{Z}/p\mathbf{Z} = \{0, 1, 2, \dots, p\}$ . From what we've learnt so far  $\mathbf{Z}/p\mathbf{Z}$  is also a field with modular addition and multiplication as the two operations. And we will refer to the set as  $\mathbf{F}_p$  when we view it as a field.

If we look at the elements generated by  $1_{\mathbf{k}}$  we see that

$$\{0_{\mathbf{k}}, 1_{\mathbf{k}}, 2.1_{\mathbf{k}}, \dots, (p_1).1_{\mathbf{k}}\} \subseteq \mathbf{k}$$

The LHS is essentially  $\mathbf{F}_p$  and we are saying that  $\mathbf{F}_p$  is a subset (infact a subfield) of  $\mathbf{k}$ .

So any finite field  $\mathbf{k}$  with characteristic  $p$  has a copy of  $\mathbf{F}_p$  in it. We call this an imbedding and symbolically denote it as follows:  $\mathbf{F}_p \hookrightarrow \mathbf{k}$ . If we started out with  $\mathbf{k} = \mathbf{F}_p$  then we obtain  $\mathbf{F}_p \hookrightarrow \mathbf{F}_p$  which is not saying anything new. But as you may have guessed the field  $\mathbf{k}$  can be bigger. What can we say about  $|\mathbf{k}|$ ?

Observe that  $\mathbf{F}_p, \mathbf{k}$  are groups wrt to  $+$  and by Lagrange's Thm  $p = |\mathbf{F}_p|$  divides  $|\mathbf{k}|$  but more is true.

**Lemma.** Let  $\mathbf{k}$  be a finite field of  $\text{char } \mathbf{k} = p$ . Then  $|\mathbf{k}| = p^d$  for some  $d \in \mathbf{Z}_{>0}$

For the proof we'll make an excursion into linear algebra in particular vector spaces.

### 3. Vector Spaces

A recap of vector spaces over the field of reals  $\mathbf{R}$ .

**Definition.**  $V$  a *vector space* over  $\mathbf{R}^n$  is a set of vectors for which any vectors  $X, Y, Z \in \mathbf{R}^n$  and any scalars  $r, s \in \mathbf{R}$  have the following properties:

1. Commutativity.  $X + Y = Y + X$ .
2. Associativity of vector addition.  $(X + Y) + Z = X + (Y + Z)$ .
3. Additive identity. For all  $X$ ,  $0 + X = X + 0 = X$ .
4. Existence of additive inverse. For any  $X$ , there exists a  $-X$  such that  $X + (-X) = 0$ .
5. Associativity of scalar multiplication.  $r(sX) = (rs)X$ .
6. Distributivity of scalar sums.  $(r + s)X = rX + sX$ .
7. Distributivity of vector sums.  $r(X + Y) = rX + rY$ .
8. Scalar multiplication identity.  $1X = X$ .

So a vector space  $V$  is an abelian group (with respect to vector addition) together with some scalars which act on  $V$  through scalar multiplication.

**Definition.** Vectors  $v_1, v_2, \dots, v_n \in \mathbf{V}$  are said to be *linear dependent* over  $\mathbf{R}$  iff there exists  $a_i \in \mathbf{R}$  not all 0 such that  $a_1v_1 + \dots + a_nv_n = 0$

As any two maximally linearly independent subsets have the same cardinality, we define the dimension of a vector space  $V$  as follows:  $\dim_{\mathbf{R}} \mathbf{V} = \#$  maximally linearly independent subsets of  $\mathbf{V}$

In the case of a finite vector space, suppose  $n = \dim_{\mathbf{R}} \mathbf{V}$ .

Let  $\{v_1, v_2, \dots, v_n\}$  be a maximally linearly independent subset. Then every element can be uniquely be expressed as a linear combination of the  $v_i$ . To denote the uniqueness we'll use the ring sum  $\oplus$ .  $\mathbf{V} = \mathbf{k}x_1 \oplus \mathbf{k}x_2 \oplus \dots \oplus \mathbf{k}x_n$  that is for all  $v \in \mathbf{V}$  there exists unique  $a_1, a_2, \dots, a_n \in \mathbf{k}$  such that  $\mathbf{V} = a_1v_1 + a_2v_2 + \dots + a_nv_n$

There's nothing special about the field of reals  $\mathbf{R}$  and so we can we can replace  $\mathbf{R}$  by any arbitrary field  $\mathbf{k}$  in the above discussion. Now let's get back to our proof from the previous section.

As  $\mathbf{F}_p \hookrightarrow \mathbf{k}$  we can view  $\mathbf{k}$  as an abelian group with respect to addition,  $\mathbf{F}_p$  as scalars and we can perceive  $\mathbf{k}$  as a vector space over  $\mathbf{F}_p$

Suppose  $a \in \mathbf{F}_p$ ,  $x \in \mathbf{k}$  then  $ax := (a \cdot 1_{\mathbf{k}}) \cdot x = x + x + \dots a \text{ times } \dots + x$ .  $a \in \mathbf{F}_p$  and  $x, y \in \mathbf{k}$   $a(x + y) = ax + ay$  and clearly  $\mathbf{k}$  is a vector space over  $\mathbf{F}_p$ . Since  $\mathbf{k}$  is a finite set let  $d = \dim_{\mathbf{F}_p} \mathbf{k} = \#$  maximal l.i. elements in  $\mathbf{k} < \infty$

From our knowledge of linear algebra  $\mathbf{k} = \mathbf{F}_p x_1 \oplus \mathbf{F}_p x_2 \oplus \dots \mathbf{F}_p x_d$  where  $\{x_1, x_2, \dots, x_d\}$  is a maximally l.i subset of  $\mathbf{k}$ . As there are  $p$  choices for each coefficient we have  $|\mathbf{k}| = p^d$  and this completes out proof.

*Sanity check.*  $p = |\mathbf{F}_p|$  divides  $|\mathbf{k}| = p^d$ . Also  $\mathbf{k}^*$  is a multiplicative group and contains  $\mathbf{F}_p^*$  as a subgroup. Hence Lagrange's theorem tells us  $p - 1 = |\mathbf{F}_p^*|$  divides  $|\mathbf{k}^*| = p^d - 1$ .

## 4. Finite Field Construction

This is all good in abstract but are there any finite fields of sizes  $p^2, p^3, \dots$

Let's construct a finite field with  $p^2$  elements. Say  $a \in \mathbf{F}_p$  and as we know  $x^2 - a$  has atmost 2 roots in  $\mathbf{F}_p$ . If it has no roots then it is irreducible. For  $p \neq 2$ ,  $x^2 \equiv a \pmod p$  has either 2 or no roots in  $\mathbf{F}_p$ .

Suppose  $x^2 - a$  is irreducible over  $\mathbf{F}_p$  and consider the set

$$\mathbf{L} := \{cx + d \mid c, d \in \mathbf{F}_p\}$$

It is a vector space over  $\mathbf{F}_p$  of dim 2 with  $\{1, x\}$  as it's basis. So we have a potential candidate for  $\mathbf{F}_{p^2}$ ! Adding two polynomials modulo  $p$  is closed. What about multiplying two polynomials? No! So when we multiply we'll mod out by  $x^2 - a$ .

Ex.  $p = 2$  and the irreducible  $x^2 - 2$ .  $(2x + 3)(x + 4) \bmod (x^2 - 2) = 2x^2 + x + 2 \bmod (x^2 - 2) = x + 1 \bmod (x^2 - 2)$ . So whenever we see  $x^2 - 2$  replace by 0 or replace  $x^2$  by 2.

Take the set  $\mathbf{L}$  and consider  $+$  and  $*$   $\bmod(x^2 - a)$  and now the set is closed. Additive inverse exists as  $-(cx + d) = (-c)x + (-d)$ . What about the multiplicative inverse? Next time we'll see how we can compute the inverse using Euclid's algorithm.