

Linear Algebra, 5th day, Friday 7/2/04  
REU 2004. Info:  
<http://people.cs.uchicago.edu/~laci/reu04>.

Instructor: László Babai  
Scribe: Shreya Amin

## 1 Fields

**Definition 5.1.** A **number field** is a subset  $\mathbb{F} \subseteq \mathbb{C}$  such that  $\mathbb{F}$  is closed under arithmetic operations.

**Example 5.2.**  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}[\alpha]$  where  $\alpha$  is such that  $f(\alpha) = 0$  for  $f \in \mathbb{Z}[x]$ .

**Definition 5.3.** A **field** is a set  $\mathbb{F}$  with 2 operations (addition  $+$  and multiplication  $\bullet$ ),  $(\mathbb{F}, +, \bullet)$  such that  $(\mathbb{F}, +)$  is an abelian group:

- (a1)  $(\forall \alpha, \beta \in \mathbb{F})(\exists! \alpha + \beta \in \mathbb{F})$ ,
- (a2)  $(\forall \alpha, \beta \in \mathbb{F})(\alpha + \beta = \beta + \alpha)$  (commutative law),
- (a3)  $(\forall \alpha, \beta, \gamma \in \mathbb{F})((\alpha + \beta) + \gamma = \alpha + (\beta + \gamma))$  (associative law),
- (a4)  $(\exists 0 \in \mathbb{F})(\forall \alpha)(\alpha + 0 = 0 + \alpha = \alpha)$  (existence of zero),
- (a5)  $(\forall \alpha \in \mathbb{F})(\exists(-\alpha) \in \mathbb{F})(\alpha + (-\alpha) = 0)$ ,

and for  $(\mathbb{F}, \bullet)$  have the following.  $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$  is an abelian group with respect to multiplication:

- (b1)  $(\forall \alpha, \beta \in \mathbb{F})(\exists! \alpha \bullet \beta \in \mathbb{F})$ ,
- (b2)  $(\forall \alpha, \beta \in \mathbb{F})(\alpha \bullet \beta = \beta \bullet \alpha)$  (commutative law),
- (b3)  $(\forall \alpha, \beta, \gamma \in \mathbb{F})((\alpha \bullet \beta) \bullet \gamma = \alpha \bullet (\beta \bullet \gamma))$  (associative law),
- (b4)  $(\exists 1 \in \mathbb{F})(\forall \alpha)(\alpha \bullet 1 = 1 \bullet \alpha = \alpha)$  (existence of identity),
- (b5)  $(\forall \alpha \in \mathbb{F}^\times)(\exists(\alpha^{-1} \in \mathbb{F}^\times)(\alpha \bullet (\alpha^{-1}) = (\alpha^{-1}) \bullet \alpha = 1)$ ,

(b6)  $1 \neq 0$

(b7)  $(\forall \alpha, \beta, \gamma \in \mathbb{F})((\alpha \bullet (\beta + \gamma) = \alpha \bullet \beta + \alpha \bullet \gamma)$  (distributive law)

**Example 5.4.** Examples of fields:

(1) Number fields (Every number field is a field)

(2)  $\mathbb{R}(x)$  (Recall  $\mathbb{R}[x]$  = polynomials over  $\mathbb{R}$ . This is not a field since reciprocal of a polynomial is not necessarily a polynomial. Thus, consider  $\mathbb{R}(x) = \{\text{rational functions}\} = \{\frac{f(x)}{g(x)} \mid g(x) \neq 0, f, g \in \mathbb{R}[x]\}$ .

(3) Finite fields: mod  $p$  residue classes,  $p$  prime. Denote it by  $\mathbb{Z}/p\mathbb{Z}$ .

**Example 5.5.**  $\mathbb{Z}/p\mathbb{Z}$ :

+	0	1
0	0	1
1	1	0

•	0	1
0	0	0
1	0	1

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Part of the group structure of  $(\mathbb{Z}/p\mathbb{Z}, +)$  is reflected in the facts that each row and each column is a permutation. Similarly for  $(\mathbb{Z}/p\mathbb{Z})^\times, \bullet$ .

**Latin Squares:**  $n \times n$  square filled with  $n$  symbols. Every symbol appears in each row and each column exactly once. So,  $(\mathbb{Z}/p\mathbb{Z}, +)$  is  $5 \times 5$  Latin square and  $(\mathbb{Z}/p\mathbb{Z})^\times, \bullet$  is a  $4 \times 4$  Latin square.

Note: Commutativity  $\longleftrightarrow$  symmetric matrix

**Definition 5.6.** Let  $A \in \mathbb{F}^{k \times n}$ . **Transpose of  $A$ :** flip matrix over main diagonal. Let  $A = (\alpha_{ij})_{(i=1)(j=1)}^{(k)(n)}$ , then  $A^T = (\beta_{ij})_{(i=1)(j=1)}^{(n)(k)}$ . The matrix  $A$  is **symmetric** if  $A = A^T$ .

**Axiom (d)**

$$(\forall \alpha, \beta \in \mathbb{F})(\alpha\beta = 0 \Leftrightarrow \alpha = 0 \text{ or } \beta = 0)$$

**Exercise 5.7.** Prove that Axiom (d) holds in every field.

**Exercise 5.8.** Show that Axiom (d) fails in  $\mathbb{Z}/6\mathbb{Z}$ . So  $\mathbb{Z}/6\mathbb{Z}$  is not a field.

**Exercise 5.9.** If  $\mathbb{F}$  is finite and satisfies all field axioms except possibly (b5), then (b5)  $\iff$  (d). Note: (d) does **not** necessarily imply (b5) if  $\mathbb{F}$  is infinite:  $\mathbb{Z}$  is a counterexample.

**Theorem 5.10.**  $\mathbb{Z}/m\mathbb{Z}$  is a field  $\iff m$  is prime.

**Proof:**

- (1) If  $m$  is composite, i.e.,  $m = ab$  where  $a, b > 1$ , then  $\mathbb{Z}/m\mathbb{Z}$  is not a field: it violates axiom (d) because  $ab = 0$ .
- (2)  $\mathbb{Z}/p\mathbb{Z}$  is finite, thus need to show that it satisfies axiom (d):  $ab = 0$  in  $\mathbb{Z}/p\mathbb{Z}$ . **Prime property:**  $p \mid ab \implies p \mid a$  or  $p \mid b$ .

This property plays a key role in proving the **Fundamental Theorem of Arithmetic:** Every number has a unique prime decomposition.

**Exercise 5.11.** Use exercises below and the prime property to prove the Fundamental Theorem of Arithmetic.

**Definition 5.12 (Greatest Common Divisor).** Let  $a, b, d \in \mathbb{Z}$ . Then  $d = \text{g.c.d.}(a, b)$  if

- (i)  $d \mid a, d \mid b$  ( $d$  is a common divisor),
- (ii)  $(\forall e)(e \mid a \text{ and } e \mid b \implies e \mid d)$  ( $d$  is a multiple of every common divisor).

(This definition cannot distinguish between numbers and its negative: Example:  $\text{g.c.d.}(4, 6) = ?$ ; 2 is a g.c.d. and so is  $-2$ ).

**Theorem 5.13.**  $(\forall a, b)(\exists d = \text{g.c.d.}(a, b))$  and  $d$  is unique up to factor of  $\pm 1$ .

What is the greatest common divisor of  $(0, 0)$ ? Divisors of 0:  $(\forall x)(x \mid 0)$ , so every integer is a divisor of 0. Every divisor of 0 satisfies (i) above, but only 0 satisfies (ii) so  $\text{g.c.d.}(0, 0) = 0$ . (With respect divisibility, everything is a divisor of 0; and 1 is the divisor of everything).

**Exercise 5.14.**  $(\forall a, b \in \mathbb{Z})(\exists x, y \in \mathbb{Z})(d = ax + by)$  where  $d = \text{g.c.d.}(a, b)$ .

**Example 5.15.**  $\text{g.c.d.}(7, 11) = 1$ :  $7x + 11y = 1$ , for  $x = -3$  and  $y = 2$ .

**Exercise 5.16.** Prove; do not use prime factorization: if  $\text{g.c.d.}(a, b) = d$  then  $\text{g.c.d.}(ac, bc) = cd$ .

## 2 Polynomials, rational functions

Let  $\mathbb{F}$  be a field and let  $\mathbb{F}[x]$  be the set of polynomials over  $\mathbb{F}$ . Let  $f, g \in \mathbb{F}[x]$ .

**Definition 5.17 (Divisibility of polynomials).**  $f \mid g$  if  $\exists h \in \mathbb{F}[x]$  s.t.  $g = fh$ .

**Definition 5.18 (Greatest common divisor of polynomials).** Let  $d, f, g \in \mathbb{F}[x]$ .  $d = \text{g.c.d.}(f, g)$  is the **greatest common divisor** of  $f$  and  $g$  if

- (i)  $d \mid f$ ,  $d \mid g$ , and
- (ii)  $d$  is a multiple of all common divisors:  $(\forall e)(e \mid f \text{ and } e \mid g \implies e \mid d)$ .

g.c.d. is unique up to non-zero constant factors.

**Example 5.19.**  $\text{g.c.d.}(x^2 - 1, (x - 1)^2) = x - 1$  (there is no distinction between  $x - 1$  and  $73(x - 1)$ ).

**Definition 5.20.**  $f$  is irreducible if

- (i)  $\deg f \geq 1$
- (ii)  $(\forall g, h)(\text{if } gh = f \text{ then } \deg g = 0 \text{ or } \deg h = 0)$

**Theorem 5.21 (Division Theorem for Integers).**  $(\forall a, b)(\text{if } |b| \geq 1, \text{ then } (\exists q, r)(a = bq + r \text{ and } 0 \leq r < |b|))$ .

**Theorem 5.22 (Division Theorem for polynomials over a field).**  $(\forall f, g \in \mathbb{F}[x])(\text{if } g \neq 0, \text{ then } \exists q, r \in \mathbb{F}[x] \text{ s.t. } f = gq + r \text{ and } \deg(r) < \deg(g))$ .

**Theorem 5.23.** Every polynomial has a unique factorization (up to constant multiples) into irreducible factors.

**Example 5.24.**  $(x^2 - 1) = (x - 1)(x + 1) = (3x - 3)(\frac{1}{3}x + \frac{1}{3})$

Everything done so far in linear algebra is true for all fields (not just number fields). Denote “order of field  $\mathbb{F}$ ” by  $|\mathbb{F}|$ .

**Theorem 5.25 (Galois).** The orders of finite fields are the prime powers;  $\forall$  prime power  $q$ ,  $\exists!$  field  $\mathbb{F}_q$  of order  $q$  (unique up to isomorphism).

Note:  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  when  $p$  is a prime, but  $\mathbb{F}_q \neq \mathbb{Z}/q\mathbb{Z}$  when  $q$  is not a prime  $q = p^k$ ,  $k \geq 2$ .

**Definition 5.26.** The field  $\mathbb{F}$  has **characteristic**  $m$  ( $m \geq 1$ ) if  $\underbrace{1 + 1 + \dots + 1}_m = m \cdot 1 = 0$  and  $m$  is the smallest positive integer with this property. If no such  $m$  exists, we say that the field has characteristic 0.

What is the characteristic of  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ? Answer:  $\text{char } \mathbb{F}_p = p$ . What is the characteristic of  $\mathbb{C}$ ? Answer:  $\text{char } \mathbb{C} = 0$ . The same is true for number fields.

Consider the field of rational functions  $\mathbb{F}(x)$  over the field  $\mathbb{F}$ .

**Exercise 5.27.**  $\text{char } \mathbb{F}(x) = \text{char } \mathbb{F}$ . This gives examples of infinite fields of finite (i. e., non-zero characteristic).

**Exercise 5.28.** If  $\mathbb{F} \subset G$  is a subfield, then  $\text{char } \mathbb{F} = \text{char } G$ .

**Example 5.29.**  $\mathbb{Z}/5\mathbb{Z} \subset \mathbb{Q}$ . Is this a subfield? Answer: No, the operations are different; e. g.,  $3 + 4 = 7$  in  $\mathbb{Q}$  but  $3 + 4 = 2$  in  $\mathbb{Z}/5\mathbb{Z}$ .

**Exercise 5.30.**  $\text{char } \mathbb{F} = 0$  or prime.

**Exercise 5.31.** If  $\text{char } \mathbb{F} = 0$ , then  $\mathbb{Q}$  is a subfield of  $\mathbb{F}$ . If  $\text{char } \mathbb{F} = p$ , then  $\mathbb{Z}/p\mathbb{Z}$  is a subfield of  $\mathbb{F}$ .

**Theorem 5.32.** *If  $\mathbb{F}$  is a finite field of characteristic  $p$ , then  $|\mathbb{F}| = p^k$ .*

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ,  $\mathbb{F}_p \subset \mathbb{F}$ . If we have a field extension  $\implies$  bigger field is a vector space over the smaller field. Thus, we can treat  $\mathbb{F}$  as a vector space over  $\mathbb{F}_p$ . Let We can find a basis of  $\mathbb{F}$  over  $\mathbb{F}_p$ , i.e., every vector can be written as a linear combination of these basis vectors. Let  $\dim_{\mathbb{F}_p} \mathbb{F} = k$ . We, therefore, have a bijection:  $\mathbb{F} \longleftrightarrow \mathbb{F}_p^k$  so  $|\mathbb{F}| = |\mathbb{F}_p^k| = p^k$ , where  $x \mapsto [x]_B$ .

**Exercise 5.33.** Find an irreducible quadratic polynomial over  $\mathbb{F}_2$ .

**Solution:** What are quadratic polynomials:  $ax^2 + bx + c$ ,  $a, b, c \in \mathbb{F}_2 = \{0, 1\}$ . Since we want quadratic polynomials,  $a \neq 0$  so  $a = 1$ . Thus, we have  $x^2 + bx + c$  with  $b, c \in \{0, 1\}$ . Thus, there are 4 quadratic polynomials:

- (1)  $x^2 = x \cdot x$  not irreducible,
- (2)  $x^2 + x = x(x + 1)$  not irreducible,
- (3)  $x^2 + 1 = x^2 + 2x + 1 = (x + 1)^2$  not irreducible,
- (4)  $x^2 + x + 1$  irreducible.

Another way to see this: the deg = 1 polynomials are  $x$ ,  $x + 1$ , so  $x \cdot x$ ,  $x(x + 1)$ , and  $(x + 1)^2$  are the only reducible polynomials  $\implies x^2 + x + 1$  is irreducible).

**Theorem 5.34.**  $(\forall p), (\forall k), (\exists \text{ irreducible polynomials of deg } k \text{ over } \mathbb{F}_p.)$

**Corollary 5.35.**  $(\forall p)(\forall k)(\exists \mathbb{F}_{p^k}).$

Once we have irreducible polynomials of deg  $k$  over  $\mathbb{F}_p$ , we can immediately construct  $\mathbb{F}_{p^k}$ .