Scribe Notes for *Algorithmic Number Theory*
Class 4—May 21, 1998

Scribes: Jeremy Rotter, Yizhong Wang, and Wen Wang

Abstract

In this class we will finish the discussion of rings and cover some basic concepts related to fields.

1 Rings

In the previous class, a ring and its ideal were discussed. Suppose R is a ring and $I \subset R$ is an ideal. Then R/I is a factor ring.

Example 1.1. Let $R = \mathbb{Z}/(3)[X]$ and let $f(X) = 2X^2 + X + 1$. We can create a factor ring $I = R \cdot f(X)$ from the polynomial ring R. We can use the canonical representation of $R/I = R/(f)$, namely

$$\{0,\ 1,\ 2,\ X,\ X+1,\ X+2,\ 2X,\ 2X+1,\ 2X+2\}.$$

Addition is the same as addition in R, e.g. $(2X+1) + (X+2) = 0$. Multiplication is the multiplication in R mod f, e.g. $(2X+1) \cdot (X+2) = 2X^2 + X + X + 2 \bmod f = X + 1$.

Example 1.2. Let $R = \mathbb{Z}$ and let $I = \{6i : i \in \mathbb{Z}\}$. I is an ideal in R, and we can create the factor ring $R/I = \mathbb{Z}/(6)$.

2 Fields

Definition 2.1. A commutative ring R is a *field* if $R - \{0\}$ is an abelian group with respect to multiplication.

Some examples of fields are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}/(p)$. It is easy to prove that $\mathbb{Z}/(p)$ is a field. Clearly multiplication is commutative mod p. Also, $\mathbb{Z}/(p)$ is closed under multiplication and $\bar{1}$ is the identity mod p, so all it needs to be an abelian group (and therefore a commutative ring) is an inverse for all elements. By Fermat's theorem (2.1.3) [1], we know that any element $a \in \mathbb{Z}/(p)$ will have inverse $a^{p-2} \in \mathbb{Z}/(p)$, hence $\mathbb{Z}/(p)$ is a field.

Some non-examples of fields are $\mathbb{Z}$, $R[X]$, and $\mathbb{Z}/(n)$ where n is not prime. For a non-prime n, $\mathbb{Z}/(n)$ would possess zero-divisors, and hence $\mathbb{Z}/(n)$ would not be a group with respect to multiplication. For example, in $\mathbb{Z}/(6)$, $\bar{2} \cdot \bar{3} = \bar{0} \notin \mathbb{Z}/(6) - \{\bar{0}\}$. $\mathbb{Z}/(6) - \{\bar{0}\}$ is not closed under multiplication, and therefore is not a group. Hence, $\mathbb{Z}/(6)$ is not a field.

2.1 Vector Spaces

Definition 2.2. $\mathbb{V}$ is a *vector space* over a field $\mathbb{F}$ if $+$ is defined on $\mathbb{V}$ and $\mathbb{V}$ is an abelian group under addition. $\mathbb{F}$ acts on $\mathbb{V}$ by scalar multiplication, which satisfies

- $\cdot : \mathbb{F} \times \mathbb{V} \to \mathbb{V}$; and

- For $a, b \in \mathbb{F}$ and $v_1, v_2 \in \mathbb{V}$,
$$a \cdot v_1 + a \cdot v_2 = a \cdot (v_1 + v_2)$$
and
$$a \cdot v_1 + b \cdot v_1 = (a + b) \cdot v_1.$$

Facts

1. For every vector space $\mathbb{V}$ over field $\mathbb{F}$, there is a basis $B \subseteq \mathbb{V}$ such that every element of $\mathbb{V}$ can be written uniquely as a linear combination of elements of B, e.g. for $V \in \mathbb{V}$,
$$V = \sum_{b \in B} v_b \cdot b,$$
where all but a finite number of v_b are zero.

   Examples

   - $\mathbb{E}^n = \{(r_1, r_2, \ldots, r_n) : \ r_i \in R\}$ is a vector space over R,
   $\{(1, 0, \ldots, 0), \ (0, 1, \ldots, 0), \ \ldots, \ (0, 0, \ldots, 1)\}$ is a basis for $\mathbb{E}^n$.
   - $\mathbb{F}[x]$ is a vector space over $\mathbb{F}$,
   $\{1, x, x^2, x^3, \ldots, \}$ is a basis for $\mathbb{F}[x]$.

   Any two bases of a vector space $\mathbb{V}$ have the same cardinality, called the *dimension* of $\mathbb{V}$.

2. If U and V are finite dimensional vector spaces, with dimensions m and n, respectively, then any linear function
$$T : U \longrightarrow V$$
can be represented by an $n \times m$ matrix with respect to fixed bases of U and V.

   Example 2.3. Let $T : E^2 \to E^3$ be a linear mapping. In this case, $m = 2$ and $n = 3$. We can represent T with the 3×2 matrix
$$\begin{bmatrix} 3.5 & 7 \\ 50.7 & 0 \\ 3.3 & \frac{11}{3} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} r \\ s \\ t \end{bmatrix}.$$

2.2 Finite Fields

Definition 2.4. A field containing a finite number of elements is called a *finite field*.

Facts

1. There is a positive integer n such that $na = 0$ for all a in the field. The smallest such n is called the *characteristic* of the field.

2. The characteristic of a finite field $\mathbb{F}$ is always prime.

3. Let $\mathbb{F}$ be a field containing m elements with characteristic p. Then $\mathbb{F}$ is a vector space over $\mathbb{Z}/(p)$.

X	$\xrightarrow{\cdot X}$	$X+1$	$\xrightarrow{\cdot X}$	$2X+1$	$\xrightarrow{\cdot X}$	2
$\uparrow \cdot X$						$\downarrow \cdot X$
1	$\xleftarrow{\cdot X}$	$X+2$	$\xleftarrow{\cdot X}$	$2X+2$	$\xleftarrow{\cdot X}$	$2X$

Table 1: Powers of X in $\mathbb{Z}/(3)[x]/(f)$.

4. Let d be the dimension of $\mathbb{F}$ over $\mathbb{Z}/(p)$, and let $\{b_1, b_2, ..., b_d\}$ be a basis. Then

$$\mathbb{F} = \left\{ \sum_{i=1}^{d} a_i b_i : a_i \in \mathbb{Z}/(p), i = 1, 2, ..., d \right\}.$$

Hence $|\mathbb{F}| = p^d = m$.

Example 2.5. Choose $\alpha \in \mathbb{F} - \{0\}$. The set $A = \{\alpha^i : i \geq 0\}$ is finite. A spans a sub-vector space $\mathbb{F}'$ of $\mathbb{F}$. We can find the largest integer r such that $1, \alpha, \alpha^2, ..., \alpha^{r-1}$ are linearly independent. (This implies that $1, \alpha, \alpha^2, ..., \alpha^{r-1}, \alpha^r$ are linearly dependent.) Clearly $r \leq d$ (actually, $r|d$). $\mathbb{F}$ has dimension r and basis $\{1, \alpha, \alpha^2, ..., \alpha^{r-1}\}$. $\mathbb{F}'$ is a subfield of $\mathbb{F}$. In fact, $\mathbb{F}'$ is the smallest subfield of $\mathbb{F}$ that contains α. We have $\mathbb{Z}/(p) \subset \mathbb{F}' \subset \mathbb{F}$. $\mathbb{F}$ is also a vector space over $\mathbb{F}'$.
By the choice of r, we know there exist $a_{r-1}, a_{r-2}, ..., a_1, a_0 \in \mathbb{Z}/(p)$ such that

$$\alpha^r + a_{r-1}\alpha^{r-1} + ... + a_1\alpha + a_0 = 0.$$

This implies that

$$f_\alpha(X) = X^r + a_{r-1}X^{r-1} + ... + a_1X + a_0 \quad \in \ \mathbb{Z}/(p)[X]$$

is the *minimal polynomial* of α over $\mathbb{Z}/(p)$ and is irreducible. Actually, $\mathbb{Z}/(p)[X]/(f_\alpha) \cong \mathbb{F}'$.

In order to get a finite field of characteristic p, choose an irreducible polynomial f over $\mathbb{Z}/(p)$. Then, adjoin a root of f to $\mathbb{Z}/(p)$ to get $\mathbb{Z}/(p)[\alpha]$.

Example 2.6. Let $p = 3$ and let $f = X^2 + 2X + 2 \ \in \mathbb{Z}/(3)[X]$. Then f is irreducible over $\mathbb{Z}/(3)$. In $\mathbb{Z}/(3)[x]/(f) - \{0\}$, there are 8 distinct elements, which can be generated by X, as can be seen in Table 1. To understand Table 1 better, consider $(2X+1) \cdot X$:

$$(2X+1) \cdot X = 2X^2 + X - 2f = 2X^2 + X - (2X^2 + X + 1) = -1 = 2$$

From Table 1, we can see that $\mathbb{Z}/(3)[x]/(f) - \{0\}$ is a cyclic group with respect to multiplication.

Facts

1. $\mathbb{F}^* = \mathbb{F} - \{0\}$ is a cyclic group of order $p^d - 1$.
2. For every $a \in \mathbb{F}^*$, $a^{p^d-1} = 1$.
3. For every $a \in \mathbb{F}$, $a^{p^d} = a$.

4. The Frobenious map on $\mathbb{F}$: $\tau(a) = a^p$ is a linear function on $\mathbb{F}$ of characteristic p that fixes $\mathbb{Z}/(p)$.

   To see that the Frobenious map fixes $\mathbb{Z}/(p)$, notice that for any $a \in \mathbb{Z}/(p)$, $\tau(a) = a^p = a * a^{p-1}$, but by Fermat's Theorem, $a^{p-1} = 1$ in $\mathbb{Z}/(p)$, so $a^p = p$, and we have $\tau(a) = a$ for any $a \in \mathbb{Z}/(p)$.

   To see that the Frobenious map is linear, let $\{1, \alpha, \alpha^2, ...\alpha^{d-1}\}$ be a basis for $\mathbb{F}$ over $\mathbb{Z}/(p)$. Then for any $a \in \mathbb{F}$,

$$a = \sum_{i=1}^{d-1} a_i \alpha^i,$$

   where $a_i \in \mathbb{Z}/(p)$. So

$$a^p = \left(\sum_{i=1}^{d-1} a_i \alpha^i \right)^p = \sum_{i=1}^{d-1} a_i^p \alpha^{ip}$$

   But $a_i^p = a_i$ (since τ fixes $\mathbb{Z}/(p)$), so $\tau(a) = \sum_{i=1}^{d-1} a_i \alpha^{ip}$. From this, it is easy to see that, for any $k \in \mathbb{Z}/(p), \tau(ka) = k\tau(a)$, i.e., τ is linear.

2.3 Field Extensions

Definition 2.7. If $K \subseteq L$ are fields, L is called an *extension* of K.

Definition 2.8. If L is finite dimensional over K, then L is called a *finite extension* and the dimension of L over K is the degree of the extension, denoted by $[L{:}K]$.

Choose an irreducible polynomial f of degree d over K, and let α be a root of the polynomial. Then $K(\alpha)$ is a field extension of degree d. Note that $K(\alpha) \cong K[x]/(f)$.

Example 2.9. Let $K = \mathbb{Q}$, then $L = \mathbb{Q}(\sqrt{2})$ is a degree 2 extension of $\mathbb{Q}$. In this case, the irreducible polynomial is $f_{\sqrt{2}}(x) = x^2 - 2$. Notice that L is a vector field over K, with basis $\{1, \sqrt{2}\}$. With this basis, every element in L can be written as $a + b\sqrt{2}$ and the multiplication in L is

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

3 Next Time

In the next class we will begin to discuss complexity theory, from Chapter 3 in the book.

References

[1] E. Bach and J. Shallit, *Algorithmic Number Theory*, The MIT Press, Cambridge, Massachusetts, 1996.