

ICT12 T

9. *Finite fields*

26.10, 30.10, 6.11, 9.11 2012 SX.

9.1 The ring $\mathbb{Z}_n$

9.2 Construction of finite fields

9.3 Structure of the multiplicative group

9.4 Primitive polynomials

Notes

9.1 The ring $\mathbb{Z}_n$

Set $\mathbb{Z}_n$ to denote the **ring** $\mathbb{Z}/(n)$ of classes of integers modulo n . We usually represent its elements by the elements of the set $\{0, 1, \dots, n - 1\}$, which are the residues of the division by n , with the operations of sum and product the ordinary sum and product of integers, but reduced modulo n . So $i + j$ and $i * j$ really mean, when referred to the representation $\{0, 1, \dots, n - 1\}$ of $\mathbb{Z}_n$,

$\text{remainder}(i+j, n)$ and $\text{remainder}(i*j, n)$,

respectively.

Example. In $\mathbb{Z}_{15}$, $4 \times 11 = 14$ and $4 \times 4 = 1$.

We will also set $G(\mathbb{Z}_n)$, or $\mathbb{Z}_n^*$, to denote the (multiplicative) **group** of invertible elements of $\mathbb{Z}_n$.^{N1}

An element $k \in \{0, 1, \dots, n - 1\}$ is invertible modulo n if and only if $\gcd(k, n) = 1$.

In particular we see that $\mathbb{Z}_n$ is a **field** if and only if n is prime.

Example. The invertible elements of $\mathbb{Z}_{15}$ are $\{1, 2, 4, 7, 8, 11, 13, 14\}$; its inverses are $\{1, 8, 4, 13, 2, 11, 7, 14\}$.

We have, therefore, $|G(\mathbb{Z}_n)| = \varphi(n)$, where $\varphi(n)$ is *Euler's function* (by definition, $\varphi(n)$ is the number of $k \in \{0, 1, \dots, n - 1\}$ such that $\gcd(k, n) = 1$). In particular we have

$$a^{\varphi(n)} \equiv 1 \pmod{n} \text{ for any integer } a \text{ such that } \gcd(a, n) = 1. \text{ } ^{\text{N2}}$$

CC resources. [G\(Zn\(N\)\).cc](http://G(Zn(N)).cc), order.cc, inverse-mod-n.cc (in this example you can see that the inverse of $k \bmod n$ can be computed as an integer or directly as an element of $\mathbb{Z}_n$).

The function $\varphi(n)$ has the following properties:

1. $\varphi(nn') = \varphi(n)\varphi(n')$ if $\gcd(n, n') = 1$.
2. If p is prime, $\varphi(p^r) = p^{r-1}(p - 1)$.

Proposition. $\sum_{d|n} \varphi(d) = n$.

CC resources. See divisors.cc.

Examples. We can use the fields $\mathbb{Z}_p$ to construct RS codes, and they can be decoded by means of the decoder RS_ID implemented as a result of **P28**. Moreover, we know that $RS_p(k)$ has type $[p, k, p - k + 1]$ and hence that it can correct up to $\left\lfloor \frac{p-k}{2} \right\rfloor$ errors ($RS_p(k)$ is a short notation for $RS_{0..(p-1)}(K)$).

In particular, if $p - k = 2t$, then the type is $[p, p - 2t, 2t + 1]$, which gives us a wealth of possibilities for experimenting.

CC resources. See [RS5\(3\).cc](http://RS5(3).cc), [RS7\(3\).cc](http://RS7(3).cc), [RS11\(5\).cc](http://RS11(5).cc) and [RS_p\(p-2t\).cc](http://RS_p(p-2t).cc).

9.2 Construction of finite fields

Suppose A is a finite ring, like $\mathbb{Z}_n$ for n a positive integer. Let $q = |A|$.

Let $f = a_0 + a_1x + \cdots + a_{r-1}x^{r-1} + x^r \in A[x]$ be a **monic polynomial with coefficients in A** .

Then the call `extension(A,f)` constructs a structure that mathematically is denoted $A[X]/(f)$ and which can be described in concrete terms as follows:

- Its elements α have the form $\alpha_0 + \alpha_1x + \cdots + \alpha_{r-1}x^{r-1}$, $\alpha_j \in A$.
- The sum of two such elements, $\alpha + \beta$, is defined as the usual sum of polynomials: $(\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)x + \cdots + (\alpha_{r-1} + \beta_{r-1})x^{r-1}$.
- The product $\alpha * \beta$ is defined as the remainder of the division of the usual product of polynomials $\alpha * \beta$ by f , that is, `remainder( $\alpha * \beta$ ,f)`.

Theorem. With these operations $A[x]/(f)$ is a ring. Its cardinal is q^r .

Remark. $x^r = -(a_0 + a_1x + \cdots + a_{r-1}x^{r-1})$.

Remark. The call `extension(A,t,f)` works as `extension(A,f)`, but using t , instead of x , to express the elements α .

CC resources. `ring.cc` contains several illustrations of those calls.

Definition. A polynomial $f \in K[x]$ is said to be **reducible** if it is the product of two polynomials of degree lower than the degree of f . If f is not reducible, it is called **irreducible**.

Example. Assume $K = \mathbb{Z}_2$. Then in $K[x]$ there are only two polynomials of degree 1: x and $1 + x$. So the polynomials

$$x^2, x + x^2, (1 + x)^2 = 1 + x^2$$

are all the reducible polynomials of degree 2 in $K[x]$. It follows that $1 + x + x^2$ is the only irreducible polynomial of degree 2 over K . The ring $K[x]/(1 + x + x^2)$ has 4 elements: $\{0, 1, x, 1 + x\}$. The multiplication table is determined by the relation $x^2 = 1 + x$. It is easy to check that it is a field.

Theorem. The ring $K[x]/(f)$ is a field iff f is **irreducible**.

Remark. It is an easy exercise to see that any field of cardinal 4 is isomorphic to $\mathbb{Z}_2[x]/(1 + x + x^2)$.

Example. The reducible polynomials of degree 3 over $\mathbb{Z}_2$ are

$$x^3, x^2 + x^3, x + x^3, 1 + x + x^2 + x^3, x + x^2 + x^3, 1 + x^3.$$

It follows that there are only two irreducible polynomials of degree 3:

$$x^3 + x + 1, x^3 + x^2 + 1.$$

Remark. The method in the previous example also works for any field F_q in the place of $\mathbb{Z}_2$. For $r = 2$, the number of monic reducible polynomials is $(q + 1)q/2$, while the number of monic polynomials of degree 2 is q^2 . Hence the number of monic irreducible polynomials of degree 2 over F_q is $I_2(q) = q(q - 1)/2$. Note that in particular $I_2(2) = 1$, a fact that we already know.

A similar reasoning is valid for monic polynomial of degree 3. Indeed, there are q^3 monic polynomials of degree 3, while the number of monic reducible polynomials of degree 3 is

$$R_q = \binom{q+2}{3} + \frac{q^2(q-1)}{2} = \frac{2}{3}q^3 + \frac{1}{3}q$$

(the first summand counts polynomials that are the product of three monic linear factors and the second those that are the product of a monic linear factor and monic quadratic factor. It follows that the number of monic irreducible polynomials of degree 3 is

$$I_3(q) = q^3 - R_q = \frac{q^3}{3} - \frac{q}{3}.$$

In particular, $I_3(2) = 2$, as seen in a previous example.

Examples. If $a \in K$, K a field, $X^2 - a$ is irreducible over K if and only if a is not a square in K . For example, $X^2 + 1$ is irreducible over $\mathbb{Z}_3$, as the squares in $\mathbb{Z}_3$ are 0 and 1. Similarly, the squares of $\mathbb{Z}_7$ are 0, 1, 4 and 2, and hence the polynomials

$$X^2 - 3 = X^2 + 4, \quad X^2 - 5 = X^2 + 2, \quad X^2 - 6 = X^2 + 1$$

are irreducible over $\mathbb{Z}_7$.

Examples. If $a \in K$, $X^3 - a$ is irreducible over K if and only if a is not a cube in K . Since the cubes in $\mathbb{Z}_7$ are 0, 1 and 6, the polynomials

$$X^3 - 2 = X^3 + 5, \quad X^3 - 3 = X^3 + 4, \quad X^3 - 4 = X^3 + 3 \quad \text{and} \quad X^3 - 5 = X^3 + 2$$

are irreducible over $\mathbb{Z}_7$.

CC resources. The call `irreducible?(f,K)` returns true if f is irreducible over K and false otherwise. See irreducible1.cc for examples.

Theorem. For any $r > 0$ and any finite field K , there are irreducible polynomials in $K[x]$ of degree r .

Corollary. For any prime number p and any positive integer r there exists a finite field with p^r elements.

CC resources. If K is a field, r a positive integer and t a (free) variable, then the call `irreducible_polynomial(K, r, t)` produces an a monic polynomial of degree r with coefficients in K . This polynomial can be used to construct a field of cardinal q^r , where $q = |K|$. See irreducible2.cc for examples.

Theorem. The cardinal q of any finite field F has the form $q = p^r$, with p prime and r a positive integer.^{N3}

The prime p is called the *characteristic* of F . It is the least positive integer such that $p \cdot 1_F = 0$.

Theorem. Two finite fields with the same cardinal are isomorphic. And conversely, of course.

Corollary. Any finite field can be constructed, up to isomorphism, by a call `extension(Zmod(p),f)`, where f is any monic irreducible polynomial of degree r over $\mathbb{Z}_p$.

We will write $GF(q)$ to denote a finite field with q elements. In mathematics the notation $\mathbb{F}_q$ is often used.

Examples

- $1 + x + x^r \in \mathbb{Z}_2[x]$ is irreducible for $r = 2,3,4,6,7$. This allows us to construct $GF(4)$, $GF(8)$, $GF(16)$, $GF(64)$, $GF(128)$.
- $GF(32)$ can be constructed with the polynomial $1 + x^2 + x^5$
- $GF(256)$ with the polynomial $1 + x + x^3 + x^7 + x^8$.

CC resources. The fields constructed with these polynomials provide a new series of RS codes with interesting properties. See the examples in [RS4\(2\)](#), [RS8\(8-2t\).cc](#), [RS16\(16-2t\).cc](#), [RS32\(16-2t\).cc](#), [RS64\(16-2t\).cc](#).

9.3 Structure of the multiplicative group of a finite field

Order of an element. If K is a finite field and α is a non-zero element of K , the *order* of α , $\text{ord}(\alpha)$, is the least positive integer r such that $\alpha^r = 1$. Note that r exists and that it is a divisor of $q - 1$ (q the cardinal of K). Moreover, $r > 1$ except for $\alpha = 1$.

Example. In $\mathbb{Z}_5$ we have $\text{ord}(2) = \text{ord}(3) = 4$ and $\text{ord}(4) = 2$.

CC resources. If x is an invertible element in a constructed ring, `order(x)` yields its order.

Proposition. Let K be a finite field, $\alpha \in K - \{0\}$ and $r = \text{ord}(\alpha)$.

1. If $x \in K - \{0\}$ is such that $x^r = 1$, then there exists an integer k such that $x = \alpha^k$.
2. For every integer k , $\text{ord}(\alpha^k) = r / \gcd(k, r)$.
3. The elements of order r of K have the form α^k , with $\gcd(k, r) = 1$. In particular we have that if there exists an element of order r , then there are exactly $\varphi(r)$ elements of order r .

Proof. Consider the polynomial $f = X^r - 1 \in K[X]$. Since f has degree r and K is a field, f has at most r roots in K . Since r is the order of α , all the elements of the subgroup

$$R = \{1, \alpha, \dots, \alpha^{r-1}\}$$

are roots of f and hence f has no roots other than the elements of R . Since x is a root of f by hypothesis, $x \in R$. This settles point 1.

To establish 2, let $d = \gcd(r, k)$ and $s = r/d$. We want to see that α^k has order s . If $(\alpha^k)^m = 1$, then $\alpha^{km} = 1$ and hence $r|km$. Dividing by d we see that $s|(m(k/d))$. As s and k/d have no common prime divisors, it follows that $s|m$. Finally it is clear that

$$(\alpha^k)^s = \alpha^{k(r/d)} = \alpha^{r(k/d)} = 1$$

and this completes the proof of 2.

Finally 3 is a direct consequence of 1, 2 and the definition of $\varphi(r)$. $\square$

Primitive roots. A non-zero element α of a finite field K of cardinal $q = p^r$ is said to be a *primitive root* (or a *primitive element*) of K if $\text{ord}(\alpha) = q - 1$. In this case it is clear that

$$K^* = \{1, \alpha, \dots, \alpha^{q-2}\}.$$

Examples. In $K = \mathbb{Z}_2[x]/(x^2 + x + 1)$, $K^* = \{1, x, x^2\}$, so x is a primitive root of K . Similarly, in $L = \mathbb{Z}_2[t]/(t^3 + t + 1)$, $K^* = \{1, t, t^2, \dots, t^6\}$.

Exponential representation. If α is a primitive root of K , the representation $K^* = \{1, \alpha, \dots, \alpha^{q-2}\}$ of the elements of K is called *exponential representation* relative α . With this representation, the product of elements of K is particularly easy to obtain:

$$\alpha^i \alpha^j = \alpha^k, \text{ where } k = i + j \bmod q - 1 .$$

Examples. The elements 2 and 3 are the primitive roots of $\mathbb{Z}_5$. The elements x and t in the examples in the previous page are primitive roots of $GF(4)$ and $GF(8)$, respectively.

Theorem. Let K be a finite field of cardinal q and d a positive integer. If $d|(q-1)$, then K contains exactly $\varphi(d)$ elements of order d .

Proof. Let $p(d)$ be the number of elements of K that have order d . It is clear that

$$\sum_{d|(q-1)} p(d) = q - 1,$$

as the order of any non-zero element is a divisor of $q-1$. Now observe that $p(d) = \varphi(d)$ if $p(d) \neq 0$ and that $\sum_{d|(q-1)} \varphi(d) = q-1$, with which the proof is easily completed. $\square$

Proposition. Let L be a finite field, K a subfield of L and $q = |K|$. Let r be the positive integer such that $|L| = q^r$. If α is a primitive element of L , then $1, \alpha, \dots, \alpha^{r-1}$ is a basis of L as a K -vector space.^{N4}

9.4. Primitive polynomials

If f is an irreducible polynomial of degree r over $\mathbb{Z}_p$, p a prime, then

$$\mathbb{Z}_p(x) = \mathbb{Z}_p[x]/(f)$$

is a field of cardinal p^r . The element x may be primitive or not. In the case $\mathbb{Z}_2(x) = \mathbb{Z}_2[x]/(x^2 + x + 1)$, for example, it is primitive, but in the case $\mathbb{Z}_3(x) = \mathbb{Z}_3[x]/(x^2 + 1)$, $\text{ord}(x) = 4$.

Proposition. Let K be a finite field and $f \in K[x]$ a monic irreducible polynomial, $f \neq x$ and consider the field $L = K[x]/f$. If $m = \deg(f)$, then $\text{ord}(x)$ is the least divisor d of $q^m - 1$ such that $f \mid (x^d - 1)$.

Proof. The order of x is the least divisor d of

$$|L| - 1 = q^m - 1$$

such that $x^d = 1$. But this is equivalent to say that $x^d - 1$ is 0 mod f , which is the same as asserting that $x^d - 1$ is a multiple of f . $\square$

Definition. If x is a primitive root, we say that f is *primitive* over $\mathbb{Z}_p$. The least divisor d of $q^m - 1$ such that $f|(x^d - 1)$ is called the *period* (or *exponent*) of f .

CC resources. The period of over a field of q elements is computed by `period(f,q)`, or `period(f)` if $q = 2$:

```

period(f,q):=
begin
  local r=degree(f),
        D=set(divisors(q^r-1)),
        x=variable(f)
  for d in D do
    if remainder(x^d-1,f)==0
    then
      return d
    end
  end
end
#
period(f):= period(f,2)

```

For examples, see [period.cc](#)

Notes

N1 (p. 2). If A is a ring with multiplicative unit (usually denoted 1 , or 1_A), then the set $G(A)$ of invertible elements of A forms a group with the product operation of A . Note that if $x, y \in G(A)$, then $x * y \in G(A)$, for

$$(x * y) * (y^{-1}x^{-1}) = 1$$

and hence $y^{-1}x^{-1}$ is the inverse of $x * y$. Note that the proof shows that the product of A need not be commutative.

The group $G(A)$ is also denoted A^* .

Examples. 1) $G(\mathbb{Z}) = \{\pm 1\}$. 2) A is a field if and only if $G(A) = A - \{0\}$. 3) If K is a field, $G(K[X]) = K - \{0\} = G(K)$. 4) If $M_n(K)$ is the ring of square matrices of dimension n , then $G(M_n(K))$ is the set of invertible matrices of order n with entries in K (this group is usually denoted $GL(n, K)$ and it is called the *linear group* over K of dimension n).

N2 (p. 3). If G is a finite group of order n , then $a^n = e$ for any $a \in G$ (e denotes the identity element of G). Indeed, there is a least positive integer r such that $a^r = e$. As $\{e = a^0, a, \dots, a^{r-1}\}$ is a subgroup of order r of G , we know that $r|n$ (Lagrange lemma) and this implies the assertion.

N3 (p. 10). Let F be a finite field and $q = |F|$. Consider the sequence

$$1 \cdot 1_F, 2 \cdot 1_F, 3 \cdot 1_F, \dots, n \cdot 1_F, \dots$$

Since F is finite, we either can find a term $n \cdot 1_F$ in this sequence such that $n \cdot 1_F = 0_F$ or else a term $k \cdot 1_F$ that is repeated n steps later, $k \cdot 1_F = (k + n) \cdot 1_F$, in which case we also have $n \cdot 1_F = 0$. Let p the least positive integer such that $p \cdot 1_F = 0$. This p is primer, for if $p = r \cdot s$, then $0 = p \cdot 1_F = (r \cdot s) \cdot 1_F = (r \cdot 1_F) \cdot (s \cdot 1_F)$, which can only occur if either $r \cdot 1_F = 0$ ($\Leftrightarrow r = p$) or $s \cdot 1_F = 0$ ($\Leftrightarrow s = p$). Now it is easy to check that $K = \{0_F, 1_F, 2 \cdot 1_F, \dots, (p-1) \cdot 1_F\}$ forms a subfield of F and that K is isomorphic to $\mathbb{Z}_p$. Finally we can regard F as a vector space over K and therefore $|F| = |K|^r = p^r$, where $r = \dim_K(F)$.

N4 (p. 15) **Proof.** If $\alpha \in L$ and $1, \alpha, \dots, \alpha^{r-1}$ are linearly dependent over K , there would exist $a_0, \dots, a_{r-1} \in K$, not all zero, such that

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

If we let

$$h = a_0 + a_1x + \cdots a_{r-1}x^{r-1} \in K[X],$$

then h is a polynomial of positive degree $< r$ such that $h(\alpha) = 0$. It follows that there exists a monic irreducible polynomial $f \in K[x]$ of degree $s < r$ such that $f(\alpha) = 0$. This implies that the set of expressions

$$\{k_0 + k_1\alpha + \cdots + k_{s-1}\alpha^{s-1} \text{ with } k_0, k_1, \dots, k_{s-1} \in K\}$$

is a subfield isomorphic to $K' = K[x]/(f)$. But then the order of α divides $|K'| - 1 = q^s - 1 < q^r - 1$ and α would not be a primitive root. $\square$