Finite Fields of Order p^m (1)

The following results were discussed in the previous lecture:

- ▷ The order of a finite field is a prime power.
- ▷ There is a unique finite field for each such order.
- ▷ If the order of a finite field is a prime p, one may act on $\{0, 1, \ldots, p-1\}$ with addition and multiplication modulo p.

The case p^m, $m > 1$, is (somewhat) more complicated. In the sequel, p is always a *prime*.

Finite Fields of Order p^m (2)

The collection of all polynomials $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with arbitrary degree and $a_i \in \mathrm{GF}(q)$ is denoted by $\mathrm{GF}(q)[x]$. (Earlier example: these polynomials form a commutative ring with identity.)

Example. We consider $\mathrm{GF}(3)[x]$:

$$(x^3 + 2x^2 + 1) + (x^2 + x + 1) = x^3 + 3x^2 + x + 2 = x^3 + x + 2,$$

$$(x + 1) \cdot (x^2 + 2x + 1) = x^3 + 2x^2 + x + x^2 + 2x + 1 = x^3 + 1.$$

Irreducible Polynomials

A polynomial $f(x) \in \mathrm{GF}(q)[x]$ is **irreducible** if $f(x)$ cannot be factored into a product of lower-degree polynomials in $\mathrm{GF}(q)[x]$. Otherwise, it is said to be **reducible**.

Example 1. The polynomial $x^3 + 1 \in \mathrm{GF}(3)[x]$ is not irreducible (a factoring is given in the previous example).

Example 2. The polynomial $x^2 + x + 1 \in \mathrm{GF}(2)[x]$ is irreducible, but $x^2 + x + 1 \in \mathrm{GF}(4)[x]$ is not. (Irreducibility in $\mathrm{GF}(2)[x]$ follows as $x \cdot (x + 1) = x^2 + x$, $(x + 1) \cdot (x + 1) = x^2 + 1$, and $x \cdot x = x^2$.)

- ⇒ The term *irreducible* must be used only with respect to a specific ring.

Primitive Polynomials

An irreducible polynomial $f(x) \in \mathrm{GF}(p)[x]$ of degree m is **primitive** if the smallest n for which $f(x)$ divides $x^n - 1$ is $n = p^m - 1$. (It can be shown that $f(x)$ always divides $x^{p^m - 1} - 1$.)

Example. The polynomial $x^3 + x + 1 \in \mathrm{GF}(2)[x]$ is primitive, since it is irreducible and does not divide any of $x^4 - 1$, $x^5 - 1$, and $x^6 - 1$ ($p^m - 1 = 2^3 - 1 = 7$).

NOTE!!! In $\mathrm{GF}(2)$, $-1 = 1$.

Example. In $\mathrm{GF}(2)[x]$, $x^7 - 1 = x^7 + 1$.

There are $\phi(2^m - 1)/m$ binary primitive polynomials of degree m; for small values of m, see [Wic, Appendix A].

Constructing a Field of Order p^m

Let p be a prime and $m > 1$.

1. Take a primitive polynomial $f(x)$ of degree m in $\mathrm{GF}(p)[x]$, and let α be a root of $f(x)$ ($f(\alpha) = 0$).
2. The elements of the field are $0, 1 = \alpha^0, \alpha^1, \ldots, \alpha^{p^m-2}$ taken modulo $f(\alpha)$.
3. Carry out addition and multiplication modulo $f(\alpha)$.

Note: We do not explicitly solve $f(\alpha) = 0$ for α.

Example: Constructing GF(4)

We take the primitive polynomial $f(x) = x^2 + x + 1 \in \mathrm{GF}(2)[x]$, and let α be a root of $f(x)$. Then $\alpha^0 = 1$, $\alpha^1 = \alpha$, and $\alpha^2 = \alpha + 1$ (and $\alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha = 1$).

$+$	0	1	α	$\alpha{+}1$
0	0	1	α	$\alpha{+}1$
1	1	0	$\alpha{+}1$	α
α	α	$\alpha{+}1$	0	1
$\alpha{+}1$	$\alpha{+}1$	α	1	0

$\cdot$	0	1	α	$\alpha{+}1$
0	0	0	0	0
1	0	1	α	$\alpha{+}1$
α	0	α	$\alpha{+}1$	1
$\alpha{+}1$	0	$\alpha{+}1$	1	α

A Finite Field as a Vector Space

The polynomial representation for $\mathrm{GF}(p^m)$ has coefficients in the *ground field* $\mathrm{GF}(p)$. Therefore, one may interpret $\mathrm{GF}(p^m)$ as a vector space over $\mathrm{GF}(p)$.

Example. GF(4).

0	$\leftrightarrow$	$(0, 0)$
1	$\leftrightarrow$	$(0, 1)$
α	$\leftrightarrow$	$(1, 0)$
$\alpha^2 = \alpha + 1$	$\leftrightarrow$	$(1, 1)$

A field of prime power order $\mathrm{GF}(p^m)$ is often called an *extension* of $\mathrm{GF}(p)$.

Computing in Fields (1)

- ▷ Addition is direct if one considers polynomials modulo $f(\alpha)$ = vectors over $\mathrm{GF}(p)$.
- ▷ Multiplication is direct if one represent the elements of the field as 0 and α^i, $0 \le i \le p^m - 2$.
- ▷ **But:** In neither of these cases can the other operation be carried out in a direct way.

Computing in Fields (2)

The study of algorithms for operating on fields is one of most important research topics in computational algrebra with many important applications (in coding, cryptography, etc.).

Two possibilities if the field is relatively small:

- Construct a look-up table of size $q \times q$.
- Use so-called *Zech logarithms*; this requires a table of size q.

Subfields

A subset $S \subseteq \mathrm{GF}(p^m)$ that is a field is called a **subfield** of $\mathrm{GF}(p^m)$. Every field $\mathrm{GF}(p^m)$ has itself as subfield; any other subfield is called *proper*.

Theorem. The subfields of $\mathrm{GF}(p^m)$ are exactly the fields $\mathrm{GF}(p^a)$ where $a \mid m$.

Example. $\mathrm{GF}(64) = \mathrm{GF}(2^6)$ contains $\mathrm{GF}(2^1)$, $\mathrm{GF}(2^2)$, $\mathrm{GF}(2^3)$, and $\mathrm{GF}(2^6)$ as subfields.

Minimal Polynomials

Let $\alpha \in \mathrm{GF}(q^m)$. The **minimal polynomial** of α with respect to $\mathrm{GF}(q)$ is the smallest-degree nonzero polynomial $f(x) \in \mathrm{GF}(q)[x]$ such that $f(\alpha) = 0$.

Theorem 3-2. For each $\alpha \in \mathrm{GF}(q^m)$ there exists a unique monic polynomial $f(x) \in \mathrm{GF}(q)[x]$ of minimal degree such that

1. $f(\alpha) = 0$,
2. $\deg(f(x)) \leq m$,
3. $g(\alpha) = 0$ implies that $g(x)$ is a multiple of $f(x)$,
4. $f(x)$ is irreducible in $\mathrm{GF}(q)[x]$.

Another definition for *primitive polynomials:* the minimal polynomials for primitive elements in a Galois field.

Conjugates of Field Elements

Motivation: If we want a polynomial $f(x) \in \mathrm{GF}(q)[x]$ to have a root $\alpha \in \mathrm{GF}(q^m)$, what other roots must the polynomial have?

The **conjugates** of $\alpha \in \mathrm{GF}(q^m)$ with respect to the subfield $\mathrm{GF}(q)$ are the elements $\alpha^{q^0} = \alpha, \alpha^{q^1}, \alpha^{q^2}, \ldots$, which form the *conjugacy class of α with respect to* $\mathrm{GF}(q)$.

Theorem 3-3. The conjugacy class of $\alpha \in \mathrm{GF}(q^m)$ with respect to $\mathrm{GF}(q)$ contains d elements (that is, $\alpha^{q^d} = \alpha$) with $d \mid m$.

Conjugacy Classes and Roots

Example. By Theorems 2-10 and 2-12, the orders of elements in GF(16) are 1, 3, 5, and 15. Let α be an element of order 3. The conjugates of α with respect to GF(2) are $\alpha, \alpha^2, \alpha^{2^2} = \alpha^3\alpha = \alpha$, so the conjugacy class is $\{\alpha, \alpha^2\}$.

Theorem 3-4. Let $\alpha \in \mathrm{GF}(q^m)$ and let $f(x)$ be the minimal polynomial of α with respect to $\mathrm{GF}(q)$. The roots of $f(x)$ are exactly the conjugates of α with respect to $\mathrm{GF}(q)$.

Corollary. All the roots of an irreducible polynomial have the same order.

Example: Minimal Polynomials for GF(8)

Let α be root of the primitive polynomial $x^3 + x + 1 \in \mathrm{GF}[2](x)$. Then the elements of GF(8) are

$0 = 0$, $\alpha^0 = 1$, $\alpha^1 = \alpha$, $\alpha^2 = \alpha^2$, $\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = \alpha^2 + \alpha + 1$, $\alpha^6 = \alpha^2 + 1$.

Conjugacy class	Minimal polynomial
$\{0\}$	$M_*(x) = x - 0 = x$
$\{\alpha^0 = 1\}$	$M_0(x) = x - 1 = x + 1$
$\{\alpha, \alpha^2, \alpha^4\}$	$M_1(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4) = x^3 + x + 1$
$\{\alpha^3, \alpha^6, \alpha^5\}$	$M_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^5) = x^3 + x^2 + 1$

Factoring $x^n - 1$ (1)

Theorem 3-5. The nonzero elements in $\mathrm{GF}(q^m)$ form the complete set of roots of $x^{(q^m-1)} - 1 = 0$.

Proof: For an arbitrary $\alpha \in \mathrm{GF}(q^m)$, $\mathrm{ord}(\alpha) \mid (q^m - 1)$ by Theorem 2-10, and therefore α is a root of $x^{(q^m-1)} - 1 = 0$. Moreover, the equation $x^{(q^m-1)} - 1 = 0$ is of degree $(q^m - 1)$ and can therefore have at most $(q^m - 1)$ roots. Therefore, the nonzero elements of $\mathrm{GF}(q^m)$ comprise the complete set of roots. □

Example. Factorization of $x^7 - 1$ in $\mathrm{GF}(2)[x]$. Using the results on the previous slide,

$$x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1).$$

Factoring $x^n - 1$ (2)

We now know how to factor $x^{(q^m-1)} - 1$ into irreducible polynomials in the ring $\mathrm{GF}(q)[x]$. What about the general case $(x^n - 1)$?

All roots of $(x^n - 1)$ are nth roots of unity. We need to

1. identify the field where we can find all of these roots,
2. separate the roots into conjugacy classes, and
3. compute the minimal polynomials of the nth roots of unity.

If we have an element $\beta \in \mathrm{GF}(p^m)$ of order n, then the solutions to $x^n - 1 = 0$ are $1, \beta, \beta^2, \ldots, \beta^{n-1}$. These *distinct* elements of order n are often called *primitive nth roots of unity.*

How to find β and the order of the field?

Factoring $x^n - 1$ (3)

By Theorem 2-12, we know that if $n \mid (p^m - 1)$, then there are $\phi(n) > 0$ elements of order n in $\mathrm{GF}(p^m)$.

The **order of** q **modulo** n is the smallest integer m such that $n \mid (q^m - 1)$.

Example. Since $5 \not| \, (2^1 - 1)$, $5 \not| \, (2^2 - 1)$, $5 \not| \, (2^3 - 1)$, $5 \mid (2^4 - 1)$, GF(16) is the smallest binary extension field in which one may find primitive 5th roots of unity (and the order of 2 modulo 5 is 4).

Example: Factoring $x^{25} - 1$ in GF$(2)[x]$

Let β be a primitive 25th root of unity. The order of 2 modulo 25 is 20, so we consider $\mathrm{GF}(2^{20})$. The 25 roots of $x^{25} - 1 = 0$ can be grouped into the following conjugacy classes with respect to GF(2):

$\{1\}$,
$\{\beta, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^7, \beta^{14}, \beta^3, \beta^6, \beta^{12}, \beta^{24}, \beta^{23}, \beta^{21}, \beta^{17}, \beta^9, \beta^{18}, \beta^{11}, \beta^{22}, \beta^{19}, \beta^{13}\}$,
$\{\beta^5, \beta^{10}, \beta^{20}, \beta^{15}\}$.

Consequently, $x^{25} - 1$ factors into three irreducible binary polynomials: one of degree one $(x - 1)$, one of degree four, and one of degree twenty.

Cyclotomic Cosets

The **cyclotomic cosets** *modulo* n with respect to GF(q) constitute a partitioning of the integers into sets of the form

$$\{a, aq, aq^2, \ldots, aq^{d-1}\}.$$

Example. Cyclotomic cosets modulo 25 with respect to GF(2) (cf. previous example):

$\{0\}$,
$\{1, 2, 4, 8, 16, 7, 14, 3, 6, 12, 24, 23, 21, 17, 9, 18, 11, 22, 19, 13\}$,
$\{5, 10, 20, 15\}$.

Polynomials Modulo $f(x)$

Earlier result: If the ring of integers is reduced modulo m, then we get a field if m is a prime, and a commutative ring with identity otherwise. What if rings of polynomials are reduced modulo a polynomial $f(x)$?

The ring of polynomials GF$(q)[x]$ modulo $f(x)$ is usually denoted by GF$(q)[x]/f(x)$.

Theorem 3-6. If $p(x) \in \mathrm{GF}(q)[x]$ is an irreducible polynomial, then GF$(q)[x]/p(x)$ is a field.

Ideals

Let R be a ring. A nonempty subset $I \subseteq R$ is said to be an **ideal** if

1. I forms a group under the additive operation in R.
2. For all $a \in I$ and all $r \in R$, $r \cdot a \in I$ and $a \cdot r \in I$.

Example 1. In any ring R, $\{0\}$ and R are ideals. These are the *trivial* ideals.

Example 2. Let $R_n = \mathrm{GF}(2)[x]/(x^n + 1)$. The set $\{0, x^4 + x^3 + x^2 + x + 1\}$ forms an ideal in R_5. (Note that $x^5 + 1 = (x^4 + x^3 + x^2 + x + 1)(x + 1)$.)

Principal Ideals

An ideal I contained in a ring R is said to be a **principal ideal** if there exists $g \in I$ such that every element $c \in I$ can be expressed as $m \cdot g$ for some $m \in R$.

The element g is commonly called a **generator element**, and the ideal generated by g is denoted by $\langle g \rangle$.

▷ Ideals in $\mathrm{GF}(q)[x]/(x^n - 1)$ play a central role in the theory of linear cyclic codes.

Some Properties of Ideals

Theorem 3-7. Let I be an ideal in $\mathrm{GF}(q)[x]/(x^n - 1)$. Then the following hold:

1. There exists a unique monic polynomial $g(x) \in I$ of minimal degree.
2. The ideal I is principal with generator $g(x)$.
3. The polynomial $g(x)$ divides $(x^n - 1)$ in $\mathrm{GF}(q)[x]$.