Math 221B, Mon Apr 11

- Reading for today: 15.8, 16.1.
- Reading for Wed Apr 13: 16.2–16.3.
- PS07 due tomorrow; PS08 due one week after.

Five facts for finite fields

char $K = p$, i.e., $p = 0$.

Theorem: Suppose p prime, $q = p^e$, K a field of order q. Then:

1. Each element of K is a root of $x^q - x$.
2. $K^\times$ is cyclic of order $q - 1$.
3. There exists a field of order q, and all fields of order q are isomorphic.
4. For $k > 0$, K contains a subfield of order p^k if and only if k divides e.
5. The irreducible factors of $x^q - x$ over $\mathbf{F}_p[x]$ are precisely the irreducibles in $\mathbf{F}_p[x]$ whose degrees divide e.

gp thy

class'n

uniqueness

(All $K = \mathbf{F}_p[x]/(h(x))$, h irr)

Group-theoretic results

K field ord q

1. Each element of K is a root of $x^q - x$.
2. $K^\times$ is cyclic of order $q - 1$.

Proof:

① $K^\times = K - \{0\}$, so $|K^\times| = q-1$.

LAGRANGE $\Rightarrow$ every $\alpha \in K^\times$ has ord α div $q-1 \Rightarrow \alpha^{q-1} = 1 \ \forall \alpha \in K^\times$.

So every $\alpha \neq 0$ is root of $x^{q-1} - 1$ and, if $x = 0$, root of $x^q - x$. ☺

② Fact (Finite Abelian Gps)

$K^\times \cong C_{n_1} \times C_{n_2} \times C_{n_3} \times \cdots \times C_{n_s}$

where $n_s \mid n_{s-1} \mid \cdots \mid n_2 \mid n_1$ ($n = n_1$)

$n_1 = \operatorname{ord} \zeta^{-1}$

And: cyclic $\Leftrightarrow s = 1$.

Ex $C_{20} \times C_{10} \times C_5$ not cyclic,

C_{1000} ← min # cyclics.

Note: $\forall \alpha \in K^\times$, $\alpha^n = 1$. So each α is a root of $x^n - 1 \Rightarrow n \geq q-1$

$\Rightarrow n = q-1 \Rightarrow K^\times$ cyclic.

Note: Proof of 2 is very nonconstructive.
Finding a generator for a given K in any kind of constructive way is essentially an open problem.

In fact, simpler problems are still open: Still not known if there are infinitely many p such that 2 generates multiplicative group of F_p (!!!).

If you could solve this, could probably make $ in encryption....

Existence of a field of order q: preliminaries

Thm: There exists a field of order $q = p^e$, and all fields of order q are isomorphic.

Proof: First, observe that in any field of characteristic p:

1. $x^q - x$ has no multiple roots; and
2. $(x+y)^p = x^p + y^p$.

$p = 0$

Then prove:

Claim: For $q = p^e$, the roots of $x^q - x$ in K form a subfield of K.

(1) f has mult roots $\Leftrightarrow \gcd(f, f') \neq 1$.

$\frac{d}{dx}(x^q - x) = qx^{q-1} - 1 = -1$

So $\gcd(f, f') = 1 \Rightarrow$ no mult roots

(2) Pf by example: $p = 5$

$$(x+y)^5 = x^5 + 5x^4y + 10x^3y^2$$
$$+ 10x^2y^3 + 5xy^4 + y^5$$
$$= x^5 + y^5 \quad (5 = 0).$$

Gen'l: $\binom{p}{k} = 0 \pmod p$ for $0 < k < p$

1. $x^q - x$ has no multiple roots; and
2. $(x+y)^p = x^p + y^p$.

Claim
Roots of $x^q - x$ form subfield.

I.e. $F = \{\alpha \in K \mid \alpha^q = \alpha\}$ subfield.

$\alpha, \beta \in F$;

$(x^{32} = (((x^2)^2)^2)^2)^2)$

$(\alpha+\beta)^2 = (\alpha+\beta)^{\beta^2}$ ← e times

$= (\cdots((\alpha+\beta)^\beta)^\beta \cdots)^\beta = \alpha^{\beta^2} + \beta^{\beta^2} = \alpha^1 + \beta^2$

So F closed under $+$.

Closed under $-$ similar;

closed $\times, \div$ easier, e.g.:

$\alpha^2 = \alpha \Rightarrow (\alpha^{-1})^2 = \alpha^{-1}$

both

Pf Thm

By repeatedly adjoining elements, we can construct an extension L of F_p in which x^q-x factors into linear factors.

Let K be the subfield of L consisting of the roots of x^q-x in L. x^q-x has no repeated roots, so K is a field of q elements.

BOO-YAH

(pf of uniqueness omitted)

Existence of a field of order q

Thm: There exists a field of order $q = p^e$, and all fields of order q are isomorphic.

Proof of existence: Let K be an extension of $\mathbf{F}_p$ in which $x^q - x$ splits.

Not'n The field order q is $\mathbb{F}_q = GF(q)$

Subfields of a finite field K, $|K| = p^e$

If F is a subfield of K, $|F| = p^k$, then K is a v.s. over F, so:

$|K| = |F|^d$ $\quad A = \dim_F K$

$p^e = (p^k)^A \Rightarrow k \mid e$

Conversely, if k divides e, let $q' = p^k$. Then $q' - 1$ divides $q - 1$, so:

let α be gen of $K^\times$. (b/c $y-1 \mid y^q - 1$)

b/c $q'-1 \mid q-1$, $\exists \beta$ order $q-1$ in $K^\times$.

So $\{0, 1, \beta, \ldots, \beta^{q'-1}\}$ are q' roots

$x^{q'} - x$.

the

So $F = \{0, 1, \beta, \ldots, \beta^{q-1}\}$

is a subfield of K of order q.

(And those roots are only possible subfield order q.)

Ex 5 $p=2, q=2^4 (e=4)$

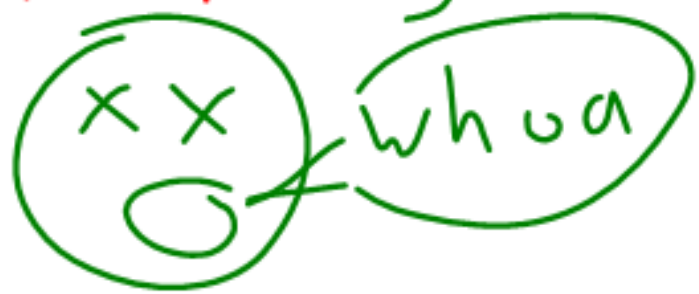
$x^{16}-x$

$= x(x+1)$ $k=1$

$\cdot (x^2+x+1)$ $k=2$

$\cdot (x^4+x+1)(x^4+x^3+1)$

$\rightarrow (x^4+x^3+x^2+x+1)$ $k=4$



Factorization of $x^q - x$ into irreducibles over $\mathbf{F}_p$

Let $q = p^e$ and let K be a field of order q.

If an irreducible $f \in \mathbf{F}_p[x]$ has degree k dividing e, let $F = \mathbf{F}_p[x]/(f) = \mathbf{F}_p(\beta)$. Since $|F| = p^k$: F subfield of K, and β is a common root of $f, x^q - x$.

Last: If irr f has common root w/ g, then f div g.

(C) f div $x^q - x$

Conversely, suppose f is an irreducible factor of $x^q - x$ in $\mathbf{F}_p[x]$. Let β be a root of f in K. deg $f = k$.

Then $\mathbf{F}_p(\beta)$ is subfield of K, order p^k.

Fact 4 $\Rightarrow$ k div e.

Primitive elements

Useful for proofs, if not in examples:

Theorem

Let F be a field of characteristic 0, and let K be a finite extension of F. Then $K = F(\alpha)$ for some $\alpha \in K$.

Why: We know

$K = F(\alpha_1, \ldots, \alpha_r)$

$F(c_1\alpha_1 + c_2\alpha_2 + \cdots + c_r\alpha_r) = K$

for all but finitely many c_i.

Point: Simplifies proofs by replacing an r-step induction with a single step.

Pf of uniqueness

Ⓐ k, k' fields order $q = p^e$

$k = \mathbb{F}_p(\alpha)$ for some $\alpha \in k$.

$\Rightarrow f = \min \text{poly}(\alpha), \deg f = e$.

$f \mid x^q - x$.

$\Rightarrow k'$ also consists of roots of $x^q - x$, and f factor, so $\exists$ root β of f in $k' \Rightarrow k' = \mathbb{F}_p(\beta) \cong \mathbb{F}_p(\alpha)$

Symmetric polynomials

R a ring of coefficients.

- S_n (symmetric group on $\{1, \ldots, n\}$) acts on $\{u_1, \ldots, u_n\}$ by permuting indices, and therefore acts on $R[u_1, \ldots, u_n]$.
- To say that $g \in R[u_1, \ldots, u_n]$ is a **symmetric polynomial** means that g is fixed by the action of every $\sigma \in S_n$. Example:

$$g(u_1, u_2, u_3) =$$

- Key examples: the **elementary symmetric polynomials**:

The point of the elementary symmetric polynomials

If

$$\begin{aligned} f(x) &= (x - u_1)(x - u_2) \cdots (x - u_n) \\ &= x^n - a_1 x^{n-1} + a_2 x^{n-2} - \cdots \pm a_{n-1} x \mp a_n, \end{aligned}$$

then:

The Symmetric Functions Theorem

Theorem

If $g \in R[u_1, \ldots, u_n]$ is symmetric, then g is a polynomial function of the elementary symmetric functions $s_1, \ldots, s_n$.

Methods:

1. Solve for undetermined coefficients by plugging in well-chosen values for $u_1, \ldots, u_n$.
2. Inductively:
   - Let $g^\circ(u_1, \ldots, u_{n-1}) = g(u_1, \ldots, u_n)$.
   - Solve for g° in terms of the elementary symmetric functions of one fewer variable: $g^\circ = Q(s_1^\circ, \ldots, s_{n-1}^\circ)$.
   - **FACT:** $g - Q(s_1, \ldots, s_n) = s_n h$, where h is a symmetric polynomial of degree smaller then $\deg g$.

Why do we care about this right now?

Theorem

For $f \in F[x]$, suppose

$$\begin{aligned} f(x) &= x^n - a_1 x^{n-1} + a_2 x^{n-2} - \cdots \pm a_{n-1} x^{n-1} \mp a_n \\ &= (x - \alpha_1) \cdots (x - \alpha_n). \end{aligned}$$

If g is symmetric in n variables with coefficients in F, then $g(\alpha_1, \cdots, \alpha_n) \in F$.

Proof: