Math 221B, Wed Apr 06

- Reading for today: 15.6–15.7.
- Reading for Mon Apr 11: 15.8, 16.1–16.2.
- ~~PS02 due Mon Feb 14.~~ PS07 due Mon Apr 11
- Problem session Fri Apr 08, time TBA on Zoom.

Abstract extensions

Suppose $f \in F[x]$, $I = (f(x))$.

- To create $K = F(\alpha)$ where $f(\alpha) = 0$, let $K = F[x]/I$ and $\alpha = x + I$. Then:

Note: operations of a quotient ring are defined by operations on coset reps, e.g., (r+I)(s+I)=rs+I, (r+I)+(s+I)=(r+s)+I

- Repeat this process until f is completely factored, get **splitting field** for $f(x)$. (Can show this is unique up to isomorphism.)

Field F(alpha_1,...,alpha_n), where f(x) = (x-alpha_1)...(x-alpha_n)

What happens to irreducibles in an extension?

$f, g \in F[x]$, K/F extension.

1. If $g = qf + r$ in $F[x]$, then same holds in $K[x]$.
2. So f divides g in $F[x]$ if and ony if f divides g in $K[x]$;
3. And $\gcd(f, g)$ same in $F[x]$ and $K[x]$.
4. If $\alpha \in K$ and $f(\alpha) = 0 = g(\alpha)$, then $\gcd(f, g) \neq 1$.
   Conversely: If $\gcd(f, g) \neq 1$, there exists α in some K/F such that $f(\alpha) = 0 = g(\alpha)$.

Pf: Extend F by a root of gcd(f,g).

5. If f irreducible in $F[x]$ and f and g have a common root, then f divides g.

(1) If division with remainder in F[x] produces g = qf + r, then deg r < deg f. That equation g = qf + r still holds in K[x], so by the uniqueness of division with remainder (given deg r < deg f), it must be the correct answer in K[x].

4 ⇒ 5 (A) f irred in F[x], f(α) = 0 = g(α), α ∈ K

By 4, gcd(f,g) ≠ 1, so f div g. (since f irreducible)

The derivative in $F[x]$

Definition

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

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$$

then we define

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2 a_2 x + a_1.$$

Can check that product rule:

$$\frac{d}{dx}(f(x)g(x)) = f'(x)g(x) + f(x)g'(x)$$

holds for this purely algebraic definition of f', even if F has nothing to do with the real numbers.

f' and multiple roots

Suppose $f \in F[x]$.

Thm: For $\alpha \in K/F$, TFAE:

1. $(x-\alpha)^2$ divides f
2. $f(\alpha) = 0$ and $f'(\alpha) = 0$

In fact:

Cor: TFAE:

1. f has a multiple root α in some extension K/F
2. $\gcd(f, f') \neq 1$

Proof of Cor:

gen'lize on P507

i.e. $(x-\alpha)^2$ div f

in $F(x)$

Thm 1 $\Rightarrow$ 2

$f(\alpha) = 0$, $f'(\alpha) = 0$.

If $f(x) = g(x)(x-\alpha)^2$

then $f'(x) = g'(x)(x-\alpha)^2 + g(x) \cdot 2(x-\alpha)$

Cor 1 $\Leftrightarrow$ 2

1 $\Rightarrow$ 2 from Thm

2 $\Rightarrow$ 1 by (result 4 from two slides back)

Both 2 ⇒ 1 PSOT

Some conditions when irreducibles never have multiple roots

char R: smallest n s.t. 1+...+1 = 0.
If 1+...+1 is never 0, char R = 0.
Fields have char either 0 or prime p.

n times

Theorem

Suppose $f \in F[x]$ and f **irreducible** *over F.*

1. *f has multiple roots in some K/F if and only if $f' = 0$.*
2. *If F has characteristic 0, then f has no multiple roots.*

Proof:

① $\deg f' < \deg f$, and f irred, so only way to get $\gcd(f, f') = f$ is if $f' = 0$. ($n \geq 1$)

② If $f(x) = a_n x^n + \cdots$, $f'(x) = n a_n x^{n-1} + \cdots$

Which can't be equal to 0 unless n=0 in F.

Ex. $F = \mathbb{F}_p(t)$

$f(x) = x^p - t \qquad \alpha = \sqrt[p]{t}$

f irred

In char p, $r, s \in R$

$(r+s)^p = r^p + s^p$ $\boxed{p=5}$

Ex $(r+s)^5 = r^5 + 5r^4s + 10r^3s^2 + 10r^2s^3 + 5rs^4 + s^5 = r^5 + s^5$

$(x-\alpha)^p = x^p - \alpha^p = x^p - t$ So we get p-fold mult root

How to make a finite field

Let K be a finite field. First observations:

- K must have **characteristic** p, where p is prime.
- If K has char p, then K has $\mathbf{F}_p$ as a subfield, so $|K| = q = p^e$ (since K is a vector space over $\mathbf{F}_p$).
- **Fact to be proven:** $K = \mathbf{F}_p[x]/(f)$, where f is some irreducible in $\mathbf{F}_p[x]$. (where deg f = e)

$\dim_{\mathbf{F}} K$

Example: Field of order 4:

char 2

$\mathbb{F}_4$ $4 = 2^2$ Need irred f of deg 2

$f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ irred

So $\mathbb{F}_2[x]/(x^2+x+1)$ field order 4.

Let $\alpha = x + I$; then $\alpha^2 + \alpha + 1 = 0$

So $\alpha^2 = \alpha + 1$

Note: we can use this relation to do all the computing you like in F_4 in terms of alpha.

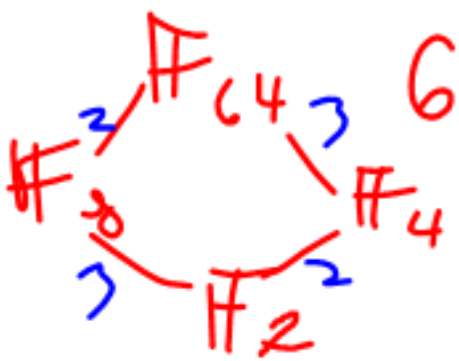
Five facts for finite fields

$F^\times = F - \{0\}$, mult gp

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.

magic poly



$64 = 2^6$ $\quad x^{64} - x$ = product of all irreds in F_2[x] of degrees 1, 2, 3, 6.

Group-theoretic results

$|K| = q = p^e$

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

Proof:

① $|K^\times| = q - 1$, so all elts of $K^\times$ order div $q-1$

So $\forall \alpha \in K^\times$, $\alpha^{q-1} = 1 \Rightarrow \alpha^{q-1} - 1 = 0$

$\Rightarrow \alpha^q - \alpha = 0$. Also works for 0. ☺

(In fact: $x^q - x = \prod_{\alpha \in K} (x - \alpha)$)

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:

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

Then prove:

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

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 a splitting field of $x^q - x$ over $\mathbf{F}_p$.

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:

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

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 $|F| = p^k$:

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.