Welcome! Everything is fine.

When you're connected by zoom:

- Use a laptop or desktop with a large screen so you can read these words clearly.
- To conserve bandwidth, please turn off your camera.
- Please mute your microphone unless I call on you.
- Please have the chat window open to ask questions.
- Reading for today: 15.7; for after break: 16.1–16.2.
- Exam 2: Take-home emailed out tomorrow, due Wed Apr 08.

Exam 2 covers PS04-07 (portions from Chs. 12 and 13)

Last: Multiple roots and the derivative

Last: For $f \in F[x]$, there exists K/F in which f has a multiple root iff $\gcd(f, f') \neq 1$.

Theorem

$f \in F[x]$ irreducible has multiple roots in an extension of F iff $f' = 0$.

some

Cor: If characteristic of $F = 0$, then irreducible f has no multiple roots in any extension of F.

char(F) = additive order of 1 in F
(unless order = infty, when char(F)=0.
(So char(Q)=0, char(Z/(p))=p.)

Proof of Thm:

If f in F[x] irreducible, then gcd(f,g) = f if f divides g and 1 otherwise. The only way that f can divide the polynomial f' of lower degree is when f' = 0.

Example: If char(F)=2, f(x) = x^4+x^2+1, then f'(x)=4x^3 + 2x = 0.

Converse: If f'=0, then gcd(f,f')=f.

Proof of Cor: When char(F) = 0, no positive integer = 0. So:

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots \neq 0$$

$(a_n \neq 0)$ unless f(x) is a const polynomial.

Finite fields: First facts

Goal: Understand all finite fields K.

* Because finite fields are finite, they must have finite characteristic.

* If char(K) = a*b, a,b>1, then K can't be a field b/c a,b are then zero divisors. So char(K) = p for some integer prime p.

* That means that there exists a copy of F_p = Z/(p) (where p = char(K)) as a subfield of K.

* That also means that K is a field extension of F_p, which means that K is a vector space over F_p, which means that the order of K is a power of p -- we'll usually denote this |K| = q = p^r.

Example: $\mathbb{F}_4$

Let K = F_2[x]/(x^2+x+1). x^2+x+1 is irreducible over F_2, so K is a field.

Let α = image of x in K. So $\alpha^2+\alpha+1=0$

Recall: $\{1, \alpha\}$ is basis for K over $\mathbb{F}_2$

So $K=\{0,1,\alpha,\alpha+1\}$, $|K|=4=2^2$ $p=2, r=2$

$\mathrm{char}(K)=2$, so $K \neq \mathbb{Z}/(4)$ $(2=0)$

$\cdot$	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	1	α

$\alpha^2=\alpha+1$

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

$=2\alpha+1=1$

$(\alpha+1)^2=\alpha^2+2\alpha+1=\alpha^3+1$

$K^\times \cong C_3$ cyclic of order 3

Five finite field facts

Theorem

p prime, $q = p^r$, K a field of order q.

1. *Elements of K are roots 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. *K contains a subfield of order $p^k \Leftrightarrow k$ divides r.*
5. *Irreducible factors of $x^q - x$ over $\mathbb{F}_p$ are irreducibles in $\mathbb{F}_p[x]$ whose degrees divide r.*

precisely the

There exists a unique field of order q=p^r.

Proof of Fact (1)

K a field of order q.
Observe that $|K^\times| = q - 1$.

So by Lagrange's Thm, multiplicative order of any a in $K^\times$ divides q-1.
I.e., a^{q-1} = 1, i.e., a^{q-1} - 1 = 0.

So any nonzero a in K is a root of x^{q-1} - 1, and since 0 is a root of x, all elements of K are roots of x(x^{q-1} - 1) = x^q - x.

Conversely, since degree of x^q-x is q, x^q-x can have at most q roots, so K contains all of the (distinct) roots of x^q-x, and we can write:

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

So elements of K are precisely roots of $x^q - x$.

Proof of Fact ~~(1)~~ (2)

WTS $K^\times$ cyclic

Definition

Exponent of a finite multiplicative group G is smallest n such that $x^n = 1$ for all $x \in G$.

LCM of all orders so

Cor of classification of finite abelian groups: If G is a finite abelian group of exponent n, there exists an element of G of order n.

By contradiction:

So suppose exponent of $K^\times$ is $n < q - 1$.

So ETS exponent of $K^\times$ is equal to q-1.

By argument from proof of (1), we see that every nonzero element of K is a root of x^n - 1, and therefore, each of the q distinct elements of K is a root of x^{n+1} - x.

But n+1 < q, which means that the polynomial x^{n+1} - x has more than n+1 roots (the q distinct elements of K).

Contradiction.

Proof of (3): Existence

Recall: can always add roots to split any polynomial in a finite extension.

Let $x^q - x$ split completely in L/F; let K be roots of $x^q - x$ in L.

Claim: K is a subfield of L. Enuf to show that K closed under addition, negation, product, inverse, and contains 1. Interesting parts are addition and negation.

Suppose $\alpha, \beta \in K$. K = all roots of x^q - x.

$q = p^r$

$(\alpha+\beta)^p = \alpha^p + \binom{p}{1}\alpha^{p-1}\beta + \cdots + \binom{p}{p-1}\alpha\beta^{p-1} + \beta^p$

$\binom{p}{k}$ div by p so $= 0 \pmod p$

pth power is a field automorphism, called Frobenius autom.

$= \alpha^p + \beta^p$

$(\alpha+\beta)^q = (\alpha+\beta)$ to pth power r times

$= \alpha^{p^r} + \beta^{p^r} = \alpha^q + \beta^q = \alpha + \beta$ b/c $\alpha, \beta \in K$.

So $\alpha+\beta \in K$.

Pf - $\alpha \in K$ similar (cases $p=2$, $p=$ odd).

So K subfield; q elts?

K will have q elements in it unless f(x) = x^q - x has multiple roots.
But f'(x) = qx^{q-1} - 1 = -1 b/c q=0 (mod p).
So gcd(f, f') = 1, so roots of f are distinct, and K contains q elements.

Proof of (3): Uniqueness

Suppose K and K' have order $q = p^r$. Note: $x^q - x$ splits completely in K and in K'.

Let $K^\times = \langle \alpha \rangle$, $f(x)$ irr poly of α in $\mathbb{F}_p$.

After break: Uniqueness then Ch. 16.

Exam 2 is on PS04-07, Ch 12 and 13 parts.

Proof of (4): subfields

Suppose $|K| = p^r$.
If L is a subfield of K: $[K : \mathbb{F}_p] =$

Converse: Suppose $q' = p^k$, $r = kd$. B/c $K^\times$ cyclic order $q - 1$:

Proof of (4): factoring $x^q - x$

Let K be a field of order $q = p^r$.

Suppose $g(x)$ irred factor of $x^q - x$ over $\mathbb{F}_p$. g has a root $\beta \in K$.

Converse: Suppose $g(x)$ irreducible degree k, k divides r.

Example: Computing in $\mathbb{F}_{16}$

$m(x) = x^4 + x + 1$ irreducible over $\mathbb{F}_2$. Let α be a root of $m(x)$, so $\mathbb{F}_{16} = \mathbb{F}_2(\alpha) = \mathbb{F}_2[x]/(m(x))$.