Math 128B, Mon Apr 19

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: Chs. 22–23. ~~Reading for Mon: Ch. 23~~
- Reading for Wed: Chs. 1, 4, 5, 7 (S_n, A_n, D_n, $C_n \approx \mathbf{Z}_n$). We'll be going off-book somewhat. . . 8, 9, 10
- PS08 due tonight, PS09 outline due Wed night.
- Problem session Fri Apr 23, 10am–noon.
- Second round of music: `https://forms.gle/v4Xta3E9u3At9sRV8`

Finite fields

Recall: Finite field of characteristic p is a vector space over $\mathbf{Z}/(p)$ and therefore has order p^e for some $e \geq 1$. In fact:

Theorem

(up to isomorphism)

For each prime p and $e \geq 1$, there exists a unique field of order $q = p^e$, denoted by $GF(q)$; namely, $GF(q)$ is the splitting field of $x^q - x$ over $\mathbf{F}_p$.

Proof: Uses existence and uniqueness of splitting fields.

Let E be a field of order q = p^e.
The nonzero elements of E are all units and therefore form the group of units of E, denoted by E*. Note that |E*| = q-1, so by Lagrange's Theorem (!!!!), the (multiplicative) order of any nonzero element of E must divide q-1.

I.e., for $a \in E$, $a \neq 0$, $a^{q-1} = 1$.
$\Rightarrow$ Every non-0 elt of E is root of $x^{q-1} - 1 = 0$

$\Rightarrow$ Every elt of E is root of $x^q - x = \underbrace{x(x^{q-1}-1)}_{\deg q}$,

$\Rightarrow$ $x^q - x = \prod_{a \in E} (x-a)$

<u>Cor</u> $\forall a \in E$, $a^q = a$.

$\Rightarrow$ E splitting field of $x^q - x$.

Let K = splitting field of $x^q - x$ over $\mathbb{Z}_p$

(Don't yet know that $|K| = q$.)

Let $E = \{a \in K \mid a^q = a\}$

B/c K char p.
We know $\rho: K \to K$ given by $\rho(x) = x^p$ is an autom. of K.

Let $\varphi = \rho^e = \underbrace{\rho \cdot \rho \cdots \rho}_{e \text{ times}}$, autom.

But $\varphi(x) = x^{p^e} = x^q$

Since E is fixed set of an autom, E subfield of K; and since $x^q - x$

has q roots, E has order q

So E is a field of order q.

(Note! No mult roots b/c b/c $(x^q - x)' = q x^{q-1} - 1 = -1$.)

<u>Ex</u> Field of order 4:

$E = \mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ $\quad |E| = 2^2 = 4$

$\alpha^2 = \alpha + 1$ $\quad E = \{0, 1, \alpha, \alpha+1\}$

$\alpha^2 + \alpha + 1 = 0$

Observe: $\quad (+1 = -1)$

$$(x+0)(x+1)(x+\alpha)(x+(\alpha+1))$$

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

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

$$= x(x^3+0x^2+\underbrace{(\alpha^2+1+\alpha)}_{=0}x+\underbrace{(\alpha^2+\alpha)}_{1})$$

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

$$= x^4+x = x^4-x$$

Note: Typo here corrected from live class

So in $E = \mathbb{Z}_2[x]/\langle x^2+x+1\rangle$

$\alpha^2 = \alpha+1$ $\quad GF(4)$

$$x^4 - x = x(x-1)(x-\alpha)(x-(\alpha+1))$$

$\Rightarrow E$ is split field of $x^4 - x$.

A common confusion

Note that while $GF(p) \approx \mathbf{Z}_p$, for $e \geq 2$ and $q = p^e$, $GF(q) \not\approx \mathbf{Z}_q$.

Example: $GF(8)$ vs. $\mathbf{Z}_8$.

The ring Z_8 has zero divisors, and also 2 has no inverse in Z_8.

$GF(8) \approx \mathbb{Z}_2[x]/(x^3+x+1)$

irred, so field

$\mathbb{Z}_8$

$\cdot$	0	1	2	3	4
2	0	2	4	6	0
4					

The multiplicative group of a finite field is cyclic

p prime, $e \geq 1$, $q = p^e$.

So GF(q) has an element of order q-1, called a primitive elt.

Theorem

The group of units of $GF(q)$ is cyclic of order $q-1$.

Proof: Define the **exponent** of a finite group G to be smallest $n \geq 1$ such that $a^n = 1$ for all $a \in G$.

Let G be the group of units of $GF(q)$, $|G| = q-1$. From classification of finite abelian groups (!!), the exponent of

(Ch 8!!)

$$G \approx \mathbf{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbf{Z}_{p_k^{n_k}}$$

is $\mathrm{lcm}(p_1^{n_1}, \ldots, p_k^{n_k})$. This $= q-1$ if and only if no primes p_i are repeated if and only if G is cyclic; otherwise $< q-1$.

$\mathbb{Z}_n \oplus \mathbb{Z}_k \approx \mathbb{Z}_{nk} \Leftrightarrow \gcd(n,k) = 1$

Assume (by way of contradiction) that G is not cyclic.

Then $\exists\, n < q-1$ s.t. $a^n = 1$ for all $a \in G = GF(q)^*$.

So the poly $x^n - 1$ has $q-1$ distinct zeros (elts of G).

But that means that x^n - 1 is a polynomial of degree n < q-1 with q-1 zeros, and a polynomial of degree n can't have more than n zeros!!!!! Contradiction, which means that G is cyclic.

Note: Proof is by contradiction and therefore extremely nonconstructive.

If you could figure out an algorithm for finding primitive elements in a finite field => for sure a Ph.D., probably a fancy job, maybe you would be famous (for math).

Example: $GF(9)$

Construction, orders of elements, primitive elements, factorizations of $x^9 - x$ and $x^2 + 1$.

$GF(9) = \mathbb{Z}_3[x] / \langle x^2+1 \rangle$ $\alpha^2 = -1$

$\alpha^1 = \alpha, \alpha^2 = -1, \alpha^3 = -\alpha, \alpha^4 = (-1)^2 = 1$

order$(1) = 1$

order$(\alpha) = 4$

order$(-1) = 2$

order$(-\alpha) = 4$

If ord$(a) = n$

ord$(a^k) = \dfrac{n}{\gcd(k, n)}$

$GF(9)^*$ cyclic order 8

$\Rightarrow$ every other non-0 elt is prim.

(Recall: Cyclic order 8 has 4 generators b/c $\underbrace{\varphi}_{\text{Euler phi}}(8) = 4$)

<u>Check</u>: $\operatorname{ord}(1+\alpha) = 8$.

$$x^9 - x = x(x-1)(x-(-1))(x-\alpha)(x-(\alpha+1))(x-(\alpha-1))(x-(-\alpha))(x-(-\alpha+1))(x-(-\alpha-1))$$

$$x^2+1 = (x-\alpha)(x+\alpha)$$

Construction of finite fields

$\mathbb{F}_p = \mathbb{Z}_p$

Theorem

Let E be a finite field of order p^e. Then there exists some irreducible $m(x) \in \mathbf{F}_p[x]$ such that $E \approx F_p[x]/\langle m(x) \rangle$.

Proof: $|E| = p^e$ $\quad E^* = \langle \alpha \rangle$

So $E = \mathbb{Z}_p(\alpha)$

Let $m(x) =$ min poly of α

$E \approx \mathbb{Z}_p[x]/\langle m(x) \rangle$

B/c $|E| = p^{\deg m} \Rightarrow \deg m = e$.

<u>Cor</u> $m(x)$ divide $x^q - x$

(actually $x^{q-1} - 1$)

So if $q = p^e$, then

$(x^{q-1} - 1)$ is a mult of

every irr poly of

deg e.

<u>Ex</u> Can find irr polys of deg 7 over $\mathbb{Z}_3$ by factoring $(x^{3^7} - x)$

Subfields of a finite field

p prime, $e \geq 1$, $q = p^e$.

Theorem

For each divisor d of e, $GF(q)$ has exactly one subfield of order p^d, and those are the only subfields of q.

Exmp: Subfields of $GF(5^{12})$.

Next time.

Proof of subfields theorem

p prime, $e \geq 1$, $q = p^e$.

Theorem

For each divisor d of e, $GF(q)$ has exactly one subfield of order p^d, and those are the only subfields of q.

Proof: Only possible orders are p^d where d divides e because $GF(q)$ is a v.s. over any subfield K:

Existence: Suppose d divides e, $K = \left\{\alpha \in GF(q) \mid \alpha^{p^d} = \alpha\right\}$, $GF(q)^* = \langle \beta \rangle$.

Ruler-and-compass constructions

Suppose we start w/a straightedge, compass, and a unit length:

I.e., from those starting ingredients, we can:

1. Intersect two lines
2. Intersect a circle and a line
3. Intersect two circles

Q: Which lengths can we construct? I.e., which points can we capture as one of those types of intersections?

Constructible fields

Call $\alpha \in \mathbf{R}$ **constructible** if we can construct a segment of length α. Then

Theorem

The set of constructible numbers F is closed under $+$, $-$, $\times$, and reciprocals; i.e., F is a subfield of $\mathbf{R}$.

Proof: Suppose we have a and b constructed. To construct ab:

Square root extensions are possible

Theorem

F is closed under taking square roots.

Only square root extensions are possible

Suppose we follow a sequence of steps $1, \ldots, n$ to construct a given length. Let F_k be the field generated by all lengths constructed up through step k (and $F_0 = \mathbf{Q}$). Because each operation involves taking an intersection of two lines, a line and a circle, or two circles, $F_{k+1} \subseteq F_k(\sqrt{a})$ for some $a \in F_k$. By multiplicativity of degree, we see that:

Theorem

$[F_n : \mathbf{Q}] = 2^t$ for some $t \geq 0$.

So for any constructible length a, considering $\mathbf{Q} \subseteq \mathbf{Q}(a) \subseteq F_n$:

A specific non-constructible angle

Let $\theta = \frac{2\pi}{18} = 20^\circ$. If we can construct θ, we can construct $\alpha = \cos\theta$, and from trig identities, can show that α is a zero of $p(x) = 8x^3 - 6x - 1$. Can show $p(x)$ is irreducible, so $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 3$, which means that α is non-constructible.