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....
- 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 $e \ge 1$. In fact:

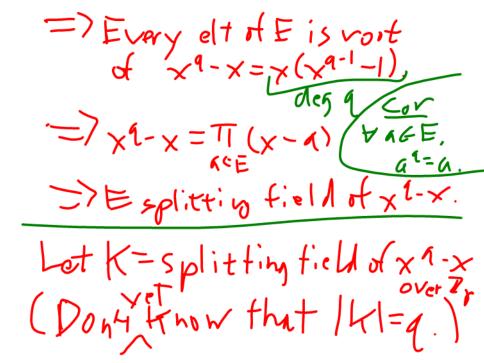
Theorem (up to isomorphism)

For each prime p and $e \ge 1$, 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.



Lot E= {a+ | a1 = a} BICK Charp K > Kgiven by

We know p. K > Kgiven by

p(x)=xolis an autom. of K. Let 4=p=p.p. , anton. But $\varphi(x) = xp^e - x^1$ Since E'il fixed set of an intem, Eshbeight Ki, and since x1-x

has grouts, Enasorder Moto! No nult roots b/c) (Noto! No nult roots b/c) (Noto! (x1-x)=qx-1=-1. Ex Field & order 4: F=Z.6x)/(x+x+1) |E|=2=4 2= 4+1 = = <0,1, x, x+1) 0 b s p r ve: (+1=-1)

$$(x+0)(x+1)(x+a)(x+(a+1))$$
= $x(x^2+(x+1)x+a)(x+(a+1))$
= $x(x^2+(x+1)+(x+1))x^2+(a+(x+1))x$
+ $x(a+1)$
= $x(x^2+(x^2+1)+(x^2+1+a)x+(x^2+a)$
= $x(x^2+1)$
= $x(x^2+1)$
= $x(x^2+1)$
= $x(x^2+1)$
= $x(x^2+1)$
Note: Typo here corrected from live class

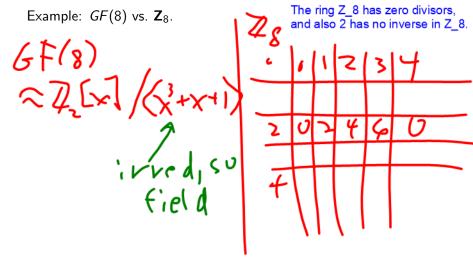
So in
$$E = \mathbb{Z}[x]/(x^{2}+x+1)$$

 $x^{2} = a+1$ $GF(4)$
 $x^{4}-x=x(x-1)(x-x)(x-(x+1))$

=>Eis split field of x"-x.

A common confusion

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



The multiplicative group of a finite field is cyclic

p prime, $e \ge 1$, $q = p^e$. So GF(q) has an element of order Theorem q-1, called a primitive elt.

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 $n \ge 1$ 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 7 + 7 = 7

(Ch 8!!)
$$G \approx \mathbf{Z}_{\rho_1^{n_1}} \oplus \cdots \oplus \mathbf{Z}_{\rho_k^{n_k}}$$

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

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

So the poly x"-1 has q1 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 .

G+(9)=
$$\mathbb{Z}_3[x]/\langle x^2+1\rangle$$
 $\alpha^2=\cdot 1$
 $\alpha^2-\alpha,\alpha^2=-1,\alpha^3=-\alpha,\alpha^4=+1)^2=1$

order(1) Order($\alpha^2=-1$) order(1) order($\alpha^2=-1$) or

(Recall: Cyclic or Arr 8 has

4 generators
$$b/c_{\varphi}(8)=4$$
)

Enler phi

Chect: $ora(1+\alpha)=8$.

 $x^{-1}-x^{-1}=x^{-1}(x^{-1})(x^{-1}-x^{-1})(x^{-1}-x^{-1})(x^{-1}-x^{-1})(x^{-1}-x^{-1})(x^{-1}-x^{-1})(x^{-1}-x^{-1})(x^{-1}-x^{-1})(x^{-1}-x^{-1})(x^{-1}-x^{-1})(x^{-1}-x^{-1})(x^{-1}-x^{-1})(x^{-1}-x^{-1})$

Construction of finite fields

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:
$$E = pe E^* = \langle a \rangle$$
So $E = \mathbb{Z}_p(x)$
Let $m(x) = min poly of a$
 $E \sim \mathbb{Z}_p(x)/\langle m(x) \rangle$
 $\mathcal{B}(c) | E | = pe f = e$.

Cor m(x) livide x1-x (actually xr-1-1) So it q=pe, then (xq-'-1) is a mult of every irr poly of Ex Cantina irrpolyed Aeg 7 over Z, by factoring (x3-x)

Subfields of a finite field

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

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 $GF(5^{12})$.



Proof of subfields theorem

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

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, $K = \{ \alpha \in GF(q) \mid \alpha^{p^d} = \alpha \}$, $GF(q)^* = \langle \beta \rangle$.

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 $t \ge 0$.

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.