Math 128B, Wed Apr 21

Exam 3: In 12 days, Mon May 3. Covers Chs 20-23, PS07-09.

- 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 Wed: Chs. 1, 4, 5, 7, 8, 9, 10. (S_n, A_n, D_n, $C_n \approx \mathbf{Z}_n$). Goal: Ch 32 $V = C_2 \oplus C_2$
- PS09 outline due tomorrow night, full version due Mon.
- Problem session Fri Apr 23, 10am–noon.
- Second round of music: `https://forms.gle/v4Xta3E9u3At9sRV8`

Fri Apr 30: Sample exam run-through 11am.

Five Facts for Finite Fields

1. **Prime power:** The characteristic of a finite field must be a prime p, and its order must be $q = p^e$ for some $e \geq 1$.
2. **Orders of elements:** The multiplicative group of a finite field is cyclic; i.e., if F has q elements, $F^\times$ must contain at least one element of order $q - 1$. F*
3. **Magic polynomial:** If F is a field of order q, then every $\alpha \in F$ is a root of $x^q - x$, or in other words, $\alpha^q = \alpha$ for every $\alpha \in F$. Consequently, $x^q - x$ factors as the product of all $(x - \beta)$, where β runs over all elements of F. I.e. F is splitting field of x^q-x
4. **Construction:** Every finite field of characteristic p is isomorphic to $\mathbf{F}_p[x]/(m(x))$ for some irreducible polynomial $m(x)$. $\mathbb{Z}_p$ If $q=p^e$, $\deg m = e$
5. **Classification:** For any prime p and $q = p^e$ ($e \geq 1$), there exists a field $\mathbf{F}_q$ of order q that is unique up to isomorphism. GF(q)

Recall:
* Any non-0 element of a field is a unit
* Units of any commutative ring form a group

F* = {all non-0 elements of F}
= group of units of F (sometimes U(F) in other contexts)

F* called "multiplicative group of F"

Ex. $GF(11) = \mathbb{Z}_{11}$

$GF(11)^* = U(\mathbb{Z}_{11}) = U(11)$

$\approx$ cyclic order 10

$|GF(11)^*| = 10$ Lagrange $\Rightarrow$ order div 10

1, 2, 5, 10

So any elt order > 5 is gen.

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^{\overbrace{4}^{\text{mod } 10}} \overset{16}{=} \underbrace{5}_{\text{mod } 11},\ 2^5 = 10$$

So $\operatorname{ord}(2) > 5$

$\Rightarrow \operatorname{ord}(2) = 10$, 2 prim.

$$\operatorname{ord}(4) = \operatorname{ord}(2^2) = \frac{10}{\gcd(10,2)} = 5$$

Ex $GF(16) = \mathbb{Z}_2(\alpha)$ $\alpha^4+\alpha+1=0$

If $a \in (GF(16)^*)$, $\text{ord}(a)$ div 15

$\Rightarrow$ orders are 1, 3, 5, 15

So if $\text{ord}(a) > 5$, a prim.

(Note: Additively, all non-0 elts have order 2:

$(\alpha^2+1)+(\alpha^2+1)=0$.)

In fact, since GF(16)* is isom to Z_{15}

prim elements in GF(16)* = # of generators of cyclic group Z_{15}
= # of integers in 1..14 that are relatively prime to 15 (Gallian Ch 4)
= phi(15) (Euler phi function)
= phi(3)phi(5) = 8.

S'pose β prim in $GF(16)^*$

$\mathrm{ord}(\beta) = 15$

$\mathrm{ord}(\beta^5) = \frac{15}{5} = 3$

$GF(4) = \mathbb{Z}_2(\beta^5) = \{0, 1, \beta^5, \beta^{10}\}$ zeros of $x^4 - x$

$\mathbb{Z}_2(\beta) = GF(16)$

$\mathbb{Z}_2(\beta^5) = GF(4)$

prim order 3 $\rightarrow$ $GF(4)$

$GF(2)$

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 $GF(5^{12})$. $e = 12$

Divs of 12:

$$\begin{tikzcd}[column sep=small]
 & 12 \arrow[dl, dash] \arrow[dr, dash] & \\
6 \arrow[d, dash] \arrow[dr, dash] & & 4 \arrow[d, dash] \\
3 \arrow[dr, dash] & & 2 \arrow[dl, dash] \\
 & 1 &
\end{tikzcd}$$

$F(\alpha) = GF(5^{12}) = E$

$$\begin{tikzcd}[column sep=small]
 & GF(5^{12}) \arrow[dl, dash] \arrow[dr, dash] & \\
GF(5^6) \arrow[d, dash] \arrow[dr, dash] & & GF(5^4) \arrow[d, dash] \\
GF(5^3) \arrow[dr, dash] & & GF(25) \arrow[dl, dash] \\
 & GF(5) \cong \mathbb{Z}_5 &
\end{tikzcd}$$

s.f. of $x^{25} - x$ in E

For each such q', subfield GF(q') will be the splitting field of x^{q'}-x in GF(q).

Why is the magic poly $x^q - x$?

Ans In $GF(q)$:

Every non-zero elt a sats

$a^{q-1} = 1$ (Lagrange)

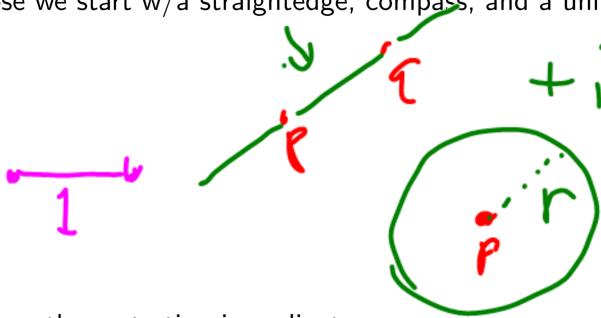
$\forall a \neq 0$, a root of $x^{q-1} - 1 = 0$

$\forall a \in GF(q)$ a root of $x(x^{q-1} - 1) = 0$

$x^q - x$

Ruler-and-compass constructions

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



+ intersections

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? (which lengths?)

Classical problems include:

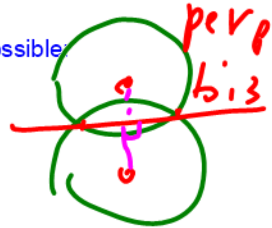
* Can we construct a square with the same area as a given circle?

* Can you produce a procedure that will trisect *any* angle?

(Note: You can trisect some angles, like 90 degrees, but can you trisect *any* angle?)

Field theory shows that the above operations are impossible.

Specifically, you can't construct a square of area pi,
and you can't construct an angle of 20 degrees. (!!!!)



Q: Can you get arbitrarily close to trisection?
A: Yes, by using the binary digits of 1/3 and angle bisections.

angle (Geogebra)
bisection

Constructible fields

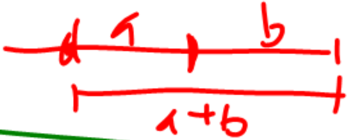
Call $\alpha \in \mathbf{R}$ **constructible** if we can construct a segment of length α. Then

Theorem

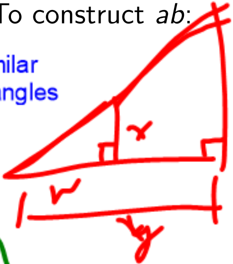
The set of constructible numbers F is closed under $+$, $-$, $\times$, and reciprocals; i.e., F is a subfield of $\mathbf{R}$.

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

$a+b$

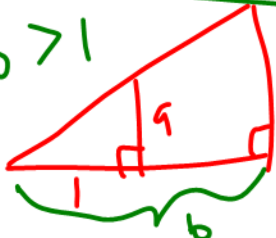


similar triangles



$\dfrac{x}{w} = \dfrac{z}{y}$

$b > 1$

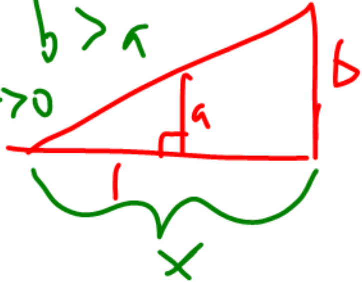


$\dfrac{x}{b} = \dfrac{a}{1}$

$x = ab$

$b > a$

$a > 0$



$$\frac{b}{x} = \frac{a}{1}$$

$$ax = b \qquad x = \frac{b}{a}$$

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.

Review: Permutations

- In cyclic notation, permutation written as product of **cycles**: $(a\ b\ c\ \ldots\ z)$ means a goes to b goes to c goes to... goes to z goes back to a.
- If permutation written as a product of disjoint cycles, order is LCM of cycle lengths.

Examples: α, β, α^{-1}, $\alpha\beta$, orders.

Review: Even and odd permutations

Recall:

- Every permutation is a product of 2-cycles (maybe not disjoint), in many different ways.
- But for a given α, products are either all an even number of 2-cycles or an odd number of 2-cycles. Always even means α is **even**, always odd means α is odd.
- Cycles of odd length are even permutations and cycles of even length are odd permutations.
- So a permutation in disjoint cycle form is even iff it has an even number of even cycles.

Examples:

Permutation groups

Definition

S_n is the group of all permutations on n objects.
A_n is the subgroup of S_n consisting of all **even** permutations on n objects.
A **permutation group** on n objects is a subgroup of S_n.

Definition

To say that a permutation group G on n objects is **transitive** means that for any $a, b \in \{1, \ldots, n\}$, there is some $\alpha \in G$ such that $\alpha(a) = b$. ("You can always get here from there.")

S_4, A_4, D_4, C_4, V_4

Types of elements, numbers of elements of each type.