Math 128B, Mon Apr 26

- 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 and Wed: Review Chs. 1, 4, 5, 7, 9, 10. (S_n, A_n, D_n, $C_n \approx \mathbf{Z}_n$); new reading pp. 387–388. (Ch. 24)
- PS09 due Wed night.
- Exam 3 in one week, Mon May 03.
- Exam review Fri Apr 30, 10am–noon.

Extra office hour today, 1-2pm

Exam 3: Chs 20-23
PS07, PS08, PS09
Sample exam and study guide posted tonight.

PS09 #3(a) $\to E = \mathbb{Z}_5[x]/\langle f(x)\rangle$, $\deg f = 3$

$E = GF(125) = GF(5^3)$

$\alpha \in E^*$, α not zero of $x^5 - x$

$\to$ Prove $E = \mathbb{Z}_5(\alpha)$

Q: What are the possible subfields of E?

(b) $\mathrm{ord}(\alpha)$ div $|E^*| = 124$

Could $\mathrm{ord}(\alpha) = 1$?

No! Only elt ord 1 is 1, $\alpha \neq 1$

Could $\text{ord}(\alpha) = 2$?

If $\text{ord}(\alpha) = 2$

$\Rightarrow \boxed{\alpha^2 = 1}$ No:

Solve $x^2 = 1$ $x^2 - 1 = 0$

$(x+1)(x-1) = 0 \Rightarrow x = \pm 1$

$x = 1$ or 4

Recap: Constructible numbers

Suppose we start w/a straightedge, compass, and a unit length, and from those starting ingredients, we can:

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

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 $\mathbf{R}$.

Square root extensions are possible

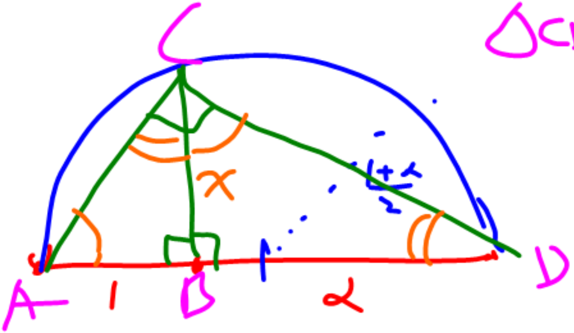
$\boxed{\text{Ex. 3}}$

Theorem

F is closed under taking square roots.

$\triangle ABC$ sim to $\triangle CBD$

Pf



So $\frac{1}{x} = \frac{x}{\alpha} \Rightarrow x = \sqrt{\alpha}$.

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 $\mathbf{Q} \subseteq \mathbf{Q}(a) \subseteq F_n$:

$$2^t \left(\begin{array}{c} F_n \\ | \\ \mathbb{Q}(a) \\ |\, n \\ \mathbb{Q} \end{array} \right.$$

So n divides 2^t.

$\Rightarrow$ E.g. $[\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] = 3$. So $a \neq \sqrt[3]{7}$ not constructible.

A specific non-constructible angle

Let $\theta = \dfrac{2\pi}{18} = 20^\circ$. 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.

over $\mathbb{Q}$

Cor: The angle 60° is not trisectable, so no general trisection algorithm can possibly exist.

End fields
(for now...)

Review (Ch. 5): 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: (Randomly generated by Maple!) α, β, α^{-1}, $\alpha\beta$, orders.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 8 & 9 & 5 & 1 & 7 & 2 & 10 & 4 & 6 \end{pmatrix}$$

e.g. $\alpha(3)=9$

$\alpha(7)=2$

$$\alpha = (1\ 3\ 9\ 4\ 5)(2\ 8\ 10\ 6\ 7)$$

$\mathrm{ord}(\alpha) = 5$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 7 & 2 & 4 & 10 & 1 & 5 & 9 & 3 & 8 \end{pmatrix}$$

$$\beta = (1\ 6)(2\ 7\ 5\ 10\ 8\ 9\ 3)(4)$$

$\text{ord}(\beta) = 14$

$\alpha\beta = \beta$ first, then α $(\alpha \circ \beta)$

$$= (1\ 7)(2)(3\ 8\ 4\ 5\ 6)(9)(10)$$

$$= (1\ 7)(3\ 8\ 4\ 5\ 6)$$

$\text{ord}(\alpha\beta) = 10$

$$\alpha^{-1} = (5\ 4\ 9\ 3\ 1)(7\ 6\ 10\ 8\ 2)$$

$\alpha^{-1} = (1\ 5\ 4\ 9\ 3)(2\ 7\ 6\ 10\ 8)$

ord 5

Review (Ch. 5): Even and odd permutations

Recall:

- Every permutation is a product of 2-cycles (maybe not disjoint), in many different ways.

that are $= \alpha$

- 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.

$\boxed{S_{10}}$

Examples:

5 even 5 even

in A_{10} $\alpha = (1\ 3\ 9\ 4\ 5)(2\ 8\ 10\ 6\ 7)$ even perm

2nd

not in A $\beta = (1\ 6)(2\ 7\ 8\ 10\ 5\ 9\ 3)$ odd perm

7 even

in A_{10} $\alpha\beta = (1\ 7)(3\ 8\ 4\ 5\ 6)$ odd perm

Review (Ch. 5): 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.

E.g.: S_n, A_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.")

E.g.: S_n, A_n $(n \geq 3)$

To prove that the quintic is unsolvable:

- Need to understand transitive permutation groups on 4 and 5 objects.
- Need to understand (all) subgroups of those groups, especially normal vs. non-normal subgroups.

$\boxed{\text{Lagrange}}$

Conjugacy (Ch. 24, new)

Definition

G a group. To say that $a \in G$ is **conjugate** to $b \in G$ means that there exists some $g \in G$ such that $gag^{-1} = b$. The **conjugacy class** of $a \in G$ is the set of all elements of G conjugate to a, i.e.,

$$\left\{ gag^{-1} \mid g \in G \right\}.$$

Ch. 9

Note that a subgroup is **normal** exactly when it is also closed under ~~conjugacy~~. conjugation.

Example: $a \in S_6$, random examples of $g \in S_6$:

$$a = (1\,2\,3\,5)(4\,6)$$

$$g = (2\,3\,5)$$

$$gag^{-1} = (2\,3\,5) \cdot (1\,2\,3\,5)(4\,6) \cdot (2\,5\,3)$$

$$= (1\,3\,5\,2)(4\,6)$$

Note: gag^{-1} has the same cycle-shape as a

S_4 (Ch. 5)

Shapes of elements, numbers of elements of each type.

A_4 (Ch. 5)

Shapes of elements, numbers of elements of each type.

D_4, C_4, and $V \approx C_2 \oplus C_2$ (Chs. 1, 4)

$S_3 \approx D_3$ (Chs. 1, 5) and $C_3 \approx A_3$ (Chs. 4, 5)

Shapes of elements, numbers of elements of each type.