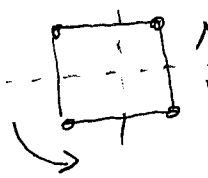
Math 500: Abstract Algebra.

Welcome: (go over syllabus at end, mention HW1 due date now.)

Course divided into 3 parts:

Groups: $\mathbb{Z}/n\mathbb{Z}$, S_n, $GL_3\mathbb{F}_2$, ... [Usually finite]

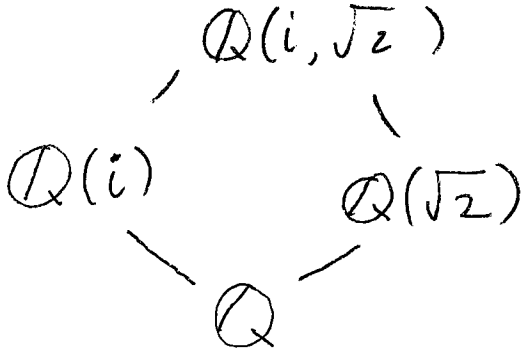
and their actions: D_4  - S_n on $\{1,\dots,n\}$

Rings and **Modules** $\mathbb{Z}$, $\mathbb{Z}[i]$, ... $5 = (2+i)(2-i)$

[like vector spaces over rings rather than just fields]

Fields and Galois Theory

[Origin of group theory.]



Today: Review of basic group theory.

Def: A group is a set G with a binary operation $(x,y) \longmapsto x \cdot y$ that is

1. Associative: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, z \in G$.
2. Identity: there is $e \in G$ such that $e \cdot x = x = x \cdot e$ for all $x \in G$
3. Inverses: for all $x \in G$, there exists $y \in G$ with $x \cdot y = y \cdot x = e$.

[Many variants: monoids sat ① and ②, $e = 1, \ldots$]

Key examples:

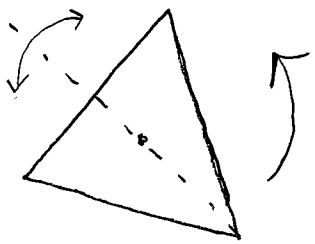
Finite cyclic groups: $C_n = \mathbb{Z}_n = \{e, a, a^2, \ldots, a^{n-1}\}$ [DF]

where $a^i \cdot a^j = a^{(i+j) \bmod n}$.

$(\mathbb{Z}/n, +)$: $\{0, 1, \ldots, n-1\}$

commutative/abelian: $x + y = y + x \quad \forall x, y \in G$

D_{2n}: Symmetry group of regular n-gon



$|D_{2n}| = 2n$

↑ # of elts, called the order.

Symetric groups, e.g. S_n = all permutations of $\{1, 2, \dots, n\}$

$GL_n \mathbb{F}$ = invert. $n \times n$ matrices with entries in a field $\mathbb{F}$.

Subgroups: $H \subseteq G$ where
① $e \in H$
② $x \in H \Rightarrow x^{-1} \in H$
③ $x, y \in H \Rightarrow x \cdot y \in H$.

Write $H \leq G$. [Same as saying that H is itself a group with the rest. binary op.]

Ex: $SL_n \mathbb{F} = \{ A \in GL_n \mathbb{F} \mid \det A = 1 \}$

Ex: Given $S \subseteq G$, set

$$\langle S \rangle = \bigcap_{\substack{H \leq G \\ S \subseteq H}} H = \{ g_1 \circ g_2 \cdots \circ g_k \mid g_i \in S \text{ or } g_i^{-1} \in S \}$$

Suppose $G = C_{10}$ with gen $\langle a \rangle$. Then

$|\langle a^2 \rangle| = 5$ and $|\langle a^5 \rangle| = 2$

A left-coset of $H \leq G$ is any subset of the form $xH = \{xh \mid h \in H\}$

These partition G into pairwise disjoint sets, with $xH = yH \iff x^{-1}y \in H$. Then G/H is the set of left-cosets, and the index $[G:H]$ is $|G/H| \in \mathbb{Z}_{>0} \cup \{\infty\}$.

[Lagrange] For $H \leq G$ with G finite, both $|H|$ and $[G:H]$ divide $|G|$.

Pf: All left-cosets have the same size (e.g. $H \to xH$ sending $h \mapsto xh$ is a bijection), namely $|H|$. So $|G| = [G:H] \cdot |H|$. □

The order $|g|$ of g is $|\langle g \rangle| \in \mathbb{Z}_{>0} \cup \{\infty\}$

Cor: $|g|$ divides $|G|$ when $|G| < \infty$.

Go over syllabus!