

2. E.g. A field is an abelian group $(F, +)$ with additive identity $0 \in F$ such that

- $F^* = F \setminus \{0\}$ is an abelian group (F^*, \cdot) and
- multiplication \cdot distributes over addition $+$: $a \cdot (b+c) = a \cdot b + a \cdot c$.

E.g. $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_2 = \{0, 1\}, \mathbb{F}_3 = \{-1, 0, 1\}, \mathbb{F}_p = \{0, 1, \dots, p-1\}$ for $p \in \mathbb{Z}$ prime
 $\mathbb{R}(i), \mathbb{Q}(i) \quad \mathbb{Z}?$ What is $\mathbb{Z} \setminus \{0\}$? under \times ? monoid (commutative)

Note: Math 221 works verbatim with any F in place of \mathbb{R} ,
except for notions of length, angle, order ($a < b$)
↓
closeness (topology)

E.g. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Is it a field? Use:

Def: A subgroup of a group G is a subset $H \subseteq G$ that is

- closed under composition: $a, b \in H \Rightarrow ab \in H$
 - closed under inversion: $a \in H \Rightarrow a^{-1} \in H$
- notation: $H < G$

Lemma: $H < G$ is a group with same identity as G .

Pf: Associativity is for free: $(ab)c = a(bc)$ in H because it is so in G .

inversion $\Rightarrow a^{-1}a = e \in H$. \square

E.g. $\mathbb{Q}[\sqrt{2}] < \mathbb{C}$ closed under $+$ and $-$ because it is a \mathbb{Q} -vector subspace

• because $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2}$

$(-)^{-1}$ because $\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}$

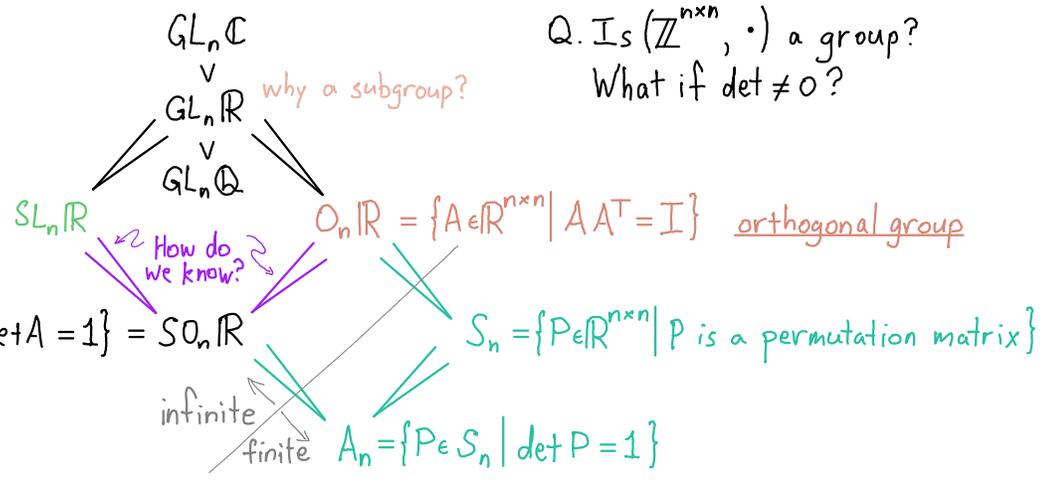
E.g. general linear group $GL_n F = \{A \in F^{n \times n} \mid \det A \neq 0\} = (F^{n \times n})^*$ # since $a, b \in \mathbb{Q}$!

Q. Is $(\mathbb{Z}^{n \times n}, \cdot)$ a group?
What if $\det \neq 0$?

special linear group
 $SL_n F = \{A \in F^{n \times n} \mid \det A = 1\}$

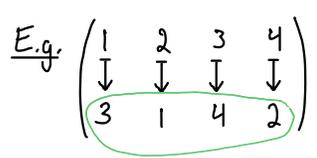
Exercise: $H_1, H_2 \leq G$
 $\Rightarrow H_1 \cap H_2 < G$.

$\{A \in \mathbb{R}^{n \times n} \mid AA^T = I \text{ and } \det A = 1\} = SO_n \mathbb{R}$



infinite \leftarrow $A_n = \{P \in S_n \mid \det P = 1\}$
finite \leftarrow

Def: A permutation of a set X is a bijection $\pi: X \rightarrow X$. The symmetric group is

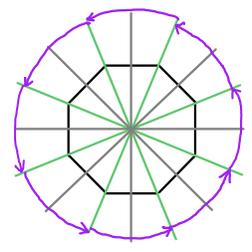
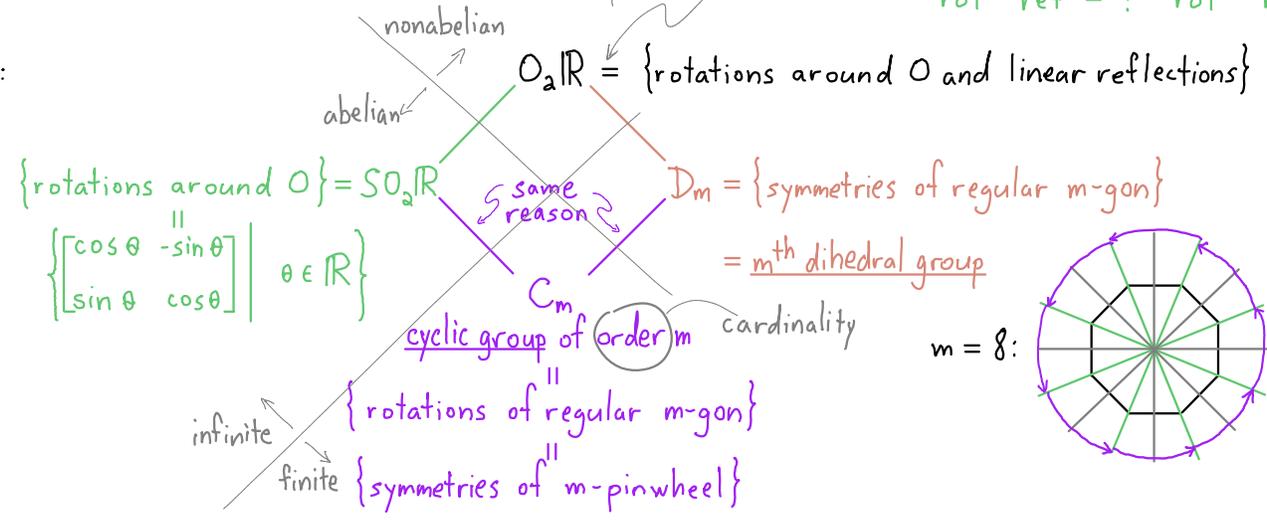


$3142 \leftrightarrow \begin{bmatrix} & & & \\ & & & \\ 1 & & & \\ & & & 1 \end{bmatrix} \in S_4$

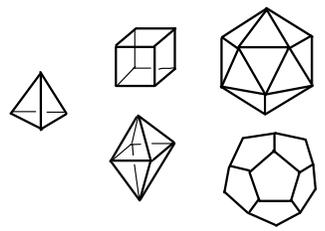
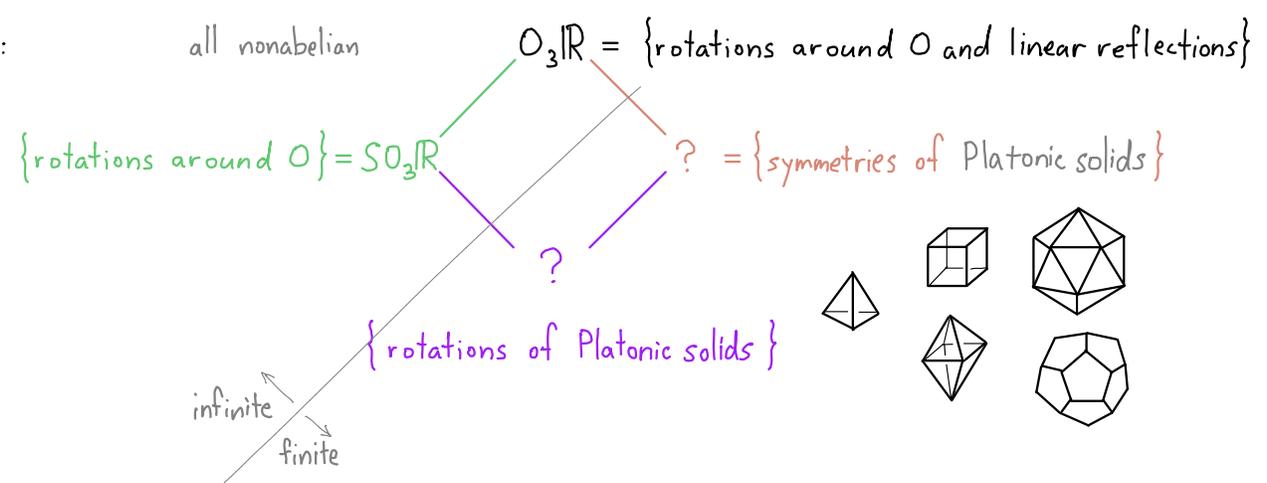
$S_n = \{\text{permutations of } \{1, \dots, n\}\}$

not obvious! $\text{ref} \circ \text{rot} = ?$ $\text{ref} \circ \text{ref} = ?$
 $\text{rot} \circ \text{ref} = ?$ $\text{rot} \circ \text{rot} = ?$

$n=2$:



$n=3$:



E.g. $(\mathbb{C}, +) > (\mathbb{R}, +) > (\mathbb{Q}, +) > (\mathbb{Z}, +) > (d\mathbb{Z}, +)$

e.g. $2\mathbb{Z} = \text{even integers}$

all abelian, all infinite

E.g. $\mathbb{C}^* > \mathbb{R}^* > \mathbb{Q}^* > \mathbb{Z}^*$ all abelian
 infinite | finite