1 4/10/2024 lecture

1.1 Quotient groups

Example 1.1. $SO(n)$ is a normal subgroup of $O(n)$, so we can define the quotient group $O(n)/SO(n)$, which is isomorphic to $C_2 := \langle x | \, x^2 = e \rangle \cong \{\pm 1\}^\times$.

Let $n\mathbb{Z}$ be the subgroup $\{nm : m \in \mathbb{Z}\}$. Since $\mathbb{Z}$ is an additive group, be sure not to confuse $n\mathbb{Z}$ with the coset $n + \mathbb{Z}$. We know that $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$ – it's easy to prove that every subgroup of an abelian group is normal.

Now we can define the *group of integers modulo n* to be $\mathbb{Z}/n\mathbb{Z}$. Some people write this as $\mathbb{Z}_n$, because that's shorter.

Theorem 1.2. For any $N \in \mathbb{N}$, the cyclic group $C_n := \langle x | \, x^n = e \rangle$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Therefore, we can use C_n and $\mathbb{Z}_n$ interchangeably.

Proof. Let $\varphi : C_n \to \mathbb{Z}/n\mathbb{Z}$ be the homomorphism which maps x to the coset $1 + n\mathbb{Z}$ (and thus, also maps x^m to $m + n\mathbb{Z}$). You can easily shows that φ is an injective and surjective homomorphism. $\square$

1.2 Exact sequences and extensions

A path in a commutative diagram is called an *exact sequence* iff the kernel of each morphism (except the first one) is equal to the image of the previous one. Right now, we only care about the category **Grp**, in which morphisms are group homomorphism. For example, if $H \trianglelefteq G$, then

$$0 \hookrightarrow H \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} G/H \twoheadrightarrow 0$$

is an exact sequence because $\ker \pi = \operatorname{im} i$.

A group G is called an *extension of Q by K* iff there is an exact sequence

$$0 \hookrightarrow K \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q \twoheadrightarrow 0.$$

Example 1.3. The *Klein 4-group* $K_4 := \mathbb{Z}_2 \times \mathbb{Z}_2$ and the group $\mathbb{Z}_4$ are distinct extensions of $\mathbb{Z}_2$ by $\mathbb{Z}_2$.

1.3 Conjugacy classes

Two elements $g_1, g_2 \in G$ are called *conjugate* iff there exists some $h \in G$ such that $hg_1h^{-1} = g_2$. Conjugacy is an equaivalence relation, and the equivalence classes of that relation are called the *conjugacy classes.* The conjugacy class of $g \in G$ is written as

$$C(g) := \{h \in G : \; h \text{ and } g \text{ are conjugate}\}.$$

For matrices, conjugacy is the same as similarity, meaning two matrices are conjugate iff they represent the same linear transformation in different bases.

Since every permutation $\sigma \in S_n$, σ can be written as the product of disjoint cycles (by lemma **??** WHY IS THIS NUMBER OFF?), we can define the *cycle type* of a permutation to be the multiset of the lengths of those cycles (CHECK THAT THIS IS UNIQUELY DEFINED).

Theorem 1.4. The conjugacy class of some permutation $\sigma \in S_n$ is the set of permutations in S_n with the same cycle type as σ.

Proof. By **??**. FINISH THIS PROOF. $\square$

Problem 1.5. How many conjugacy classes does S_n have? If this is too hard, just consider the $n = 4$ case.

Any permutation which is conjugate to $\sigma \in S_n$ must have the same number of 1-cycles as σ, the same number of 2-cycles, etc. Therefore each conjugacy class of S_n can be uniquely determined by a partition of n of the form $n = a_1 + a_2 + \cdots + a_m$, where $a_1 > a_2 > \cdots > a_m$. So if $n = 4$, there are 5 conjugacy classes of S_n:

- $4 = 4$
- $4 = 3 + 1$
- $4 = 2 + 2$
- $4 = 2 + 1 + 1$
- $4 = 1 + 1 + 1 + 1$

IS THERE A GENERAL FORMULA FOR THE NUMBER OF CONJUGACY CLASSES OF THE SYMMETRIC GROUP

1.4 The alternating group

The *sign of a permutation* is 1 if it can be written as a product of an even number of permutations, and -1 otherwise.

Let *the permutation matrix* $P(\sigma)$ of some permutation $\sigma \in S_n$ be the orthogonal matrix which permutes the basis vectors $e_i \in \mathbb{R}^n$. Then we can define the sign of σ to be $\det(P(\sigma))$. Note that the sign of any transposition is -1.

$$S_n \overset{P}{\hookrightarrow} O(n) \overset{\det}{\twoheadrightarrow} \mathbb{Z}_2.$$

Now we can define *the alternating group* A_n to be the kernel of $\det \circ P$. By Lagrange's theorem (CITE THAT), $|A_n| = n!/2$.

Proposition 1.6. For $n \geq 5$, A_5 is simple. In fact, every group of order less than 60 is *solvable.* This is not really relevant to us, but in Galois theory, this is used to prove the Abel-Ruffini theorem.

TO PROVE THAT A_5 IS SIMPLE, FIND THE SIZES OF ALL CONJUGACY CLASSES SINCE EVERY SUBGROUP OF A_5 CONTAINS EITHER AN ENTIRE CONJUGACY CLASS OF ITS ELEMENTS, THE SIZE OF ANY SUBGROUP OF A_5 IS THE SUM OF SOME SUBSET OF $(1, 15, 20, 12, 12)$ BUT THAT SUM CAN ONLY DIVIDE 60 IF IT IS EITHER 1 OR 60.

ALSO TALK ABOUT THE SYLOW THEOREMS