MATH 3311, FALL 2025: LECTURE 22, OCTOBER 20

Video: `https://youtu.be/bMa9RnSdKAk`

Again, we will fix a finite group G and a prime p. Let $m \geq 0$ be the integer such that p^m is the largest power of p dividing the order $|G|$.

Let's recap:

Theorem 1 (Sylow Theorem A)**.** *There exists a subgroup $Q \leq G$ of order $|Q| = p^m$. That is, $\mathrm{Syl}_p(G)$ is non-empty.*

Theorem 2 (Sylow Theorem B)**.** *The conjugation action of G on $\mathrm{Syl}_p(G)$ is* transitive*. That is, if $P, Q \in \mathrm{Syl}_p(G)$ are two Sylow p-subgroups of G, then there exists $g \in G$ such that $gPg^{-1} = Q$.*

Theorem 3 (Sylow Theorem C)**.** *Let $n_p = |\mathrm{Syl}_p(G)|$ be the number of Sylow p-subgroups of G.*

(1) $n_p = [G : N_G(P)]$ and $n_p \mid [G : P]$ for any $P \in \mathrm{Syl}_p(G)$.

(2) $n_p \equiv 1 \pmod{p}$.

The Sylow theorems in particular give us *non-trivial* actions of finite groups on their sets of Sylow p-subgroups for every prime p dividing the order of the group.

Example 1. Suppose that $|G| = 48 = 2^4 \cdot 3$. Then $n_2 \equiv 1 \pmod{2}$ is odd and $n_2 \mid 3$. So the only possibilities are $n_2 = 1, 3$. If $n_2 = 1$, then there is exactly one Sylow 2-subgroup (of order 16), which is normal. If $n_2 = 3$, then we have three such subgroups. But we can still obtain some more information about G by now looking at the action $G \curvearrowright \mathrm{Syl}_2(G)$, which gives a *non-trivial* group homomorphism $\rho : G \to S_3$.

But note that by the first isomorphism theorem (or really the factoring triangle) we have

$$48/|\ker \rho| = |G|/|\ker \rho| = |\mathrm{im}\ \rho|,$$

where the right hand side is a divisor of $|S_3| = 6$ (why?). Since the homomorphism is non-trivial, the only options for such a divisor are $2, 3, 6$, corresponding to the cases where $|\ker \rho| = 24, 16, 8$[1]. Since $\ker \rho$ is normal, we obtain a *non-trivial, proper* normal subgroup of G.

So whether $n_2 = 1$ or $n_2 = 3$, we will always have a non-trivial proper normal subgroup of G, and so no group of order 48 can be simple.

The sign homomorphism and the alternating group

So far the only examples of finite simple groups we have encountered are the cyclic groups $\mathbb{Z}/p\mathbb{Z}$ of prime order, which are precisely the *abelian* finite simple groups (Homework 7). We haven't seen any examples of *non-abelian, finite simple* groups. Such examples will be provided by the *alternating groups*, which are index 2 subgroups $A_n \leq S_n$ that are simple when $n \geq 5$.

Defining such an index 2 subgroup is equivalent to writing down a surjective homomorphism $S_n \to \{\pm 1\}$, where the right hand side side is the group of order 2 viewed in a multiplicative way: $(-1) \cdot (-1) = 1$.

I will first give a definition of such a homomorphism that requires some stuff from linear algebra that you're not assumed to know about:

- First, given a permutation $\sigma \in S_n$, we can build an $n \times n$ *matrix* $A(\sigma) \in M_n(\mathbb{Z})$ with integer coefficients as follows: Its (i, j)-th entry[2] is 1 if $i = \sigma(j)$ and is 0 otherwise. This is the matrix of the linear transformation that permutes the basis vectors by permuting their indices via σ.

[1] The order actually cannot be 16, since then it would be a 2-Sylow subgroup, and we know that no 2-Sylow subgroup is normal under our assumptions.

[2] This means the i-th row and j-th column

- For instance, if $n = 2$ and σ is the permutation that flips 1 with 2, then $A(\sigma)$ is the 2×2-matrix
$$A(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
- If $n = 3$ and σ is the cyclic permutation $1 \mapsto 2 \mapsto 3 \mapsto 1$, then we have
$$A(\sigma) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$
- Now, one checks that for $\sigma_1, \sigma_2 \in S_n$, we have
$$A(\sigma_1 \circ \sigma_2) = A(\sigma_1)A(\sigma_2)$$
where the right hand side is *matrix multiplicaiton*: This comes down to the fact that composition of linear transformations corresponds to multiplication of matrices.
- Next, one considers the *determinant* $\det(A(\sigma))$: A general property of the determinant is that $\det(AB) = \det(A)\det(B)$ forr two $n \times n$-matrices A and B.
- Therefore, we find that the function
$$\begin{aligned} \operatorname{sgn} : S_n &\to \{\pm 1\} \\ \sigma &\mapsto \det(A(\sigma)) \end{aligned}$$
satisfies $\operatorname{sgn}(\sigma_1 \circ \sigma_2) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$, and so is a homomorphism of groups. Moreover it takes any permutation that simply flips two elements (and keeps everything else fixed) to -1, since the determinant of the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is -1.

Cycle notation

To give a different definition of the sign homomorphism that does not require appealing to properties of matrices, we need to introduce a new way of talking about elements of S_n.

Definition 1. (Cycle notation) Given $m \in \{2, \dots, n\}$, an m**-cycle** $\alpha \in S_n$ is an element written in the form
$$(a_1\ a_2\ \cdots\ a_m),$$
where $a_1, a_2, \dots, a_m \in \{1, 2, \dots, n\}$ are *distinct* elements, and where, as a permutation of $\{1, 2, \dots, n\}$, α behaves as follows:

- It moves the elements $a_1, \dots, a_m$ like so: $\overbrace{a_1 \mapsto a_2 \mapsto \cdots \mapsto a_{m-1} \mapsto a_m \mapsto}$
- It fixes all elements not in the subset $\{a_1, \dots, a_m\}$.

A **cycle** is an element $\alpha \in S_n$ that is an m-cycle for some integer m.

Definition 2. A 2-cycle in S_n will be called a **transposition**.

Theorem 4 (The sign homomorphism)**.** *There is a* unique *surjective homomorphism*
$$\operatorname{sgn} : S_n \to \{\pm 1\}$$
such that $\operatorname{sgn}(\tau) = -1$ *for every transposition* $\tau \in S_n$.

Remark 1. Note that this property holds for the 'definition' given above using the determinant.

Definition 3. The **alternating group** A_n is the index 2 normal subgroup of S_n given by $A_n = \ker \operatorname{sgn}$.