M621, Oct. 13 Class notes: Oct. 14

Fix $n \in \mathbb{N}$, and let $X = \{(i,j) : n \geq i > j \geq 1\}$. Let $\alpha \in S_n$, and let $Fl(\gamma)$ ("flip of γ") be the the pairs (i,j), $n \geq i > j \geq$ such that $\gamma(j) > \gamma(i)$. For example, in S_4, $Fl((13)) = \{(3,1),(2,1),(3,2)\}$, and $Fl((123)) = \{(3,2),(3,1)\}$. For $\alpha \in S_n$, let $fl(\gamma) = |Fl(\alpha)|$, and let $\Gamma(\alpha) = fl(\alpha)_2$, where for all $n \in \mathbb{Z}$, "n_2" means "n *mod* 2". Of course, the map $\mathbb{Z} \to Z_2$ is a homomorphism.

So Γ is a map from S_n to $\{0,1\}$. Observe that with e the identity of S_n, $\Gamma(e) = fl(e)_2 = 0_2 = 0$, and $\Gamma((12)) = fl((12))|_2 = 1_2 = 1$, so Γ is onto. We can regard Γ as a map from S_n to Z_2. We show show that Γ is a homomorphism.

Let $\alpha, \theta \in S_n$, let $fl(\alpha) = j$, let $fl(\theta) = k$, and let $k_1 = |Fl(\theta) \cap Fl(\theta)|$, the number of pairs that are flipped by both θ and α.

Notice that $fl(\theta\alpha) = (k-k_1)+(j-k_1) = k+j-2k_1$. (The left-most equality follows since (i,j) is flipped by $\theta\alpha$ if and only if (i,j) is flipped by θ but not α, or (i,j) is flipped by α but not θ.) So $\Gamma(\theta\alpha) = (k+j-2k_1)_2 = (k+j)_2 = k_2 + j_2 = \Gamma(\theta) + \Gamma(\alpha)$. Thus, Γ is a homomorphism.

Observe that $\Gamma^{-1}(0)$ consists of the even permutations, while $\Gamma^{-1}(1)$ consists of the odd permutations. We let A_n denote the even permutations. Since $A_n = ker(\Gamma)$, we have that A_n is normal in S_n.

Each transposition is an odd permutation: Indeed, with $n \geq i > j \geq 0$, consider (ij), a transposition. Observe that if $\beta \in S_n$ is such that $\beta(1) = i, \beta(2) = j$ (and there are such β), then $\beta(12)\beta(^{-1}(ij)$, and since Γ is a homomorphism, $\Gamma(\beta(12)\beta(^{-1}) = \Gamma(\beta) + \Gamma((12) - \Gamma(\beta) = 1$.

Since Γ is a homomorphism, it follows now that the product of an odd number of transpositions is again odd, and the product of an even number of transpositions is even (that is, in A_n).

We observe that every odd permutation is in the coset $(12)A_n$. Indeed, if ϕ is odd, then $\phi = (12)(12)\phi = (12)((12)\phi) \in (12)A_n$ since $(12)\phi)$ is even. So S_n is the disjoint of the two cosets $A_n \sqcup (12)A_n$, which implies that $|A_n| = \frac{n!}{2}$.

A little more about A_n, left as quick exercises you should do.

1. In their cycle notation, list the elements of S_3; do the same for S_4.
2. If $\alpha \in S_n$, then $\alpha^2 \in A_n$.
3. $\alpha \in A_n$ if and only if $(12)\alpha \notin A_n$.
4. For $n \in \mathbb{N}$, the 2-cycles are not in A_n, the 3-cycles are is in A_n, the 4-cycles are not in A_n, the 5-cycles are in A_n, and so on.
5. Determine the shapes of the elements of S_5 that are A_5.

0.1 Cayley's Theorem

An *embedding* $\Gamma : G \hookrightarrow K$ of a group G into a group K is a one-to-one homomorphism of G into K. Since it's one-to-one, the map from $G \to \Gamma(G)$ is an isomorphism of groups, and $\Gamma(G)$ is a subgroup of K that is isomorphic to G. We say that "G is embedded in K".

Let A be a set. As you know, S_A is the symmetric group on A, the group of permutations of A. Each subgroup of S_A is referred to as a *permutation group.* For example, D_8 is a permutation group since it's a subgroup of D_4.

Theorem. Let G be a group. Then there exists a set A and an embedding $\Gamma : G \to S_A$. Thus every group G is isomorphic to a permutation group. then there exists a set A such that G can be e

Proof. Let G be a group, and for an element $g \in G$, for each $x \in G$, let $\Gamma(g)(x) = gx$. Of course $\Gamma(g)$ is a function, $\Gamma(g) : G \to G$. If x, y are in G, and $\Gamma(g)(x) = \Gamma(g)(y)$, then $gx = gy$, and by left-cancellativity, $x = y$. So $\Gamma(g)$ is one-to-one. If $z \in G$, then $\Gamma(g)(g^{-1}z) = g(g^{-1}z) = z$, so $\Gamma(g)$ is onto. We've shown that for all $g \in G$, $\Gamma(g)$ is a permutation of G. So the map $\Gamma : G \to S_G$ is well-defined. We show Γ is a one-to-one homomorphism of groups. Let g, h be in G. If $\Gamma(g) = \Gamma(h)$, then $g = ge = \Gamma(g)(e) = \Gamma(h)(e) = he = h$, so Γ is one-to-one. Also, for all $x \in G$, $\Gamma(gh)(x) = ghx = g(hx) = \Gamma(g)(hx) = \Gamma(g)\Gamma(h)(x)$. Since x was arbitrarily chosen element of G, we have shown that $\Gamma(gh) = \Gamma(g)\Gamma(h)$, completing the proof.

Above we showed that G is isomorphic to a subgroup of S_G. It was important that any group is isomorphic to a permutation group, but the embedding $G \hookrightarrow S_G$ is pretty much impractical—for example, we could start with a quite small group G having say 12 elements, and embed it into a group S_G having 12! elements. But 12! is over 400 million, so good luck getting interesting specifics concerning G in S_G.

It's more informative if somehow you can find a much smaller n than $|G|$, and embed G into S_n.

Given a finite group G, one of the interesting questions is this: What is the least $n \in \mathbb{N}$ such that $G \hookrightarrow S_n$ (i.e. G embeds in S_n)? If n is really small with respect to $|G|$, the embedding may contain serious information about G. But sometimes you can't do better than $n = |G|$.

Exercise. Show that Z_8 can't be embedded into S_n if $8 > n$.

0.2 Simple groups

A non-trivial group G is *simple* if its only normal subgroups are $\{e\}$ and G.

Example 0.1 *1. $S_2 \cong Z_2$ is simple, but S_3 is not simple since $A_3 = \{e, (123), (132)\}$ is a proper, non-trivial normal subgroup of S_3.*

2. Can we classify the simple Abelian groups?

Observe first that if G is Abelian, then **every** *subgroup of G is normal. So if G is Abelian and simple, since G is non-trivial, there exists $g \neq e$ in G. So $< g >$ is non-trivial, and by simplicity $< g >= G$, and we've shown that in order for G to be Abelian and simple, G is cyclic. We 've classified the cyclic groups up to isomorphism— every cyclic group J is isomorphism to either $\mathbb{Z}$ (if it is infinite) or $\mathbb{Z}_n$, for some $n \in \mathbb{N}$. As we showed, if $k \in \mathbb{N}$, and $k|n$, then there exists a (unique) cyclic subgroup H of J such that $|H||n$. Hence, if $|J|$ is not prime, J is not simple. This leaves the cyclic groups of prime order p, the Z_p's. By Lagrange, Z_p contains no proper, non-trivial subgroup; hence, Z_p is simple. This completes the classification of the simple Abelian groups.*

For non-Abelian groups, even finite non-Abelian groups, it is not so easy to classify the simple ones (a vast understatement—-it took many years, and many thousands of journal pages, to complete the classification). It turns out—and we will prove this— that A_5 is the smallest non-Abelian simple group, and that if $n \geq 5$, then A_n is simple.

If the goal is to classify all finite groups, we have a formidable task—they are beyond any neat, tidy classification. However, for the special case of finite Abelian groups, an M521 result theorem states that every finite Abelian group G is isomorphic to a direct product of cyclic prime-power groups (i.e. groups of the form Z_{p^n}, where p is prime, and $n \in \mathbb{N}$). But the non- Abelian groups are another matter.

But we'll see that the simple finite groups can be used as building blocks of the finite groups, in a way that took group theorists a while to discover, and in a way that provides a "classification" that is more of an "approximation" than a classification: We'll discuss this on Tuesday, when we talk about *composition series* of groups.

Recall that if H is a subgroup of G, then the *index* of H in G, denoted $[G : H]$ is the number of left cosets of H in G. If G is finite, $[G : H] = |G|/|H|$. For example, $[S_n : A_n] = 2$. As we saw, A_n is normal in S_n. If we had known $[S_n : A_n] = 2$, we could have the normality of A_n in S_n in another way:

Classic exercise..maybe you did it in M521: If G is a group, $H \leq G$, and $[G : H] = 2$, then H is normal in G.

Could it be true that $[G : H] = p$, a prime, then that's enough to guarantee that H is normal in G. We've observed that D_8 is an 8-element subgroup of S_4. Since $[S_4 : D_8] = 3$, we'd have to have D_8 is normal in S_4? Is D_8 normal in S_4?