ALGEBRA 245 LECTURE 3

NOTES BY MAX WEINSTEIN

1. Free Groups

If A a set, then $F(A)$ is the free group generated by the elements of S and we get a correspondence between sets and groups.

Example 1.1. The empty set corresponds with the trivial group

$$\varnothing \longleftrightarrow \{1\}$$

and a set with one element corresponds to a group generated by that element (with no relations)

$$\{a\} \longleftrightarrow \langle a \rangle \cong \mathbb{Z}$$

Definition 1.2. Define a category of maps j from the set A to any group G with morphisms σ group homomorphisms that make the diagram commute:

$$\begin{tikzcd} A \arrow[r, "j_1"] \arrow[dr, "j_2"'] & G \arrow[d, "\sigma"] \\ & H \end{tikzcd}$$

$F(A)$ is defined to be the initial object in this category (Like final objects, initial objects are unique up to isomorphism).

Why do Free Groups exist?
A a finite set, A' the formal "inverses" of elements of A, then define $W(A)$ to be the set of words in $A \cup A'$

Example 1.3. $A = \{a, b, c\}$, $A' = \{a^{-1}, b^{-1}, c^{-1}\}$, then $aaab^{-1}bc \in W(A)$

Definition 1.4. $r : W(A) \to W(A)$ takes words in $W(A)$ and removes the first occurrence of ll^{-1} for any letter l, so $r(aaa^{-1}bb^{-1}) = abb^{-1}$, and fully reduced words remain unchanged, i.e. $r(abc) = abc$. The maximum number of iterations of r to reduce a word of length n is $\lfloor \frac{n}{2} \rfloor$, so now we define $R : W(A) \to W(A)$ to be the map taking words w of length n to $r^{\lfloor \frac{n}{2} \rfloor}(w)$, the fully reduced version of w.

In this context, $F(A)$ is defined to be the group $(R(W(A)), \cdot)$ where $w \cdot w' = R(ww')$

Proof that $F(A)$ is a group:
- Associativity: $w \cdot (w' \cdot w'') = R(wR(w'w'')) = R(ww'w'') = R(R(ww')w'') = (w \cdot w') \cdot w''$
- Identity: the empty word
- Inverse: write the anti-word, i.e. $(abba^{-1})^{-1} = ab^{-1}b^{-1}a^{-1}$

Date: January 2024.

We can now finish the diagram:

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[dr, "j"'] & F(A) \arrow[d, "\sigma"] \\ & G \end{tikzcd}$$

where $i(a) = a \in F(A)$ as a word, j any map from the set A to a group G, and σ the unique homomorphism making the diagram commute. $\sigma(a) = j(a)$ and $\sigma(a^{-1}) = j(a)^{-1}$.

2. **Subgroups**

We write $(H, \cdot) < (G, \cdot)$ and say $(H, \cdot)$ is a subgroup of $(G, \cdot)$ if H is a subset of G which is itself a group under the same operation as G, i.e. $i : (H, \cdot) \hookrightarrow (G, \cdot)$ is a homomorphism.

Lemma 2.1. *Let H be a non-empty subset of G, then H is a subgroup iff $\forall a, b \in H$, $ab^{-1} \in H$*

Proof: $\Rightarrow$ If H is a subgroup, then H is a group so $a, b \in H$ implies $b^{-1} \in H$ and $ab^{-1} \in H$

$\Leftarrow$ Suppose $ab^{-1} \in H$ whenever $a, b \in H$, then in particular for $h \in H, hh^{-1} = e \in H$. $e, h \in H$ implies $eh^{-1} = h^{-1} \in H$, and finally if $g, h \in H$, $g(h^{-1})^{-1} = gh \in H$, so H is a group and therefore a subgroup of G

3. **Normal Subgroups**

Definition 3.1. $N < G$ is normal if $\forall h \in N$, and $\forall g \in G$, $ghg^{-1} \in N$. Equivalently, N is normal if $gNg^{-1} = N \quad \forall g \in G$, where $gN = \{gh \mid h \in N\}$.

Definition 3.2. $\phi : G \to H$ is a homomorphism if $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$. The kernel of ϕ is the set $\mathrm{Ker}(\phi) = \{g \in G \mid \phi(g) = e\}$

Lemma 3.3. *$Ker(\phi)$ is a normal subgroup*

Proof: First notice that ϕ is a homomorphism, so $\phi(e) = e$ and $Ker(\phi)$ is always non-empty. Then let $g, h \in Ker(\phi)$, and observe $\phi(gh^{-1}) = \phi(g)\phi(h^{-1}) = e\phi(h)^{-1} = e^{-1} = e$, which means $gh^{-1} \in Ker(\phi)$ and $Ker(\phi)$ is a subgroup by Lemma 2.1.

$\phi(h) = id$ implies $\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)e\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = e$, so $ghg^{-1} \in Ker(\phi)$ whenever h is, hence $Ker(\phi)$ is a normal subgroup.

Theorem 3.4. *All normal subgroups are the kernel of some homomorphism.*

Proof: Let K be a normal subgroup of G, then the left cosets gK partition G since if $h \in g_1K$ and $h \in g_2K$, then $h = g_1k_1 = g_2k_2$ for some $k_1, k_2 \in K$, and then we have $g_2^{-1}g_1 = k_2k_1^{-1} \in K$, which lets us conclude that $g_2K = g_2(k_2k_1^{-1})K = g_2(g_2^{-1}g_1)K = g_1K$.

We then get a well defined operation $gK \cdot hK = ghK$, since if $gK = g'K$, $g' = gk_g$ for *some $k_g \in K$. Then $g'K \cdot hK = gk_ghK$, and since K is normal, $h^{-1}kh = k' \in K$ for all $k \in K$ and for some $k' \in K$, hence $gk_ghK = ghk'_gK = ghK$ and the operation is well defined.*

Call this new group of left cosets G/K, and take the quotient map $\pi : G \to G/K$ which takes $g \to gK$. This map is a homomorphism and $Ker(\pi) = K$

Corollary 3.5. *If $\phi : G \to G'$ is onto, then $G/Ker(\phi) \cong G'$*

4. LaGrange's Theorem

Definition 4.1. If $H < G$ is a subgroup, then $[G : H]$ = the number of left cosets = index of H in G

Theorem 4.2 (LaGrange)**.** $|G| = [G : H]|H|$

Corollary 4.3. *The order of a subgroup of G divides the order of G*

5. Group Actions

The action of a group G on a set A is a homomorphism:

$$\sigma : G \to \text{Aut}(A)$$

Definition 5.1. Alternatively, we define a (left) action as a map $\rho : G \times A \to A$ such that:

1) $\rho(e, a) = a$
2) $\rho(gh, a) = \rho(g, \rho(h, a))$

Why are group actions so great?

Every group acts *faithfully* on some set, i.e. $ga = a\ \forall a \in A$ implies $g = e$. Therefore every group is a subgroup of a permuation group.