Abstract algebra - Exercise session 6

Cayley's theorem. Every group is isomorphic to a subgroup of a symmetric group. If $|G|=n$, G is isomorphic to a subgroup of n.

Proof. Recall that the action of G on itself by left multiplication defines a homomorphism

$$\phi : G \to S_G$$
$$g \mapsto \sigma_g$$

where $\sigma_g(h) = gh$.

We prove that ϕ is injective. If $g \in \ker\phi$ we have

$$\sigma_g = id : G \to G$$

so $h = \sigma_g(h) = gh$ for all $h \in G$.

$\Rightarrow$ $g = 1$. Thus $\ker\phi = \{1\}$, so ϕ is injective.

$\Rightarrow$ $G \cong \operatorname{im}\phi \leq S_G$.

If $|G| = n$ we have

$$S_G \cong S_n,$$

by labeling the elements of G from 1 to n. ■

3.5.3. Prove that S_n is generated by

$$\{(i \ \ i+1) \mid 1 \le i \le n-1\}.$$
$$\parallel$$

Solution. Let S. Suppose $(i \ \ i+k) \in \langle S \rangle$ for some $k \geq 1$. Then

$$(i+k \ \ i+k+1)(i \ \ i+k)(i+k \ \ i+k+1)$$

$$=(i \ \ i+k+1)$$

Since $(i \ \ i+1) \in \langle S \rangle$ for all $1 \le i \le n-1$ it follows by induction that

$$(i \ \ i+k) \in \langle S \rangle$$

for all $1 \le i \le n-1$ and $1 \le k \le n-i$.

All transpositions are of this form, so since

$$\langle \{\text{transpositions in } S_n\} \rangle = S_n,$$

we are finished.

4.1.9. Assume G acts transitively on a finite set A and let $H \trianglelefteq G$. Let $\mathcal{O}_1, \dots, \mathcal{O}_r$ be the distinct orbits of H on A.

(a) • Prove that G permutes $\{\mathcal{O}_1, \dots, \mathcal{O}_r\}$, in the sense that for each $g \in G$ and each i there is a j such that $g\mathcal{O}_i = \mathcal{O}_j$.
• Prove that G acts transitively on $\{\mathcal{O}_1, \dots, \mathcal{O}_r\}$.
• Deduce that all orbits of H on A have the same cardinality.

Solution. • Let $a \in A$ and let $\mathcal{O}_i := H \cdot a$. Then

$$g Ha = \{gha \mid h \in H\} = \{ghg^{-1}ga \mid h \in H\}$$
$$\overset{gHg^{-1}=H}{=} \{hga \mid h \in H\}$$
$$= H \cdot (ga),$$

which is also an orbit, i.e. $H(ga) = \mathcal{O}_j$ for some j.

• Let $a, b \in A$ and $\mathcal{O}_i := Ha$, $\mathcal{O}_j := Hb$.

Since G acts transitively on A, there is a $g \in G$ s.t. $ga = b$. Thus

$$g\mathcal{O}_i = g(Ha) = H(ga) = Hb = \mathcal{O}_j$$

so G acts transitively on $\{\mathcal{O}_1, \dots, \mathcal{O}_r\}$.

- Let $\mathcal{O}_i$ and $\mathcal{O}_j$ be two orbits and $g \in G$ s.t. $g\mathcal{O}_i = \mathcal{O}_j$, i.e.

$$g\mathcal{O}_i = \{gx \mid x \in \mathcal{O}_i\} = \mathcal{O}_j.$$

In other words, $\varphi : \mathcal{O}_i \to \mathcal{O}_j$, $x \mapsto gx$ is a surjection. But we also have

$$g^{-1}\mathcal{O}_j = g^{-1}g\mathcal{O}_i = \mathcal{O}_i,$$

so $\varphi' : \mathcal{O}_j \to \mathcal{O}_i$, $x \mapsto g^{-1}x$ is also a surjection.

Since A is finite, it follows that the sets $\mathcal{O}_i$ and $\mathcal{O}_j$ have the same cardinality.

(b) Prove that if $a \in \mathcal{O}_1$ then

$$|\mathcal{O}_1| = |H : H \cap G_a|$$

and $r = |G : HG_a|$

Solution: We have $\mathcal{O}_1 = Ha$. Note that

$$H_a = \{h \in H \mid ha = a\}$$

$$= H \cap \{g \in G \mid ga = a\}$$

$$= H \cap G_a$$

The orbit-stabilizer thm thus implies

$$|Ha| = |H : H_a| = |H : H \cap G_a|.$$

Since the action of G on

$$\{\mathcal{O}_1, \dots, \mathcal{O}_r\} = \{Ha \mid a \in A\}$$

is transitive, we only have one orbit, so

$$r = |G \cdot Ha| = [G : G_{Ha}]$$

We want to show that $G_{Ha} = HG_a$.

Suppose that $g \in G_{Ha}$, i.e.

$$gHa = Ha$$

Since $1 \in H$ we have in particular

$$ga = ha$$

for some $h \in H \Rightarrow h^{-1} g a = a$, so $h^{-1} g \in G_a$. Thus

$$g = h h^{-1} g \in H G_a.$$

$$\Rightarrow \quad G_{Ha} \subseteq H G_a.$$

Now suppose $g \in H G_a$, so $g = hx$ for some $h \in H$, $x \in G_a$. Thus

$$\begin{aligned} gHa &= (gH)a \\ &\overset{H \text{ normal}}{=} (Hg)a \\ &= Hhxa \\ &\overset{H \text{ subgp}}{=} Hxa \\ &\overset{x \in G_a}{=} Ha, \end{aligned}$$

so $g \in G_{Ha} \Rightarrow H G_a \subseteq G_{Ha}$. ∎

Free groups.

Let S be a set, S^{-1} another set and $f : S \to S^{-1}$ a bijection. We write

$$s^{-1} := f(s) \qquad \text{for } s \in S.$$

Let

$$F_S := \left\{ s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k} \;\middle|\; \begin{array}{l} s_1, \dots, s_k \in S \\ \epsilon_1, \dots, \epsilon_k \in \{-1, 1\} \end{array} \right\} \Big/ \sim$$

Where $\sim$ is the equivalence relation generated by $s s^{-1} \sim s^{-1} s \sim 1 \;\; \forall s \in S$, where we write 1 for the empty word.

We define a binary operation

$$\bullet : F_S \times F_S \longrightarrow F_S$$

by $\left((s_1^{\epsilon_1} \cdots s_k^{\epsilon_k}), (r_1^{\delta_1} \cdots r_k^{\delta_k}) \right)$

$$\mapsto s_1^{\epsilon_1} \cdots s_k^{\epsilon_k} r_1^{\delta_1} \cdots r_k^{\delta_k} \quad \text{(concatenation)}.$$

This is associative, the empty word is the identity and $s_1^{\epsilon_1} \cdots s_k^{\epsilon_k}$ has the inverse $s_k^{-\epsilon_k} \cdots s_1^{-\epsilon_1}$, so F_S is a group: <u>the free group on the set S.</u>

If $S = \{s_1, \dots, s_n\}$ we typically write

$$F_n := F_S$$

and call F_n the free group on n generators.