Problem Set 4

Due Thursday, September 25

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly*. As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. Let G be a group, and let H and K be finite subgroups of G of relatively prime order; i.e., $\gcd(|H|, |K|) = 1$. Show that $H \cap K = \{e\}$.

Proof. Let $g \in H \cap K$. By Lagrange's Theorem, $|g|$ both divides $|H|$ and $|K|$, and hence their GCD, which is one. Thus $g = e$, so $H \cap K = \{e\}$. □

Problem 2. For $k \in \mathbb{Z}_{\geq 2}$, let C_k denote the cyclic group of order k. Show that for any relatively prime $m, n \geq 2$, there is an isomorphism $C_m \times C_n \cong C_{mn}$.

Proof. Fix generators x for C_m and y for C_n so that we have $|x| = m$ and $|y| = n$. We claim that $|(x, y)| = mn$. Indeed,

$$(x,y)^d = (x^d, y^d) = (e_{C_m}, e_{C_n})^{1} \iff \begin{cases} x^d = e_{C_m} \\ y^d = e_{C_n} \end{cases} \iff \begin{cases} m \mid d \\ n \mid d \end{cases} \iff \operatorname{lcm}(m,n) \mid d.$$

Since $\gcd(m, n) = 1$, we have $\operatorname{lcm}(m, n) = mn$ hence the smallest $d \geq 1$ so that $(x, y)^d = (e_{C_m}, e_{C_n})$ is mn. This shows $|(x, y)| = mn$ in $C_m \times C_n$.

BY the UMP of the cyclic group there is a group homomorphism $f : C_{mn} \to C_m \times C_n$ so that $f(a^i) = (x, y)^i$, where a is a generator of C_{mn} and $i \in \mathbb{Z}$ is arbitrary. We see that $f(a^i) = (e_{C_m}, e_{C_n})$ if and only if $(x, y)^i = (e_{C_m}, e_{C_n})$ if and only if $mn \mid i$ (by the argument above) if an only if $a^i = e_{C_{mn}}$. Thus $\ker(f) = \{e_{C_{mn}}\}$ and thus f is injective. Since f maps between sets of the same cardinality mn and is injective it must be bijective, hence an isomorphism. □

Problem 3. Let S_n denote the symmetric group on n symbols.

(3.1) Show that[2] the sign map $S_n \to \{\pm 1\}$ is a group homomorphism, where $\{\pm 1\}$ is considered as a subgroup of $\mathbb{R}^\times$. The kernel of this map is called the **alternating group** on n symbols and denoted A_n.

Proof. To verify that this is a homomorphism, let $\sigma, \tau \in S_n$; we proceed by cases. If $\operatorname{sign}(\sigma) = \operatorname{sign}(\tau) = 1$, then we can write σ as a product of $2m$ transpositions for some m and τ as a product of $2n$ transpositions; then $\sigma\tau$ can be written as a product of $2(m+n)$ transpositions, so $\operatorname{sign}(\sigma\tau) = 1 = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\tau)$. If $\operatorname{sign}(\sigma) = 1$ and $\operatorname{sign}(\tau) = -1$, then we can write σ as a

[1] The identity element of $G_1 \times G_2$ is (e_{G_1}, e_{G_2})

[2] Your proof should be no more than a few lines.

product of $2m$ transpositions for some m and τ as a product of $2n+1$ transpositions; then $\sigma\tau$ can be written as a product of $2(m+n)+1$ transpositions, so $\text{sign}(\sigma\tau) = -1 = \text{sign}(\sigma)\cdot\text{sign}(\tau)$. The other cases are similar. □

(3.2) Let $n \geq 3$. Show that A_n is generated by the set of 3-cycles $(i\ j\ k)$ and disjoint pairs[3] of transpositions $(i\ j)(k\ \ell)$ in S_n.

Proof. We know that every element of A_n can be written as a product of and even number transpositions, by definition. Pairing off transpositions, it follows that every element of A_n is a product of elements of the form $(a\,b)(c\,d)$, with $a \neq b$ and $c \neq d$, but $\{a, b\}$ and {c,d}*notnecessarilydisjoint.If*{a,b}*and*$\{c, d\}$ are disjoint, this is a disjoint pair of transpositions. If $|\{a, b\} \cap \{c, d\}| = 2$, then this is the identity, which is redundant in any generating set. If $|\{a, b\} \cap \{c, d\}| = 1$, since $(a\,b) = (b\,a)$ and $(c\,d) = (d\,c)$, without loss of generality we can write $(a\,b)(c\,d) = (i\,j)(j\,k) = (i\,j\,k)$ for i, j, k distinct. Thus, every element of A_n is a product of 3-cycles and pairs of disjoint transpositions, so these elements generate. □

DEFINTION: Let G be a group and N be a subgroup. We say that N is a **normal** subgroup of G if for all g in G, we have $gNg^{-1} \subseteq N$; that is, for any $g \in G$ and any $n \in N$, we have that $gng^{-1} \in N$. We write $N \trianglelefteq G$ to say N is a normal subgroup of G.

Problem 4. Let $f : G \to H$ be a group homomorphism.

(4.1) Show that $\ker(f) \trianglelefteq G$.

Proof. We already know that $\ker f$ is a subgroup of G, so we only need to prove normality. Consider $g \in \ker f$, and any $h \in G$. Then

$$\begin{aligned} f(hgh^{-1}) &= f(h)f(g)f(h)^{-1} && \text{since } f \text{ is a homomorphism} \\ &= f(h)f(h)^{-1} && \text{since } f(g) = e_H \\ &= e_H, \end{aligned}$$

so $hgh^{-1} \in H$. We conclude that H is normal. □

(4.2) Show that if $K \trianglelefteq H$, then $f^{-1}(K) \trianglelefteq G$.

Proof. We have already shown that the preimage of a subgroup is a subgroup. We justify the normality of the preimage. Let $g \in G$ and $\ell \in f^{-1}(K)$. Then $f(\ell) \in K$ and $f(g\ell g^{-1}) = f(g)f(\ell)f(g)^{-1} \in K$ by the normality of K. Therefore $g\ell g^{-1} \in f^{-1}(K)$ for all $g \in G$ and so $gf^{-1}(K)g^{-1} \subseteq f^{-1}(K)$ for all $g \in G$. This suffices to prove that $f^{-1}(K) \trianglelefteq G$. □

Problem 5. Let G be a group, S a subset of G, and $H = \langle S \rangle$.

(5.1) Prove that $H \trianglelefteq G$ if and only if $gsg^{-1} \in H$ for every $s \in S$ and $g \in G$.

[3] For $n = 3$, there are no disjoint pairs of transpositions.

Proof. Suppose $gsg^{-1} \in H$ for all $s \in S$. Let $h \in H$ and $g \in G$. Then $h = s_1^{e_1} s_2^{e_2} \cdots s_n^{e_n}$ for some $s_1, \ldots, s_n \in S$ and $e_1, \ldots, e_n \in \{\pm 1\}$. Let $g \in G$. Then

$$ghg^{-1} = g(s_1^{e_1} s_2^{e_2} \cdots s_n^{e_n})g^{-1} = (gs_1^{e_1}g^{-1})(gs_2^{e_2}g^{-1}) \cdots (gs_n^{e_n}g^{-1}).$$

Note that if $e_i = -1$ then $gs_i^{-1}g^{-1} = (gs_ig^{-1})^{-1} \in H$. Thus, $gs_i^{e_i}g^{-1} \in H$ for all i, and hence $ghg^{-1} \in H$. Therefore, $H \triangleleft G$. The reverse implication is true by definition of normal subgroup. □

(5.2) Consider the commutator subgroup of G

$$[G, G] := \langle aba^{-1}b^{-1} \mid a, b \in G \rangle$$

generated by all the commutators of elements in G. Prove that $[G, G] \trianglelefteq G$.

Proof. Let $g \in G$ and $s = aba^{-1}b^{-1}$. Set $x = gag^{-1}$ and $y = gbg^{-1}$, and note that

$$gsg^{-1} = xyx^{-1}y^{-1} \in S \subseteq H.$$

Hence, $H \trianglelefteq G$ by (5.1). □