Exercises 9, 10, pp. 116-117.

Problem 9. Assume G acts transitively on the finite set A and let H be a normal subgroup of G. Let $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ be the distinct orbits of H on A.

(a) Prove that G permutes the sets $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_r$ in the sense that for each $g \in G$ and each $i \in \{1, \ldots, r\}$ there is a j such that $g\mathcal{O}_i = \mathcal{O}_j$, where $g\mathcal{O} = \{g \cdot a \mid a \in \mathcal{O}\}$. Prove that G is transitive on $\{\mathcal{O}_1, \ldots \mathcal{O}_r\}$. Deduce that all orbits of H on A have the same cardinality.

(b) Prove that if $a \in \mathcal{O}_1$ then $|\mathcal{O}_1| = |H : H \cap G_a|$ and prove that $r = |G : HG_a|$.

Proof. Part (a): Each orbit $\mathcal{O}_i$ is of the form $H \cdot x$. Then for any $i, j \in \{1, \ldots, r\}$. Since G acts transitively on A, there is some g' such that $x = gy$. we want $H \cdot x = g \cdot (H \cdot y)$ for some $g \in G$. Since G acts transitively on A, there is some g' such that $x = g \cdot y$. Then $g \cdot (H \cdot y) = (gH) \cdot y$. The normality of H implies $gH = Hg$, thus $(gH) \cdot y = (Hg) \cdot y = H \cdot g \cdot y = H \cdot x$, which shows that G permutes $\{\mathcal{O}_1, \ldots, \mathcal{O}_r\}$.

Since we can find $\mathcal{O}_i = g\mathcal{O}_j$ for any i, j, clearly G acts transitively on $\{\mathcal{O}_1, \ldots, \mathcal{O}_r\}$. Furthermore this implies that both $|\mathcal{O}_i| \subseteq |\mathcal{O}_j|$ and $|\mathcal{O}_j| \subseteq |\mathcal{O}_i|$. Thus we conclude that all orbits have the same size. □

Proof. Part (b): By the orbit-stabilizer theorem, we have $|\mathcal{O}_1| = |H : H_a|$. But by definition $H_a = H \cap G_a$, so $|\mathcal{O}_1| = |H : H \cap G_a|$.

Next, since $H \trianglelefteq G$, we may apply the second isomorphism theorem to obtain $H/(H \cap G_a) \cong HG_a/G_a$. Thus $|\mathcal{O}_1| = |HG_a : G_a|$. Now we can use the orbit-stabilizer theorem again to compute r:

$$r = \frac{|A|}{|\mathcal{O}_1|} = \frac{|A|}{|HG_a : G_a|} = \frac{|G|/|G_a|}{|HG_a|/|G_a|} = \frac{|G|}{|HG_a|} = |G : HG_a|.$$

□

Problem 10. Let H and K be subgroups of the group G. For each $x \in G$ define the HK *double coset* of x in G to be the set

$$HxK = \{hxk \mid h \in H, k \in K\}.$$

(a) Prove that HxK is the union of left cosets in the orbit of xK generated by H acting on G/K.

(b) Prove that HxK is the union of right cosets of H.

(c) Show that the double cosets are disjoint and partition G.

(d) Prove that $|HxK| = |K| \cdot |H : H \cap xKx^{-1}|$.

(e) Prove that $|HxK| = |H| \cdot |K : K \cap xHx^{-1}|$.

Proof. Part (a): We want to show that

$$HxK = \bigcup_{h \in H} hxK.$$

If $g \in HxK$, then there exist $h \in H$ and $k \in K$ such that $g = hxk$. Then $g \in hxK \subseteq \bigcup_{h \in H} hxK$. Hence we have one inclusion. This proves $HxK \subseteq \bigcup_{h \in H} hxK$

Conversely, if $g \in \bigcup_{h \in H} hxK$, then there exists $h \in H$ such that $g \in hxK$, which again implies there exists $k \in K$ with $g = hxk$. Hence $g \in HxK$. This proves $\bigcup_{h \in H} hxK \subseteq HxK$, and thus $HxK = \bigcup_{h \in H} hxK$. □

Proof. Part (b): This is very similar to part (a). Briefly, we have:

$$g \in HxK \iff \exists h \in H, k \in K, g = hxk \iff g \in \bigcup_{k \in K} Hxk.$$

□

Proof. Part (c): Consider the relation $x \sim y$ if and only if there exist $h \in H$ and $k \in K$ such that $y = hxk$. We claim that this is an equivalence relation with classes HxK.

Indeed, $1 \in H$ and $1 \in K$, so $x = 1x1 \Rightarrow x \sim x$.

If $x \sim y$, then $y = hxk \Rightarrow h^{-1}yk^{-1}$. Hence $y \sim x$.

If $x \sim y$ and $y \sim z$, then $y = hxk$ and $z = h'yk'$ implies $z = h'hxkk'$. Clearly $h'h \in H$ and $kk' \in K$, $x \sim z$.

Thus the relation is an equivalence relation. Clearly the classes are $\{hxk \mid h \in H, k \in K\} = HxK$, as desired. □

Proof. Part (d): From part (a), take the set of coset $\{hxK \mid h \in H\}$ whose union is HxK. Note that for any $h, h' \in H$, either $hxK \cap h'xK = \varnothing$ or $hxK = h'xK$. Define $h \sim h'$ if and only if the latter $hxK = h'xK$ holds. Clearly this is an equivalence relation, because is it a subrelation on the cosets of xK. Furthermore, if $h \sim h'$, then we see that

$$hxK = h'xK \iff x^{-1}(h'^{-1}h)xK \in K \iff x^{-1}(h'^{-1}h)x \in K \iff h'^{-1}h \in xKx^{-1}.$$

.

Simultaneously, $h'^{-1}h \in H$, so we may further see that

$$h'^{-1}h \in H \cap xKx^{-1} \iff h \in h'(H \cap xKx^{-1}),$$

where we view $h'(H \cap xKx^{-1})$ as a coset of $H/(H \cap xKx^{-1})$. Thus $\{hxK \mid h \in H\}$ can be divided into $|H/(H \cap xKx^{-1})|$ distinct classes. Since each class all contain the same cosets, we may rewrite our union with a transversal $\mathcal{C}$ of the cosets $H/(H \cap xKx^{-1})$.

$$HxK = \bigcup_{h \in H} hxK = \bigsqcup_{h \in \mathcal{C}} hxK.$$

Notice that now the second union is disjoint. Hence we may take the cardinality of both sides, with $|\mathcal{C}| = |H/(H \cap xKx^{-1})|$, to obtain:

$$|HxK| = \left| \bigsqcup_{h \in \mathcal{C}} hxK \right| = |K| \cdot |\mathcal{C}| = |K| \cdot |H/(H \cap xKx^{-1})|.$$

$\square$

Proof. Part (e): This proof is very similar to part (d). We may prove that $Hxk = Hxk'$ if and only if $k \in k'(K \cap (x^{-1}Hx))$. Then again, with part (b),

$$|HxK| = \left| \bigsqcup_{k \in \mathcal{C}} Hxk \right| = |H| \cdot |\mathcal{C}| = |H| \cdot |K/(K \cap x^{-1}Hx)|.$$

$\square$

Exercises 8, 14, pp. 122-123.

Problem 8. Prove that if H has finite index n then there is a normal subgroup $K \trianglelefteq G$ with $K \leq H$ and $|G : K| \leq n!$.

Proof. Let G act on the left cosets of H with permutation representation $\pi_{G/H} : G \to S_{|G/H|}$. Then let $K = \ker(\pi_{G/H})$, which is clearly a subset of K and also a normal subgroup of G. By the first isomorphism theorem, $G/\ker(\pi_{G/H}) = G/K \cong \operatorname{im}(\pi_{G/H})$. Comparing the cardinality of both sides, we have

$$|G : K| = |G/K| = |\operatorname{im}(\pi_{G/H})| \leq |S_{|G/H|}| = n!.$$

$\square$

Problem 14. Let G be a finite group of composite order n with the property that G has a subgroup of order k dividing n for each positive integer k dividing n. Prove that G is not simple.

Proof. Choose k such that $n/k = p$, where p is the minimum prime dividing n. Then by Corollary 5, there is a normal subgroup of index p in G. Thus G cannot be simple. $\square$