Problem 2 (Ch. 1.12)

Determine representatives of the conjugancy classes in S_5 and the number of elements in each class. Use this information to prove that the only normal subgroups of S_5 are 1, A_5, S_5.

Solution. As is shown in Jacobson, the conjugancy classes of S_5 have a 1-1 correspondance to the partitions of 5, namely positive integers $r \geq s \geq \cdots \geq u$ such that $r + s + \cdots + u = 5$. The partitions of 5 are (5), $(4,1)$, $(3,2)$, $(3,1,1)$, $(2,2,1)$, $(2,1,1,1)$, and $(1,1,1,1,1)$. Thus, we present the following representatives of the corresponding equivalence classes:

$$\begin{aligned}
&(12345) = (15)(14)(13)(12)\\
&(1234)(5) = (14)(13)(12)\\
&(123)(45) = (13)(12)(45)\\
&(123)(4)(5) = (13)(12)\\
&(12)(34)(5) = (12)(34)\\
&(12)(3)(4)(5) = (12)\\
&(1)(2)(3)(4)(5) = (1)
\end{aligned}$$

If K is a normal subgroup of S_5, then $\alpha^{-1}K\alpha \in K$ for all $\alpha \in S_5$. We know that K must be some union of our conjugancy classes (otherwise if it did not contain an entire conjugancy class, it fails for α in that conjugancy class), and since it is a group, it must contain (1). Given this, since conjugancy classes imply $\alpha^{-1}K\alpha \in K$, we just need to find the subgroups of S_5 which are unions of conjugancy classes, and closed under multiplication.

If $K \subseteq A_5$, then it contains only even conjugancy classes (note that conjugancy classes all share the same sign, since any element in a conjugancy class given by the representative above can be decomposed into transpositions similarily). These are $\overline{(12345)}, \overline{(123)}, \overline{(12)(34)}, \overline{(1)}$. Note that $(15)(14) \cdot (123) = (12345) \in \overline{(12345)}$, $(14)(15) \cdot (12345) = (123) \in \overline{(123)}$ and $(315) \cdot (12345) = (12)(34)\overline{(12)(34)}$, thus the group is only closed when all of the even conjugancy classes are included in K, i.e. $K = A_5$, or $K = 1$.

Now let $K \not\subseteq A_5$. Then K must contain at least one of the odd conjugancy classes, so $\overline{(1234)}$, $\overline{(123)(45)}$ and/or $\overline{(12)}$. But the product of two odd permutations is even, and so one can see that $A_5 \subseteq K$. Similar to before, we can construct products between the odd conjugancy classes and the even ones such that K is only closed when all of the odd conjugancy classes are included. Thus $K = S_5$.

Problem 4 (Ch. 1.12)

*Show that if a finite group G has a subgroup H of index n then H contains a normal subgroup of G of index a divisor of $n!$. (*Hint*: Consider the action of G on G/H by left translations.*

Solution. Consider the action of G on G/H by left translations. By definition, this a homomorphism $T: G \to \text{Sym}(G/H)$ (where $\text{Sym}(G/H)$ are the bijective maps on G/H to itself). Let $K = \ker(T)$. Note that K is a normal subgroup of G by the fundamental theorem of homomorphisms. Furthermore, by the fundamental theorem, there is a bijection from G/K to the image $T(G) \subseteq \text{Sym}(G/H)$. Since T is a homomorphism, $T(G)$ is a group, specifically a subgroup of $\text{Sym}(G/H)$. Since the index of G/H is n, there are n elements in G/H, and so there are $n!$ elements in $\text{Sym}(G/H)$ (the number of permutations of n elements). By Lagrange's theorem, the order of a subgroup divides the order of the group, and so $|G/K| = [G : K] \mid |\text{Sym}(G/H)| = n!$.

It remains to show that K is a subgroup of H. The identity of $\text{Sym}(G/H)$ is the identity map of the cosets of G/H. Since $K = \ker(T)$, this means that for any $k \in K$, $kxH = xH$ for all $x \in G$. Fixing $x = 1_G$, we have $kH = H$. But this is true only if $k \in H$ for all $k \in K$, thus H contains a normal subgroup of index a divisor of $n!$.

Problem 5 (Ch. 1.12)

Let p be the smallest prime dividing the order of a finite group. Show that any subgroup of H of G of index p is normal.

Solution. We apply Problem 4 from 1.12 (above): if H is a subgroup of G with index p, then H contains a normal subgroup of G, call it K, such that $[G : K] \mid p!$. Now recall from Problem 2 of 1.7 of Jacobson that $[G : K] = [G : H][H : K]$ since $K \subset H$, thus $p = [G : H] \mid [G : K] \mid p!$. Thus $[G : K] = np$ for some $n \in \mathbb{N}$, $1 \leq n \leq p - 1$.

We note that p is the smallest value (other than 1) dividing the order of the group G. If there was a prime value smaller that divides $|G|$, we contradict our assumption that p was the smallest, and if there was a composite value smaller, than there are primes that divide the compositie value which must be smaller than it, which also contradicts our assumption.

By Lagrange's theorem, $|G| = |K|np \implies n \mid |G|$, but if $1 < n < p$, but since p is the smallest value that divides $|G|$ other than 1, we must have that $n = 1$. Thus $[G : K] = p = [G : H]$ as well, so $|K| = |H|$ by Lagrange's theorem (ie. $|H|p = |K|p = |G|$), and since K is a subgroup of H, we have that $H = K$. Hence, H is normal in G (since K was).

Problem 6 (Ch. 1.12)

Show that every group of order p^2, p is a prime, is abelian. Show that up to isomorphism there are only two such groups.

Solution. Let G be a group with order p^2. For the sake of contradiction, assume that G is not abelian. Then $|C(G)| = p^2$, and also by Theorem 1.11, $C(G) \neq 1$, thus since $|C(G)| \mid |G|$, we have that $|C(G)| = p$. Let $g \in G$ such that $g \notin C(G)$. Since $[G : C(G)] = p$, g and $C(G)$ generate G. Thus, if $a \in G$, we have that $a = g^i c$ where $c \in C(G)$ and $0 \leq i \leq p - 1$. So if $b \in G$ such that $b = g^j c'$ with the same assumptions as before, we have that $ab = (g^i c)(g^j c') = g^i g^j cc' = (g^j c')(g^i c)$. But since $a, b \in G$ were arbitrary, this means G is abelian, contradiction.

Now, note that G can be cyclic. If G has an element with order p^2, G is cyclic. If it is not, then all non-identity elements of G has order p (to divide the order of the group). Any two elements a, b will generate the group if $a \neq b^n$ for any n, since $p \cdot p = p^2$. Thus if two such elements are a, b, then $G = \langle a, b \rangle$.

Problem 8 (Ch. 1.12)

Let G act on S, H act on T, and assume $S \cap T = \emptyset$. Let $U = S \cup T$ and define for $g \in G$, $h \in H$, $s \in S$, $t \in T$; $(g, h)s = gs$, $(g, h)t = ht$. Show that this defines an action of $G \times H$ on U.

Solution. Note that this map is well-defined, since if $u \in U$, then either $u \in S$ or $u \in T$ but not both, so it always gets mapped to only one element in U.

The identity of $G \times H$ is $(1_G, 1_H)$. If $u \in S$, then $(1_G, 1_H)u = 1_G u = u$. If $u \in T$, then $(1_G, 1_H)u = 1_H u = u$.

Let $(g_1, h_1), (g_2, h_2) \in G \times H$. If $u \in S$, then $((g_1, h_1)(g_2, h_2))u = (g_1 g_2, h_1 h_2)u = g_1 g_2 u = (g_1, h_1)g_2 u = (g_1, h_1)(g_2, h_2)u$. If $u \in T$, then $((g_1, h_1)(g_2, h_2))u = (g_1 g_2, h_1 h_2)u = h_1 h_2 u = (g_1, h_1)h_2 u = (g_1, h_1)(g_2, h_2)u$. Thus, we have shown that this defines a group action.

Problem 9 (Ch. 1.9)

A group H is said to act on a group K by automorphisms *if we have an action of H on K and for every $h \in H$ the map $k \to hk$ of K is an automorphism. Suppose this is the case and let H be the product set $K \times H$. Define a binary composition in $K \times H$ by*

$$(k_1, h_1)(k_2, h_2) = (k_1(h_1 k_2), h_1 h_2)$$

and define $1 = (1, 1)$ – the units of K and H respectively. Verify that this defines a group such that $h \to (1, h)$ is a monomorphism of H into $K \times H$ and $k \to (k, 1)$ is a monomorphism of K into $K \times H$ whose image is a normal subgroup. G is called a semi-direct product of K and H. *Note that if H and K are finite than $|K \times H| = |K||H|$.*

Solution. We first show that this defines a group. First, the binary composition is closed, since $h_1 k_2 \in K$, since $k \to h_1 k$ is an automorphism, so $h_1 k \in K$ for all k, which includes k_2; then the product of $k_1(h_1 k_2) \in K$ by closure of K. Also, $h_1h_2 \in H$ by closure of H. Second, we show associativity:

$$\begin{aligned}((k_1,h_1)(k_2,h_2))(k_3,h_3) &= (k_1(h_1k_2),h_1h_2)(k_3,h_3)\\ &= (k_1(h_1k_2)(h_1(h_2k_3)),(h_1h_2)h_3)\\ &= (k_1(h_1(k_2(h_2k_3))),h_1(h_2h_3))\\ &= (k_1,h_1)(k_2(h_2k_3),h_2h_3)\\ &= (k_1,h_1)((k_2,h_2)(k_3,h_3))\end{aligned}$$

Where the third line is done by $(h_1k_2)(h_1(h_2k_3)) = h_1(k_2(h_2k_3))$ since $\phi\colon k \to h_1k$ is an isomorphism (since its an automorphism), so $\phi(k_2(h_2k_3)) = \phi(k_2)\phi(h_2k_3)$. The unit is in $K \times H$, specifically $(1_K, 1_H)$. Finally, we claim the inverse of $(k,h) \in K \times H$ is $(h^{-1}k^{-1}, h^{-1}) \in K \times H$. See:

$$(k,h)(h^{-1}k^{-1},h^{-1}) = (k(h(h^{-1}k^{-1})),hh^{-1}) = (k(hh^{-1})k^{-1})),1_H) = (k(1_Hk^{-1}),1_H) = (kk^{-1},1_H) = (1_K,1_H)$$

$$(h^{-1}(k^{-1},h^{-1})(k,h) = ((h^{-1}k^{-1})(h^{-1}k),h^{-1}h) = (k'^{-1}k',1_H) = (1_K,1_H)$$

where we used the fact that $h^{-1}k = (h^{-1}k^{-1})^{-1}$ since $k \to h^{-1}k$ is an isomorphism (since its an automorphism), and so we denoted $h^{-1}k = k' \in K$. Thus, ths defines a group.

To verify $\phi\colon h \to (1,h)$ is a monomorphism, we see that it is a homomorphism since $\phi(h_1)\phi(h_2) = (1,h_1)(1,h_2) = (1(h_11),h_1h_2) = (1,h_1h_2) = \phi(h_1h_2)$ where we have made the substitution $h_11 = 1$ because $x \to h_1x$ is an isomorphism (since its an automorphism) and isomorphisms must map the identity to itself; to see that the map is injective, note that if $\phi(h) = \phi(h')$, then $(1,h) = (1,h')$ which is true if and only if $h = h'$.

To verify $\psi\colon k \to (k,1)$ is a monomorphism, we see that it is a homomorphism since $\psi(k_1)\psi(k_2) = (k_1,1)(k_2,1) = (k_1(1k_2),1) = (k_1k_2,1) = \psi(k_1k_2)$ where we have made the substitution $1k_2 = k_2$ because $k \to 1k$ is the identity automorphism and so maps k_2 to itself; to see that the map is injective, note that if $\psi(k) = \psi(k')$, then $(k,1) = (k',1)$ which is true if and only if $k = k'$.

Finally, to see that the image of ψ is normal subgroup of $K \times H$, it remains only to show that the image is normal, since by the fundamental theorem of homomorphisms, since K is a group and $k \to (k,1)$ is a homomorphism (monomorphism), then the image is a subgroup of $K \times H$. If $(k',1) = \psi(k') \in \psi^{\text{img}}(K)$ for some $k' \in K$, consider $(h^{-1}k^{-1},h)(k',1)(k,h)$ for arbitrary $(k,h) \in K \times H$ (where we have shown previously the expression on the left is our inverse). See

$$\begin{aligned}(h^{-1}k^{-1},h^{-1})(k',1)(k,h) &= ((h^{-1}k^{-1})(h^{-1}k'),h^{-1})(k,h)\\ &= (h^{-1}(k^{-1}k'),h^{-1})(k,h)\\ &= (h^{-1}(k^{-1}k')(h^{-1}k),h^{-1}h)\\ &= (h^{-1}(k^{-1}k'k),1)\end{aligned}$$

(where we have been pulling out h^{-1} since $k \to h^{-1}k$ is an isomorphism from the fact it is an automorphism, and so $(h^{-1}k)(h^{-1}k') = h^{-1}(kk')$). But $k^{-1}k'k \in K$ so $h^{-1}(k^{-1}k'k) \in K$ since $k \to h^{-1}k$ is an automorphism of K. Thus, $(h^{-1}(k^{-1}k'k),1) = \psi(h^{-1}(k^{-1}k'k))$, thus $(h^{-1}k^{-1},h^{-1})(k',1)(k,h) \in \psi^{\text{img}}(K)$, so the subgroup is normal.