Kris Harper
MATH 25700
Homework 6 November 13, 2009

Problem 1 (4.6.2). *Find all normal subgroups of S_n for all $n \geq 5$.*

Proof. Since A_n is simple for $n \geq 5$, we see that no proper nontrivial subgroup of A_n is normal in S_n. Therefore the only possible proper nontrivial normal subgroup of S_n is A_n, which is indeed normal since it has index 2. Thus 1, A_n, and S_n are the only normal subgroups of S_n for $n \geq 5$. □

Problem 2 (4.6.4). *Prove that A_n is generated by the set of all 3-cycles for $n \geq 3$.*

Proof. First note that any pair of transpositions can be written as a product of 3-cycles. If $a \neq c$ and $b \neq d$ then $(ab)(cd) = (acb)(acd)$ and in the case $a = c$, $(ab)(cd) = (adb)$ (note that if $a = c$ and $b = d$ then $(ab)(cd) = 1$). Since any element of S_n can be written as the product of transpositions, and A_n is the collection of even permutations, any element $x \in A_n$ can be written as an even number of transpositions. Then we can pair these up and write x as a product of 3-cycles. This shows that A_n is generated by 3-cycles. □

Problem 3 (5.1.4). *Let A and B be finite groups and let p be a prime. Prove that any Sylow p-subgroup of $A \times B$ is of the form $P \times Q$ where $P \in Syl_p(A)$ and $Q \in Syl_p(B)$. Prove that $n_p(A \times B) = n_p(A)n_p(B)$. Generalize both of these results to a direct product of any finite number of finite groups (so that the number of Sylow p-subgroups of a direct product is the product of the numbers of Sylow p-subgroups of the factors).*

Proof. Let $|A| = p^a m$ and $|B| = p^b n$ with $p \nmid m$ and $p \nmid n$ so that $|A \times B| = p^{a+b}mn$ where $p \nmid mn$. Suppose $R \in Syl_p(A \times B)$. Then $R \leq \{(a, b) \mid a \in P, b \in Q\}$ for $P \leq A$ and $Q \leq B$. That is, if we consider the coordinates of R corresponding to A and B separately, these elements form subgroups of A and B respectively, although we are not assuming that R is the entire direct product $P \times Q$. Note that $|R| = p^{a+b}$ which means $p^{a+b} \leq |P||Q|$. Since $P \leq A$ and a is maximal for A, then $|P| = p^a$. Likewise $|Q| = p^b$. Thus $P \in Syl_p(A)$ and $Q \in Syl_p(B)$ and we must have $R = P \times Q$. Furthermore, this shows that if $P' \in Syl_p(A)$ and $Q' \in Syl_p(B)$ then $P' \times Q' \in Syl_p(A \times B)$. Therefore, $n_p(A \times B) \leq n_p(A)n_p(B)$ by the first statement and $n_p(A)n_p(B) \leq n_p(A \times B)$ by the second. Thus they must be equal.

To generalize to a finite product of finite groups, we use induction on the number of groups. The $n = 1$ case is trivial, and the inductive step has been done above by letting A be a direct product of $n - 1$ finite groups. □

Problem 4 (5.1.5). *Exhibit a nonnormal subgroup of $Q_8 \times Z_4$ (note that every subgroup of each factor is normal).*

Proof. Consider the group $H = \langle (i, x) \rangle$. Then $(j, 1)H(j, 1)^{-1}$ contains the element $(jij^{-1}, x) = (-i, x)$ which isn't in H (the only element of H with $-i$ in the first coordinate has x^3 in the second coordinate). Thus $H \ntrianglelefteq Q_8 \times Z_4$. □

Problem 5 (5.1.10). *Let p be a prime. Let A and B be two cyclic groups of order p with generators x and y respectively. Set $E = A \times B$ so that E is the elementary abelian group of order p^2: E_{p^2}. Prove that the distinct subgroups of E of order p are*

$$\langle x \rangle, \langle xy \rangle, \langle xy^2 \rangle, \ldots, \langle xy^{p-1} \rangle, \langle y \rangle$$

(note there are $p + 1$ of them).

Proof. A subgroup of order p must be generated by some element of E. We show that a given element $x^i y^j \in E$ is in one of the enumerated subgroups. This is equivalent to finding k such that $(xy^k)^i = x^i y^{ik} = x^i y^j$. That is, finding $0 \leq k \leq p - 1$ such that $ik \equiv j \pmod{p}$. Since i and k are necessarily relatively prime to p, such a k must exist. Therefore $x^i y^j \in \langle xy^k \rangle$ for some k and is thus in one of the enumerated subgroups. Since y has order p, it's clear that y^k gives distinct values for all $0 \leq k \leq p - 1$. Thus, the elements x, xy, ..., xy^{p-1}, y are all distinct elements of E and each generates a distinct subgroup of order p. Since there are $p+1$ of these elements and there cannot be more than $p+1$ subgroups of order p in E, these must be exactly the groups of order p. □

Problem 6 (5.1.11)**.** *Let p be a prime and let $n \in \mathbb{Z}^+$. Find a formula for the number of subgroups of order p in the elementary abelian group E_{p^n}.*

Proof. Note that $|E_{p^n}| = p^n$ and every nonidentity element has order p. Thus, there are $p^n - 1$ elements of order p and each of these generates a subgroup of order p. Each of these subgroups have trivial intersection since they are all distinct and every nonidentity element is a generator. Then there are $p-1$ elements of order p in each subgroup, so there are $(p^n-1)/(p-1)$ subgroups of order p. □

Problem 7 (5.1.14)**.** *Let $G = A_1 \times A_2 \times \cdots \times A_n$ and for each i let B_i be a normal subgroup of A_i. Prove that $B_1 \times B_2 \times \cdots \times B_n \trianglelefteq G$ and that*

$$(A_1 \times A_2 \times \cdots \times A_n)/(B_1 \times B_2 \times \cdots \times B_n) \cong (A_1/B_1) \times (A_2/B_2) \times \cdots \times (A_n/B_n).$$

Proof. Let $H = B_1 \times B_2 \times \cdots \times B_n$ and $K = (A_1/B_1) \times (A_2/B_2) \times \cdots \times (A_n/B_n)$. Let $a = (a_1, \ldots, a_n) \in G$ and note that since $B_i \trianglelefteq A_i$ we have $a_i B_i a_i^{-1} = B_i$. Thus

$$aHa^{-1} = (a_1, \ldots, a_n)(B_1 \times \cdots \times B_n)(a_1^{-1}, \ldots, a_n^{-1}) = a_1 B_1 a_1^{-1} \times \cdots \times a_n B_n a_n^{-1} = B_1 \times \cdots \times B_n = H$$

and $H \trianglelefteq G$. Now define $\varphi : G \to K$ by $\varphi((a_1, \ldots, a_n)) = (a_1 B_1, \ldots, a_n B_n)$. Note that for $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in G$ we have

$$\begin{aligned}
\varphi((a_1, \ldots, a_n)(b_1, \ldots, b_n)) &= \varphi((a_1 b_1, \ldots, a_n b_n)) \\
&= (a_1 b_1 B_1, \ldots, a_n b_n B_n) \\
&= (a_1 B_1 b_1 B_1, \ldots, a_n B_n b_n B_n) \\
&= (a_1 B_1, \ldots, a_n B_n)(b_1 B_n, \ldots, b_n B_n) \\
&= \varphi((a_1, \ldots, a_n))\varphi((b_1, \ldots, b_n))
\end{aligned}$$

and thus φ is a homomorphism. Also note that if $(a_1 B_1, \ldots, a_n B_n) \in K$, then $\varphi((a_1, \ldots a_n)) = (a_1 B_1, \ldots, a_n B_n)$ and so $\varphi(G) = K$. Furthermore, if $\varphi((a_1, \ldots, a_n)) = (B_1, \ldots, B_n)$ then $a_i B_i = B_i$ and so necessarily $a_i \in B_i$. Thus $(a_1, \ldots, a_n) \in H$. And if $(a_1, \ldots, a_n) \in H$ then $\varphi((a_1, \ldots, a_n)) = (a_1 B_1, \ldots, a_n B_n) = (B_1, \ldots B_n)$ since $a_i \in B_i$ implies $a_i B_i = B_i$. Therefore $\ker \varphi = H$. From the first isomorphism theorem, we now have $G/H \cong K$ and this concludes the proof. □

Problem 8 (5.2.7)**.** *Let p be a prime and let $A = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle$ be an abelian p-group, where $|x_i| = p^{\alpha_i} > 1$ for all i. Define the p^{th}-power map*

$$\varphi : A \to A \text{ by } x \mapsto x^p.$$

(a) Prove that φ is a homomorphism.
(b) Describe the image and kernel of φ in terms of the given generators.
(c) Prove both $\ker \varphi$ and $A/\mathrm{im}\varphi$ have rank n (i.e., have the same rank as A) and prove these groups are both isomorphic to the elementary abelian group, E_{p^n}, of order p^n.

Proof. (a) For $x_1^{a_1}\cdots x_n^{a_n}$ and $x_1^{b_1}\cdot x_n^{a_n}$ elements of A we have

$$\begin{aligned}\varphi(x_1^{a_1}\cdots x_n^{a_n}x_1^{b_1}\cdots x_n^{b_n}) &= \varphi(x_1^{a_1+b_1}\cdots x_n^{a_n+b_n})\\ &= (x_1^{a_1+b_1}\cdots x_n^{a_n+b_n})^p\\ &= x_1^{pa_1+pb_1}\cdots x_n^{pa_n+pb_n}\\ &= x_1^{pa_1}\cdots x_n^{pa_n}x_1^{pb_1}\cdots x_n^{pb_n}\\ &= (x_1^{a_1}\cdots x_n^{a_n})^p(x_1^{b_1}\cdots x_n^{b_n})^p\\ &= \varphi(x_1^{a_1}\cdots x_n^{a_n})\varphi(x_1^{b_1}\cdots x_n^{a_n}).\end{aligned}$$

(b) Note that in each coordinate the elements which map to 1 under φ are those of the form $x^{kp^{\alpha_i-1}}$. We therefore have

$$\ker\varphi = \prod_{i=1}^n \{x_i^{kp^{\alpha_i-1}} \mid 0 \le k \le p-1\}.$$

Since there are p choices for k in each of these components ($p^{\alpha_i} > 1$ by assumption), we find that $\ker\varphi = E_{p^n}$, or more explicitly,

$$\ker\varphi = \langle x_1\rangle/Z_{p^{\alpha_1-1}} \times\cdots\times \langle x_n\rangle/Z_{p^{\alpha_n-1}}.$$

Now since φ is a homomorphism by (a), from the first isomorphism theorem we know that $\varphi(A)\cong A/\ker\varphi = A/E_{p^n}$. In particular, each component is equal to $\langle x_i\rangle/Z_p$ using Problem 8.

(c) We showed in part (b) that $\ker\varphi\cong E_{p^n}$. Now consider

$$A/\varphi(G) = A/(A/E_{p^n}) \cong \langle x_1\rangle/(\langle x_1\rangle/Z_p)\times\cdots\times\langle x_n\rangle/(\langle x_n\rangle/Z_p).$$

Note that from Lagrange's Theorem, we know that each component has order p (again, $\alpha_i > 1$ by assumption), and is thus isomorphic to Z_p. Therefore $A/\varphi(G)\cong E_{p^n}$. Since each of $\ker\varphi$ and $A/\varphi(G)$ are isomorphic to E_{p^n}, we have shown that they each have rank n. $\square$

Problem 9 (5.2.8). *Let A be a finite abelian group (written multiplicatively) and let p be a prime. Let*

$$A^p = \{a^p \mid a\in A\} \text{ and } A_p = \{x \mid x^p = 1\}$$

(so A^p and A_p are the image and kernel of the p^{th}-power map, respectively).
(a) Prove that $A/A^p \cong A_p$.
(b) Prove that the number of subgroups of A of order p equals the number of of subgroups of A of index p.

Proof. (a) Let $A = Z_{n_1}\times\cdots\times Z_{n_t}$ and let φ be the p^{th} power map. If $p\nmid n_i$ then Z_{n_i} has no elements of order p. Thus the kernel of φ in Z_{n_i} is trivial and this map is injective. Therefore $Z_{n_i}^p\cong Z_{n_i}$. On the other hand, if $p\mid n_i$ then $n_i = p^{\alpha_i}m_i$ where $p\nmid m_i$. The kernel of φ in Z_{n_i} in this case is all elements of the form $x^{p^{k\alpha_i-1}m}$ where $0\le k\le p-1$ which is thus Z_p. Therefore, as in Problem 9, we find that $A_p = E_{p^s}$ where $s\le t$ and $t-s$ is the number of n_i which don't have p as a factor. Now using the first isomorphism theorem we have $A^p\cong A/E_{p^s}$ and using Problem 8 we have

$$\begin{aligned}A/A^p &= A/(A/E_{p^s})\\ &= Z_{n_1}\times\cdots\times Z_{n_t}/(Z_{n_1}\times\cdots\times Z_{n_t}/Z_p\times\cdots\times Z_p)\\ &\cong Z_{n_1}/(Z_{n_1}\times\cdots\times Z_{n_t}/Z_p\times\cdots\times Z_p)\times\cdots\times Z_{n_t}/(Z_{n_1}\times\cdots\times Z_{n_t}/Z_p\times\cdots\times Z_p)\\ &\cong Z_{n_1}/(Z_{n_1}/Z_p)\times\cdots\times Z_{n_t}/(Z_{n_t}/Z_p).\end{aligned}$$

Note that we've written this product so that for n_i with $p\nmid n_i$, a 1 appears in the product E_{p^s}. That is, E_{p^s} in this case is the product of s copies of Z_p along with $t-s$ trivial groups in ith place if $p\nmid n_i$. Now using

Lagrange's Theorem, each of the groups in the product has order p or 1, with $t-s$ groups of order 1, and is thus isomorphic to Z_p which shows that $A/A^p \cong E_{n^s} \cong A_p$.

(b) Note that the number of elements of order p is precisely the number of elements in A_p (minus the identity) as these elements get mapped to 1 when raised to the p^{th} power and p is prime. Each generates a subgroup of order p, and each of these subgroups trivially intersect. There are then $p-1$ distinct elements contributed from each subgroup, so the total number of subgroups of order p is

$$\frac{|A_p|-1}{p-1} = \frac{p^s-1}{p-1}.$$

Now we consider groups of index p. Each element of A/A^p corresponds to a group of index p. This can be seen by noting that $A^p \cong A/A_p$. This counts the trivial group as well, and so there are $|A/A^p|$ groups of index p subgroups, and for each one there are $p-1$ different elements which give the same group. Thus there are

$$\frac{|A/A^p|-1}{p-1} = \frac{p^s-1}{p-1}$$

groups of index p. ☐

Problem 10 (5.2.10)**.** *Let n and k be positive integers and let A be the free abelian group of rank n (written additively). Prove that A/kA is isomorphic to the direct product of n copies of $\mathbb{Z}/k\mathbb{Z}$ (here $kA = \{ka \mid a \in A\}$).*

Proof. Using Problem 8 it suffices to prove that $k\mathbb{Z} \trianglelefteq \mathbb{Z}$ for each k. But $\mathbb{Z}$ is abelian, so every subgroup is normal. ☐