# MATH 120: HOMEWORK 6 SOLUTIONS

- Section 4.3 # 28,34
- Section 4.4 # 2,13
- Section 4.5 # 13,25
- Section 7.4 # 37
- Section 7.5 # 3

**Problem 4.3 #28.** Let $p$ and $q$ be distinct primes with $p < q$. Prove that a nonabelian group $G$ of order $pq$ has a nonnormal subgroup of index $q$, so there exists an injective homomorphism $G \longrightarrow S_q$. Deduce that $G$ is isomorphic to a subgroup of the normalizer in $S_q$ of the cyclic group generated by the $q$-cycle $(1, 2, \cdots, q)$.

**Solution.** By Cauchy's theorem $G$ has element $x$ and $y$ of orders $p$ and $q$, respectively. Let $P$ and $Q$ be the cyclic subgroups they generate. Then $Q$ is normal by Corollary 5 on page 120. We claim that $P$ is not normal. If it is, then $xyx^{-1}y^{-1} = x(yxy^{-1})^{-1}$ is a product of two elements of $P$, so it is in $P$; while $xyx^{-1}y^{-1} = (xyx^{-1})y^{-1}$ is a product of two elements of $Q$ so it is in $Q$. This means that $xyx^{-1}y^{-1} \in P \cap Q = 1$ so $x$ and $y$ commute. However $x$ and $y$ generate $G$ since the order of the group they generate has order a multiple of both $p$ and $q$, so $\langle x, y\rangle = G$. If $x$ and $y$ commute then $G$ is abelian, which is a contradiction. This proves that $P$ is not normal.

Now $G$ acts on the set $X$ of left cosets of $P$ by left multiplication. Denote these $x_1P, \cdots, x_qP$. We have a homomorphism $\theta : G \longrightarrow \mathrm{Bij}(X)$, where $\mathrm{Bij}(X) \cong S_q$ is the set of bijections of $X$. We claim that $\theta$ is injective. If $k \in \ker(\theta)$ then $x_iP = \theta(k)x_iP = kx_iP$ for all $x_i$, so $x_i^{-1}kx_iP = P$ and $x_i^{-1}kx_i \in P$. This implies that $k \in \bigcap x_iPx_i^{-1}$. Since $P$ is not normal, this intersection is 1 implying that $k = 1$ and therefore $\theta$ is injective.

Because $\theta$ is injective we may identify $G$ with its image in $S_q$. The only elements of order $q$ in $S_q$ are $q$-cycles, so $\theta(y)$ is a $q$-cycle. Without loss of generality we may assume that $\theta(y) = (1, 2, \cdots, q)$. Then $Q$ is identified with $\langle(1, 2, \cdots, q)\rangle$. Since $Q$ is normal, the image of $G$ is contained in the normalizer of this cyclic subgroup, as required.

**Problem 4.3 # 34.** Prove that if $p$ is a prime and $P$ is a subgroup of $S_p$ of order $p$ then $|N_{S_p}(P)| = p(p-1)$. [Argue that every conjugate of $P$ contains exactly $p-1$ $p$-cycles and use the formula for the number of $p$-cycles to compute the index of $N_{S_p}(P)$ in $S_p$.]

**Solution.** Let $P_1 = P, P_2 \cdots, P_h$ be the subgroups of $S_p$ of order $p$. Each of these subgroups is cyclic of order $p$, and is generated by a $p$-cycle. They are all conjugate.

Let $P_i^* = P_i - \{1\}$. Then $P_i^*$ are clearly disjoint, and their union is the set of all $p$-cycles. Since $|P_i^*| = p-1$ this means that $(p-1)h$ is the total number of $p$-cycles in $S_p$. To count these another way, every $p$-cycle can be written $(1ab \cdots z)$ where $a, b, \cdots, z$ are $2, 3, \cdots, p$ in some order. There are $(p-1)!$ possibilities. Thus $(p-1)h = (p-1)!$ so $h = (p-2)!$.

Now $h$ is the number of conjugates of $P = P_1$, that is $[S_p : N_G(P)] = (p-2)!$. Now

$$|N_{S_p}(P)| = \frac{|S_p|}{[S_p : N_{S_p}(P)]} = \frac{p!}{(p-2)!} = p(p-1).$$

**Problem 4.4 # 2**. Prove that if $G$ is an abelian group of order $pq$, where $p$ and $q$ are distinct primes then $G$ is cyclic.

**Solution.** By Cauchy's theorem, $G$ has elements $x$ and $y$ of order $p$ and $q$ respectively. Let $z = xy$. We will show that $z$ generates $G$. First note that $z^q = x^q y^q = x^q$. Since $x$ has order $p$ and $p \nmid q$, $x^q$ has order $p$. Similarly $z^p$ has order $q$. The order of $z$ must therefore be a multiple of both $p$ and $q$, in other words, a multiple of $pq$. By Lagrange's theorem, the order of $z$ divides $|G| = pq$, so $pq$ is exacctly the order of $z$. Thus $z$ is a generator of $G$ and $G$ is cyclic.

**Problem 4.4 # 13.** Let $G$ be a group of order 203. Prove that if $G$ has a normal subgroup $H$ of order 7 then $H \subseteq Z(G)$.

**Solution.** We have $203 = 7 \cdot 29$. We are assuming that $H$ has order 7 and is normal. We then have a homomorphism $\phi : G \longrightarrow \mathrm{Aut}(H)$ which is the action by conjugation. In other words, $\phi(g)$ is the automorphism $c_g \in \mathrm{Aut}(H)$ defined by $c_g(x) = gxg^{-1}$. Now $\mathrm{Aut}(H)$ has order 6 by Proposition 16 on page 135 of Dummit and Foote. Therefore the image of $\phi$ is a subgroup of an order 6 that is isomorphic to $G/\ker(\phi)$; so its order divides both 6 and 203. Since 6 and 203 are coprime, this means that $\phi$ is the trivial map, so $c_g$ is the identity automorphism of $H$ for all $g$. That is, $gxg^{-1} = c_g(x) = x$ for all $x \in H$ and $g \in G$. Therefore $H$ is contained in the center of $G$.

**Problem 4.5 # 13.** Prove that a group of order 56 has a normal $p$-Sylow subgroup for some prime $p$ dividing 56.

**Solution.** Suppose that $|G| = 56$. The 7-Sylow has either 1 or 8 conjugates, since the number of 7-Sylows is $\equiv 1 \bmod 7$ and divides 56. Thus either the 7-Sylow is normal or it has 8 conjugates $P_1, \cdots, P_8$. Each $P_i$ contains 6 elements of order 7, and these are all distinct. So $G$ has $8 \cdot 6 = 48$ elements of order 7. Now let $Q$ be a 2-Sylow, so $|Q| = 8$. There are precisely 8 elements that are *not* of order 7, so

$$Q = \{g \in G | g \text{ does not have order } 7\}.$$

From this we see that the elements of $Q$ are permuted by conjugation, so $hQh^{-1} = Q$ for all $h$, and $Q$ is normal.

**Problem 4.5 # 25.** Prove that if $G$ is a group of order 385 then $Z(G)$ contains a 7-Sylow subgroup and an 11-Sylow subgroup is normal in $G$.

**Solution.** Since $385 = 5 \cdot 7 \cdot 11$, the number of 7-Sylows divides 55 and is $\equiv 1 \bmod 7$; therefore the 7-Sylow $P$ is normal. Also the number of 11-Sylows divides 35 and is $\equiv 1 \bmod 11$, so the 11-Sylow is also normal. But we have to show that the 7-Sylow is central. This is somewhat similar to We have a homomorphism $\theta : G \longrightarrow \mathrm{Aut}(P)$ in which $\theta(g)$ is conjugation by $P$. The image is a subgroup of $\mathrm{Aut}(P)$, which has order 6, which is isomorphic to $G/\ker(\theta)$; hence it has order dividing both 6 and 386. Since these are coprime, $\theta$ is trivial, meaning that $\theta(g) = 1_P$ for all $P$. Thus if $x \in P$ we have $gxg^{-1} = \theta(g)x = x$, and so $P$ is central.

**Problem 7.4 #37.** A commutative ring $R$ is called a *local ring* if it has a unique maximal ideal. Prove that if $R$ is a local ring with maximal ideal $M$ then every element of $R - M$ is a unit. Prove conversely that if $R$ is a commutative ring with unit such that the nonunits of $R$ form an ideal, then $R$ is a local ring with a unique maximal ideal $M$.

**Solution.** Let $R$ be local with maximal ideal $M$. We will show that $M$ is the set of non-units in $R$. If $x \in M$ then $Rx \subseteq M$ so $1 \notin Rx$, meaning that $x$ is a nonunit. On the other hand, suppose that $x$ is a non-unit. Then $Rx$ is a proper ideal of $R$. By Proposition 11 on page 254 of Dummit and Foote, it is contained in a maximal ideal. Since $R$ has a unique maximal ideal $M$, $Rx \subseteq M$. Therefore $x \in M$. We have proved that $M$ is the set of nonunits.

If $R$ is a commutative ring such that the nonunits form an ideal $M$, we are asked to show that $R$ is local. First let us check that $M$ is maximal. If $I$ is any ideal such that $M \subseteq I$, then either $I = M$ or $I$ contains an element $x \notin M$. Thus $x$ is a nonunit and so $R = Rx \subset RI = I$. Hence $M$ is maximal. To see that it is the unique maximal ideal, suppose that $M'$ is another maximal ideal. Then since $M'$ is proper, $M'$ consists of nonunits, so $M' \subseteq M$; since $M$ is maximal, $M' = M$.

Here is an example of a local ring: let

$$R = \{a/b \in \mathbb{Q} | a, b \in \mathbb{Z}, b \text{ odd}\}$$

It is easy to see that $R$ is closed under addition and multiplication, so it is a ring. It is local, with maximal ideal

$$M = \{a/b | a, b \in \mathbb{Z}, a \text{ even, } b \text{ odd.}\}$$

**Problem 7.5 # 3.** Let $F$ be a field. Prove that $F$ contains a unique smallest subfield $F_0$ and that $F_0$ is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime $p$.

**Solution.** In Exercise 7.3 #26 we constructed a homomorphism $\varphi : \mathbb{Z} \longrightarrow F$ such that $\varphi(1) = 1$. Let $\mathfrak{p}$ be the kernel of $\varphi$. Since $\varphi(\mathbb{Z})$ is a subring of a field, it is an integral domain. By the first isomorphism theorem, $\varphi(\mathbb{Z}) \cong \mathbb{Z}/\mathfrak{p}$, and therefore $\mathfrak{p}$ is a prime ideal. The prime ideals of $\mathbb{Z}$ are $(0)$, and $(p)$ where $p$ is a prime integer. There are thus 2 cases.

First, suppose that $\mathfrak{p} = 0$. Then $\varphi$ is injective, by Corollary 16 on page 263 of Dummit and Foote, the smallest field $F_0$ of $F$ that contains $\varphi(\mathbb{Z}) \cong \mathbb{Z}$ is isomorphic to the field of fractions $\mathbb{Q}$ of $\mathbb{Z}$. Any subfield of $F$ contains 1, hence the image of $\varphi$, and so $F_0$ is the smallest subfield of $F$.

If $\mathfrak{p} = (p)$, then $\varphi(\mathbb{Z}) \cong \mathbb{Z}/(p)$ is already a field, and it is a subfield of $F$. This is the field $F_0$ in this case. Since any subfield of $F$ contains 1, it contains $\varphi(\mathbb{Z})$, and so $F_0$ is the smallest subfield of $F$.