MATH 120: HOMEWORK 8

- Section 5.4 #5
- Section 5.5 #8,11
- Section 8.2 #1,4
- Section 8.3 #2

Problem 5.4 #5. Prove that A_n is the commutator subgroup of the symmetric group S_n for $n \geqslant 5$.

Solution. This is actually true for $n \geqslant 3$. However the following argument will make use of the simplicity of A_n (Theorem 24 in Section 4.6) so it would have to be modified for A_4.

Lemma 1. *Let G be any group then the commutator subgroup G' is normal and G/G' is abelian; moreover if H is any normal subgroup of G then G/H is abelian if and only if $G' \subseteq H$.*

Proof. This is (4) of Proposition 7 in page 169. □

We may solve the problem as follows. The subgroup A_n is normal and S_n/A_n has order 2, hence is abelian; therefore by the Lemma $S_n' \subseteq A_n$. Now the subgroup S_n' is normal in S_n, so it is normal in A_n, and nontrivial since S_n is nonabelian. Since A_n is simple, $S_n' = A_n$.

Problem 5.5 #8. Construct a nonabelian group of order 75. Classify all groups of order 75 (there are 3 of them).

Solution. Let G be a group of order 75. Let Q be a 5-Sylow subgroup, and let P be a 3-Sylow. The Sylow theorem implies that Q is normal. Indeed, the number of 5-Sylows is $\equiv 1 \bmod 5$ and divides $[G : Q] = 3$, so this number can only be 1. Thus the 5-Sylow is unique and therefore normal. $P \cong Z_3$ be a 3-Sylow. Then by Theorem 12 on page 180, G is isomorphic to the semidirect product $Q \rtimes_\theta P$ for some $\theta : P \longrightarrow \mathrm{Aut}(Q)$. There are two possibilities for Q: it could be Z_{25} or $Z_5 \times Z_5$. But if $Q = Z_{25}$ then $\mathrm{Aut}(Q) \cong (\mathbb{Z}/25\mathbb{Z})^\times$ by Proposition 16 on page 135. This has order $\varphi(25) = 20$ which is prime to 3, so in this case θ must be trivial. Thus if Q is cyclic then $G \cong P \times Q \cong Z_3 \times Z_{25} \cong Z_{75}$.

This leaves the case where $Q \cong Z_5 \times Z_5$. Then $\mathrm{Aut}(Q) \cong \mathrm{GL}_2(\mathbb{F}_5)$ by part (3) of Proposition 17 on page 136. This group has order $(5^2 - 1)(5^2 - 5) = 24 \cdot 20 = 480 = 2^5 \cdot 3 \cdot 5$ by Problem 1.4 #7 (Homework 2). So θ can be either the trivial homomorphism, producing the group $P \times Q \cong Z_3 \times Z_5 \times Z_5 \cong Z_{15} \times Z_5$, or it can be the isomorphism of P with a 3-Sylow subgroup of $\mathrm{Aut}(Q)$. These 3-Sylow subgroups are all conjugate by the Sylow theorem (applied to $\mathrm{Aut}(Q)$) and it is possible to deduce that these nontrivial homomorphisms $P \to \mathrm{Aut}(Q)$ all produce isomorphic groups.

Problem 5.5 #11. Classify groups of order 28 (there are four isomorphism types).

Solution. Let G be a group of order 28. Let P be a 2-Sylow and Q a 7-Sylow. The number of 7-Sylows is $\equiv 1 \bmod 7$ and divides $[G : Q] = 4$, so there is a unique 7-Sylow and therefore Q is normal. Since $Q \cap P = 1$, Theorem 12 on page 180 implies that G is a semidirect product $Q \rtimes_\theta P$ for some homomorphism $\theta : P \to \mathrm{Aut}(Q)$. Now Q has automorphism group

$\text{Aut}(Q) \cong \text{Aut}(Z_7) \cong (\mathbb{Z}/7\mathbb{Z})^\times$. This is a cyclic group of order 6 generated by the coset $\overline{3} = 3 + 7\mathbb{Z}$, since $\overline{3}^2 = \overline{2}$, $\overline{3}^3 = \overline{6}$, $\overline{3}^4 = \overline{4}$, $\overline{3}^5 = \overline{5}$ and $\overline{3}^6 = \overline{1}$. So $\text{Aut}(Q) \cong Z_6$ contains a unique subgroup $\langle \sigma_{-1} \rangle$ of order 2, where σ_{-1} is the automorphism $x \to x^{-1}$ of $(\mathbb{Z}/7\mathbb{Z})^\times$.

Now there are four groups that we can construct as follows. There are two possibilitys for P, which has order 4. It can be Z_4 or $Z_2 \times Z_2$. In either case there is a homomorphism $\theta : P \to \text{Aut}(Q) \cong Z_6$ which can be either trivial, or nontrivial, giving rise to four possible semidirect products.

Problem 8.2 #1. Prove that in a principal ideal domain R two ideals (a) and (b) are comaximal if and only if the greatest common divisor of a and b is 1.

Solution. By definition, the ideals (a) and (b) are *comaximal* if $(a) + (b) = R$. If (a) and (b) are comaximal, this means that we can write $1 = ra + sb$ for $r, s \in R$. Now if $d|a, b$ then d divides $1 = ra + sb$, so d is a unit. This proves that 1 is the greatest common divisor of a, b. On the other hand, suppose that 1 is the greatest common divisor of a, b. Consider the ideal $(a) + (b)$. This ideal is principal, so $(a) + (b) = (d)$ for some d. Then $a \in (d)$ so $d|a$ and similarly $d|b$. Since the greatest common divisor of a and b is 1, this means that d is a unit, so $(a) + (b) = (d) = R$, proving that $(a), (b)$ are comaximal.

Problem 8.2 #4. Let R be an integral domain. Prove that if the following two conditions hold then R is a principal ideal domain.

(i) any two nonzero elements a and b have a greatest common divisor which can be written in the form $ra + sb$ for some $r, s \in R$, and

(ii) If $a_1, a_2, \cdots$ are nonzero elements of R such that $a_{i+1}|a_i$ for all i, then there is a positive integer N such that a_n is a unit times a_N for all $n \geqslant N$.

Solution.

Lemma 2. *Suppose that $a, b \in R$ have a greatest common divisor d that can be written as $ra + sb$. Then the ideal $(a, b) = Ra + Rb$ equals (d).*

Proof. Note that a and b are both multiples of d, so $(a, b) \subseteq (d)$. On the other hand, $d \in (a, b)$ by assumption, so $(d) \subseteq (a, b)$. □

Let I be an ideal of R. We wish to show that I is principal. We will construct two sequences $c_1, c_2, c_3, \cdots$ and $a_1, a_2, a_3, \cdots$ of elements of I. The sequences will have the properties that if $I_k = (c_1, \cdots, c_k)$ then I_{k+1} strictly contains I_k, and $I_k = (a_k)$. We will obtain an contradiction if I is not principal.

If $I = 0$ then I is principal, so assume that $I \neq 0$. Pick $0 \neq c_1 \in I$, and let $a_1 = c_1$. The ideal $I_1 = (c_1)$.

If $I = I_1$ then I is principal, and we are done. Otherwise pick $c_2 \in I - I_1$, and define $I_2 = (a_1, c_2)$. This is strictly larger than I_1. By the Lemma and Assumption (i), we can find a_2 such that $I_2 = (a_2)$.

Continuing in this way, if $I_k = (c_1, \cdots, c_k) = (a_k)$ is defined, if $I_k = I$ then I is principal and we are done; otherwise, we pick $c_{k+1} \in I - I_k$, and let $I_{k+1} = (c_1, \cdots, c_k, c_{k+1}) = (a_k, c_{k+1})$; by Assumption (i) and the Lemma, I_{k+1} is principal and we let a_{k+1} be a generator.

Now since $a_k \in I_{k+1} = (a_{k+1})$ we have $a_{k+1}|a_k$. By Assumption (ii) we see that eventually the process must terminate and $a_{k+1} = a_k$ times a unit, so $I_{k+1} = (a_{k+1}) = I_k$; this is a contradiction since our construction guarantees that I_{k+1} is strictly larger than I_k.

Problem 8.3 #2. Let a and b be nonzero elements of the unique factorization domain R. Prove that a and b have a least common multiple and describe it in terms of the prime factorizations of a and b.

Solution. There is a finite set $\{p_1, \cdots, p_N\}$ of irreducible elements that divide either a or b. Since R is a unique factorization domain, we may write $a = \varepsilon p_1^{k_1} \cdots p_N^{k_N}$ where ε is a unit, and similarly $b = \delta p_1^{l_1} \cdots p_N^{l_N}$ with δ a unit. Let $m_i = \min(k_i, l_i)$ and define $d = p_1^{m_1} \cdots p_N^{m_N}$. Then we claim that d iss a greatest common divisor of a and b. Let $h \in R$. We will show that h divides both a and b if and only if $h|d$. Write $h = \mu p^{r_1} \cdots p^{r_N}$. Then $h|a$ if and only if $r_1 \leqslant k_1, \cdots, r_N \leqslant k_N$ and similarly $h|b$ if and only if $r_1 \leqslant l_1, \cdots, r_N \leqslant l_N$. So h divides both if and only if $r_i \leqslant \min(k_i, l_i) = m_i$, that is, $h|a, b$ if and only if $h|d$. Thus h is a greatest common divisor of a and b, and we have determined its factorization into primes.