MATH 120: HOMEWORK 7 SOLUTIONS

- Section 5.4 #12
- Section 5.5 #7,8
- Section 8.2 #1,4,8
- Section 8.3 #2

Problem 5.4 #12. Use Theorem 4.17 to describe the automorphism group of a finite cyclic group.

Solution. We will need the following fact.

Lemma 1. *If $|G|$ and $|H|$ are coprime then* $\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

Proof. If $\phi \in \mathrm{Aut}(G)$ and $\psi \in \mathrm{Aut}(H)$ then we define an automorphism $\phi \times \psi$ of $\mathrm{Aut}(G \times H)$ by $(\phi \times \psi)(g, h) = (\phi(g), \psi(h))$. This gives us a group homomorphism $(\phi, \psi) \mapsto \phi \times \psi$ from $\mathrm{Aut}(G) \times \mathrm{Aut}(H)$ to $\mathrm{Aut}(G \times H)$. It is obviously injective.

It is necessary to prove that every automorphism of $G \times H$ is of this form. To argue this, we will identify G and H with their images in $G \times H$. Since $|G|$ and $|H|$ are coprime, we may characterize G as the set of elements of $G \times H$ whose orders are prime to $|H|$. From this characterization of G we see that if $\alpha : G \times H \longrightarrow G \times H$ is any automorphism, then $\alpha(G) \subseteq G$. Similarly $\alpha(H) \subseteq H$. Then if ϕ is the restriction of α to G and ψ is the restriction of α to H, it is easy to see that $\alpha = \phi \times \psi$. This proves that $(\phi, \psi) \mapsto \phi \times \psi$ is a surjective map from $\mathrm{Aut}(G) \times \mathrm{Aut}(H)$ to $\mathrm{Aut}(G \times H)$. □

Let us describe the automorphism group of Z_N. First we factor N into a product of prime powers: $N = p_1^{k_1} \cdots p_r^{k_r}$ where p_i are distinct primes. By Proposition 6 on page 163 of Dummit and Foote, we have $Z_N \cong Z_{p_1^{k_1}} \times \cdots \times Z_{p_r^{k_r}}$, and using the Lemma we have

$$\mathrm{Aut}(Z_N) = \prod_{i=1}^{r} \mathrm{Aut}\left(Z_{p_i^{k_i}}\right).$$

Now the groups $\mathrm{Aut}\left(Z_{p_i^{k_i}}\right)$ are described in Proposition 4.17 of Dummit and Foote (page 136). We have

$$\mathrm{Aut}\left(Z_{p_i^{k_i}}\right) \cong \begin{cases} Z_{p_i^{k_i-1}} & \text{if } p_i \text{ is odd,} \\ Z_2 \times Z_{2^{k_i-2}} & \text{if } p_i = 2, k_i > 1, \\ 1 & \text{if } p_i^{k_i} = 2. \end{cases}$$

From this, we know the group of automorphisms of any finite cyclic group.

Problem 5.5 #7. This group describes thirteen isomorphism types of groups of order 56. (It is not too difficult to show that every group of order 56 is isomorphic to one of these.)

(a) Prove that there are three abelian groups of order 56.

(b) Prove that every group of order 56 either has a normal 2-Sylow or a normal 8-Sylow.

(c) Construct the following non-abelian groups of order 56 which have a normal 7-Sylow and whose 2-Sylow subgroup S is as specified:

- One group when $S \cong Z_2 \times Z_2 \times Z_2$

- Two nonisomorphic groups when $S \cong Z_4 \times Z_2$
- One group when $S \cong Z_8$
- Two nonisomorphic groups when $S \cong Q_8$
- Three nonisomorphic groups when $S \cong D_8$

(d) Let G be a group of order 56 with a nonnormal Sylow 7-subgroup. Prove that if S is the Sylow 2-subgroup then $S \cong Z_2 \times Z_2 \times Z_2$.

(e) Prove that there is a unique group of order 56 with a nonnormal 7-Sylow.

Solution. (a). The three abelian groups are $Z_8 \times Z_7 \cong Z_{56}$, $Z_4 \times Z_2 \times Z_7$ and $Z_2 \times Z_2 \times Z_2 \times Z_7$.

(b) (This was done in class.) Suppose that the 7-Sylow is not normal. We will prove that the 2-Sylow is normal. By the Sylow theorems, the number of 7-Sylows divides 8 and is $\equiv 1$ modulo 7. Hence if the 7-Sylow is not normal, there are 8 7-Sylows. Each contains six elements of order 7, so there are $8 \cdot 6 = 48$ elements of order 7. This leaves $56 - 48 = 8$ elements that are *not* of order 7. Let S be the set of these 8 elements. Now if Q is a 2-Sylow then $|Q| = 8$ and (since Q cannot contain an element of order 7) we have $Q \subseteq S$. Therefore $Q = S$. Now if $g \in G$ then gQg^{-1} is another 2-Sylow so by the same argument $gQg^{-1} = S = Q$ and so Q is normal.

Now the strategy for constructing all groups of order 56 can be seen: if P is a 7-Sylow and Q is a 2-Sylow, then either P or Q is normal. By the Second Isomorphism Theorem (page 97) PQ is a group, and since it contains subgroups of orders 7 and 8, $PQ = G$. Therefore G is a semidirect product. To describe it, we need to find homomorphisms $\varphi : P \longrightarrow \mathrm{Aut}(Q)$ if Q is normal, or $Q \longrightarrow \mathrm{Aut}(P)$ if P is normal. Given such a homomorphism, we can construct a semidirect product by Theorem 10 on page 176 of Dummit and Foote.

(c) If the 7-Sylow P is normal then $\mathrm{Aut}(P) \cong Z_6$, and we are looking for homomorphisms $\varphi : Q \longrightarrow Z_6$ where Q is a group of order 8. If the homorphism φ is trivial, then the group will be non-abelian only if Q is nonabelian. Thus we have two groups $Q_8 \times Z_7$ and $D_8 \times Z_7$, where Q_8 and D_8 are the quaternion and dihedral nonabelian groups. If φ is nontrivial, let $H = \ker(\varphi) \subseteq Q$. Since $\mathrm{Aut}(P) \cong Z_6$ has a unique subgroup A of order 2 and since Q has order a power of 2, the image of φ must be A and H is of index 2.

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 $75 = 3 \cdot 5^2$. Then by the Sylow theorem, the number of 5-Sylows is $\equiv 1$ mod 5 and divides 3, so the 5-Sylow Q is normal. If P is the 3-Sylow, then G is a semidirect product of P with the normal subgroup Q. Both P and Q are abelian, so for G to be nonabelian, the homomorphism $\varphi : P \longrightarrow \mathrm{Aut}(Q)$ must be nontrivial.

There are two possibilities for Q. If $Q \cong Z_{25}$ then $\mathrm{Aut}(Q)$ is cyclic of order 20, by Problem 5.4 #12. There can be no nontrivial homomorphism $Z_3 \longrightarrow \mathrm{Aut}(Q)$, so if the 5-Sylow is cyclic, G is abelian, indeed $G = Z_3 \times Z_{25} \cong Z_{75}$.

On the other hand if $Q \cong Z_5 \times Z_5$, then $\mathrm{Aut}(Q) \cong \mathrm{GL}(2, \mathbb{F}_5)$, which has order $2^5 \cdot 3 \cdot 5$, and there does exist a nontrivial subgroup of order 3, hence there does indeed exist a nontrivial homomorphism $Z_3 \longrightarrow \mathrm{Aut}(Q)$, and in this way we obtain a semidirect product.

The last remaining group is another abelian group $Z_3 \times Z_5 \times Z_5$.

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 8.2 #8. Prove that if R is a Principal Ideal Domain and D a multiplicatively closed subset of R, then $D^{-1}R$ is also a PID.

Solution. First we will argue that $D^{-1}R$ is an integral domain by showing it is a subring of a field. Since R is an integral domain, it is a subring of its field F of fractions. We will argue that $D^{-1}R$ is a subring of the same field F. Indeed, let $\phi : R \longrightarrow F$ be the inclusion map. By Theorem 15 on page 261 of Dummit and Foote, ϕ can be extended to an *injective* homomorphism $\Phi : D^{-1}R \longrightarrow F$, and we identify $D^{-1}R$ with its image. Since F is a field, $D^{-1}R$ is an integral domain.

We have also learned that R is isomorphic to a subring of $D^{-1}R$, and we will identify R with its image in D. Thus $D^{-1}R$ can be identified with all fractions a/d in F with $d \neq 0$.

Now let us show that every ideal I in $D^{-1}R$ is principal. Note that $I \cap R$ is an ideal of R, so $I \cap R = aR$ for some $a \in R$. Now we will argue that $I = aD^{-1}R$.

Since $a \in I$ and I is an ideal, $aD^{-1}R \subseteq I$. Conversely, let $u/d \in I$ with $u \in R$ and $d \in D$.

Since I is an ideal and $d \in R \subseteq D^{-1}R$, we have $u = d(u/d) \in I$, so $u \in I \cap R = (a)$, in other words, $u = ab$ for some b. But then $u/d = a(b/d) \in aD^{-1}R$ proving that $I \subseteq aD^{-1}R$.

We have proven that the ideal I equals $aD^{-1}R$ and so it is principal. Therefore $D^{-1}R$ is an integral domain in which every ideal is principal, that is, a PID.

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.