Mathematics 310
Robert Gross
Homework 4
Answers

1. Suppose that m, n, and k are positive integers, with $(m,n)=1$, $m|k$, and $n|k$. Prove that $mn|k$.

Answer: Because $(m,n)=1$, we can find integers x and y so that $mx+ny=1$. Multiply that equation by k, yielding $mxk+nyk=k$. We know that $m|m$ and $n|k$, so $mn|mxk$. We know that $n|n$ and $m|k$, so $mn|nyk$. Therefore, $mn|k$.

2. Suppose that G is an abelian group, with $a,b \in G$. Suppose that $o(a)=m$ and $o(b)=n$, and $(m,n)=1$. Prove that $o(ab)=mn$. *Note:* It is clear that $(ab)^{mn}=e$; the point is that you must show that no smaller exponent j satisfies $(ab)^j=e$.

Answer: Suppose that $(ab)^k=e$, with $k>0$. We need to show that $k \geq mn$. Take the equation $(ab)^k=e$, and raise both sides to the power m. We get $b^{km}=e$. We can now conclude that $n|km$. Because $(n,m)=1$, we know that $n|k$.

Similarly, take the equation $(ab)^k=e$, and raise both sides to the power n. We get $a^{kn}=e$, which implies that $m|kn$. Because $(m,n)=1$, we know that $m|k$.

We now have a situation in which $m|k$, $n|k$, and $(m,n)=1$. The previous problem now lets us conclude that $mn|k$, implying that $mn \leq k$.

3. Suppose that G is a finite abelian group, and $o(G)=p^a m$, where $p \nmid m$, $a \geq 1$, and p is a prime. Let $H=\{g \in G : g^{p^a}=e\}$.

(a) Prove that H is a subgroup of G.
(b) Prove that if $h \in H$, then the only prime that might divide $o(h)$ is p.
(c) Prove that the only prime dividing $o(H)$ is p. *Hint:* Apply Cauchy's Theorem.
(d) Show that $p \nmid o(G/H)$. *Hint:* Cauchy's Theorem says that if $p|o(G/H)$, then G/H contains a coset of order p. Now use an argument similar to the one which we used to prove Cauchy's Theorem.
(e) Show that $o(H)=p^a$.

This is a specific case of one of the Sylow Theorems, which apply to both abelian and non-abelian groups. The proof is much trickier in the case of non-abelian groups.

Answer: (a) Notice first that $e \in H$, so $H \neq \emptyset$. Now, suppose that $g,h \in H$. Then $g^{p^a}=e$ and $h^{p^a}=e$. Therefore, $(gh)^{p^a}=g^{p^a}h^{p^a}=e$, implying that $gh \in H$. We also can compute $(g^{-1})^{p^a}=(g^{p^a})^{-1}=e^{-1}=e$, so $g^{-1} \in H$. Because H is closed and contains the inverse of each element in H, we know that H is a subgroup.

(b) Suppose that $h \in H$ and q is a prime dividing $o(h)$. We know that $h^{p^a}=e$, so $o(h)|p^a$. We also know that $q|o(h)$, so we conclude that $q|p^a$. Because q and p are primes, we conclude that $q=p$. So the only prime dividing $o(h)=p$.

(c) Suppose that q is a prime dividing $o(H)$. We know by Cauchy's Theorem that H must contain an element of order q, so there is some element $h \in H$ with $o(h)=q$. Then (b) says that q must be p, and therefore $o(H)=p^b$.

(d) This is harder. Suppose that $p|o(G/H)$. Then G/H must contain a coset of order p. That means that there is some coset gH with $g \notin H$, and $(gH)^p=eH$. We know that $(gH)^p=g^pH$, so we have produced an element $g \in G$, with $g \notin H$ and $g^p \in H$.

Because $g^p \in H$, we know that $(g^p)^{p^a} \in H$, so $g^{p^{a+1}} = e$. The corollary to Lagrange's Theorem tells us that $g^{p^a m} = e$. Now, we know that $o(g)|p^{a+1}$ and $o(g)|p^a m$, so $o(g)|p^a$, because $p \nmid m$. If $o(g)|p^a$, then $g^{p^a} = e$, and then $g \in H$. This is a contradiction. The conclusion is therefore that $p \nmid o(G/H)$.

(e) This last step has nothing to do with group theory. We have a situation in which $o(G) = p^a m$, with $p \nmid m$. We know that $o(H) = p^b$, and $p \nmid o(G/H)$. Because $o(G/H) = o(G)/o(H)$, we know that $p \nmid p^a m/p^b = p^{a-b}m$. Therefore, $b = a$, so $o(H) = p^a$.

4. If $\phi : G_1 \to G_2$ is a surjective homomorphism, and $N \triangleleft G_1$, show that $\phi(N) \triangleleft G_2$. You may assume that $\phi(N)$ is a subgroup of G_2.

Answer: Take $g \in G_2$, and $n \in \phi(N)$. We must show that $gng^{-1} \in \phi(N)$.

Because ϕ is surjective, we can find $a \in G_1$ with $\phi(a) = g$. Similarly, we can find $m \in N$ with $\phi(m) = n$. Then $gng^{-1} = \phi(a)\phi(m)\phi(a)^{-1} = \phi(ama^{-1})$. Now, because $N \triangleleft G_1$, $ama^{-1} \in N$, and therefore $\phi(ama^{-1}) \in \phi(N)$. In other words, $gng^{-1} \in \phi(N)$.

5. If H is any subgroup of G, let $N(H)$ be defined by:

$$N(H) = \{a \in G \mid aH = Ha\}.$$

Prove that:

(a) $N(H)$ is a subgroup of G, and $N(H) \supset H$.

(b) $H \triangleleft N(H)$.

(c) If K is a subgroup of G such that $H \triangleleft K$, then $K \subset N(H)$.

These facts combine to tell us that $N(H)$ is the largest subgroup of G in which H is normal. The group $N(H)$ is called the *normalizer* of H.

Answer: (a) Suppose that $a, b \in N(H)$. We must show that $ab \in N(H)$ and $a^{-1} \in N(H)$. We have $(ab)H = a(bH) = a(Hb) = (aH)b = (Ha)b = H(ab)$, showing that $ab \in H$.

To show that $a^{-1} \in N(H)$, start with $aH = Ha$. Multiply on both the left and the right by a^{-1}, and we get $Ha^{-1} = a^{-1}H$, showing that $a^{-1} \in H$.

Finally, if $h \in H$, then $hH = H = Hh$, so $h \in N(H)$. This proves that $H \subset N(H)$.

(b) Now, we must show that if $h \in H$ and $n \in N(H)$, then $nhn^{-1} \in H$. We know that $nH = Hn$, and because $nh \in nH$, we know that $nh \in Hn$. Therefore, we can write $nh = h'n$ for some element $h' \in H$. Then $nhn^{-1} = (h'n)n^{-1} = h' \in H$, so $H \triangleleft N(H)$.

(c) Finally, if $H \triangleleft K$, we know that $kH = Hk$ for every $k \in K$. This shows that $k \in N(H)$ for every $k \in K$, and therefore $K \subset N(H)$.