Rebecca DeLand
Bob Kuo
Matt Watson

Group Theory
Assignment 3

1. Show that $\mathrm{Spec}_{\mathrm{Grp}}(k) = 2$ iff one the following is true.

   (a) $k = p_1 \cdots p_r$ is square-free and there is exactly one relation $p_i \mid (p_j - 1)$ among the prime divisors.

   (b) The prime factorization of k is $p_1 \cdots p_r \cdot q^2$ (exactly one exponent $\neq 1$, and that exponent is 2), and there are no relations among the primes. Here p_i or q is related to p_j means "$p_i \mid (p_j - 1)$" or "$q \mid (p_j - 1)$", while p_j is related to q^2 means "$p_j \mid (q^2 - 1)$".

Proof. '$\Rightarrow$' Suppose that $\mathrm{Spec}_{\mathrm{Grp}}(k) = 2$. Consider the prime factorization $k = p_1^{a_1} \cdots p_r^{a_r}$. First we claim that either $a_i = 1$ for all i or $a_j = 2$ for some unique j and $a_i = 1$ for all $i \neq j$. Suppose to the contrary that neither of these cases hold. Thus, there exists distinct i, j such that both $a_i \geq 2$ and $a_j \geq 2$. WLOG (up to reordering of the prime factors), suppose that $i = 1$ and $j = 2$. Then by the Structure Theorem for Abelian Groups, there exists the following three nonisomorphic abelian groups of order k,

$$G_1 = \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \mathbb{Z}_{p_3^{a_3}} \times \cdots \times \mathbb{Z}_{p_r^{a_r}},$$

$$G_2 = \mathbb{Z}_{p_1^{a_1-1}} \times \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2^{a_2}} \times \mathbb{Z}_{p_3^{a_3}} \times \cdots \times \mathbb{Z}_{p_r^{a_r}},$$

$$G_3 = \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2-1}} \times \mathbb{Z}_{p_2} \times \mathbb{Z}_{p_3^{a_3}} \times \cdots \times \mathbb{Z}_{p_r^{a_r}}.$$

But this contradicts the assumption that $\mathrm{Spec}_{\mathrm{Grp}}(k) = 2$, so we have proven the claim. Note that the first case of the claim implies that $k = p_1 \cdots p_r$ is square-free and the second case of the claim implies that $k = p_1 \cdots p_r \cdot q^2$, where $q = p_j$. Therefore we proceed in each of these cases to show that either (a) holds or (b) holds.

First consider the case when $k = p_1 \cdots p_r$. We want to show there is exactly one relation $p_i \mid (p_j - 1)$ among the prime divisors. Suppose to the contrary that either there are no relations or there is more than one relation. If there are no relations, then k is a cyclic number, so $\mathrm{Spec}_{\mathrm{Grp}}(k) = 1 \neq 2$, a contradiction. So we only need to consider the case where there is more than one relation. WLOG, suppose $p_1 \mid (p_2 - 1)$ and $p_3 \mid (p_4 - 1)$. Then there exists nontrivial actions $\alpha : \mathbb{Z}_{p_1} \to \mathrm{Aut}\,(\mathbb{Z}_{p_2 p_3 \cdots p_r})$ and $\beta : \mathbb{Z}_{p_3} \to \mathrm{Aut}\,(\mathbb{Z}_{p_1 p_2 p_4 \cdots p_r})$. So, $\mathbb{Z}_{p_2 p_3 \cdots p_r} \rtimes \mathbb{Z}_{p_1}$ and $\mathbb{Z}_{p_1 p_2 p_4 \cdots p_r} \rtimes \mathbb{Z}_{p_3}$ are nonisomorphic, nonabelian groups of order k. We have that $\mathbb{Z}_k$ is an abelian group of order k, and therefore witnesses a different isotype than the two semidirect products listed above, so $\mathrm{Spec}_{\mathrm{Grp}}(k) \geq 3$, which is a contradiction.

Now consider the case when $k = p_1 \cdots p_r \cdot q^2$. We want to show there are no relations among the prime divisors of k. WLOG (up to reordering), suppose to the contrary that either $p_1 \mid (p_2 - 1)$ or $q \mid (p_2 - 1)$ or $p_1 \mid (q^2 - 1)$. By the Structure Theorem for Abelian Groups there are two isotypes of abelian groups of order k, specifically $\mathbb{Z}_k$ and $\mathbb{Z}_{k/q} \times \mathbb{Z}_q$. So, it suffices to show in each case that there exists a nonabelian group of order k, because then $\mathrm{Spec}_{\mathrm{Grp}}(k) \geq 3$, which is a contradiction. If $p_1 \mid (p_2 - 1)$ then there exists a nontrivial action $\alpha : \mathbb{Z}_{p_1} \to \mathrm{Aut}\,(\mathbb{Z}_{p_2 p_3 \cdots p_r q^2})$, so $\mathbb{Z}_{p_2 p_3 \cdots p_r q^2} \rtimes \mathbb{Z}_{p_1}$ is a nonabelian group of order k, a contradiction. By an almost identical argument, if $q \mid (p_2 - 1)$, then a nonabelian group of order k is given by $\mathbb{Z}_{p_1 \cdots p_r q} \rtimes \mathbb{Z}_q$. If $p_1 \mid (q^2 - 1)$, then recall that $\mathrm{Aut}(\mathbb{Z}_q \times \mathbb{Z}_q) \cong \mathrm{GL}_2(\mathbb{F}_q^2)$ and $|\mathrm{GL}_2(\mathbb{F}_q^2)| = (q^2 - 1)(q^2 - q)$. So $q^2 - 1$ divides the order of $\mathrm{Aut}\,(\mathbb{Z}_{p_2 p_3 \cdots p_r q} \times \mathbb{Z}_q)$. Therefore, there exists a nontrivial action $\alpha : \mathbb{Z}_{p_1} \to \mathrm{Aut}\,(\mathbb{Z}_{p_2 p_3 \cdots p_r q} \times \mathbb{Z}_q)$, so there exists a nonabelian group of order k given by $(\mathbb{Z}_{p_2p_3\cdots p_rq}\times\mathbb{Z}_q)\rtimes\mathbb{Z}_{p_1}$. Thus we have shown that there must be no relations among the primes, so (b) holds.

'$\Leftarrow$' Let G be a group with $|G|=k$. Suppose first that (a) holds, so $k=p_1\cdots p_k$ and there is exactly one relation $p_i\mid(p_j-1)$. Since k is square free, G has cyclic Sylow subgroups, thus $G\cong\mathbb{Z}_m\rtimes\mathbb{Z}_n$ where $\gcd(m,n)=1$. Reorder the primes so that $m=p_1\cdots p_t$ and $n=p_{t+1}\cdots p_r$. Note that although we have re-indexed, we will still refer to the related primes as p_i and p_j where $p_i\mid(p_j-1)$. The structure of the semidirect product is determined by the action

$$\alpha:\mathbb{Z}_n\to\mathrm{Aut}(\mathbb{Z}_m).$$

Note that the domain has cardinality $n=p_{t+1}\cdots p_r$ and the codomain has cardinality $\phi(m)=(p_1-1)\cdots(p_t-1)$. Note that either $p_i\mid n$ or $p_i\mid m$ and either $p_j\mid n$ or $p_j\mid m$, so we consider the following four cases. If $p_i\mid n$ and $p_j\mid n$, then since no other primes are related we have that α must be the trivial action. Likewise, if $p_i\mid m$ and $p_j\mid m$, then α must be the trivial action. So in both of these cases, $G\cong\mathbb{Z}_{mn}$. If $p_i\mid m$ and $p_j\mid n$, then we still have that $\gcd(|\mathbb{Z}_n|,|\mathrm{Aut}(\mathbb{Z}_m)|)=1$, so α must be the trivial action, therefore $G\cong\mathbb{Z}_{mn}$. If $p_i\mid n$ and $p_j\mid m$, then since $p_i\mid(p_j-1)$ and there are no other relations, we have that $\gcd(|\mathbb{Z}_n|,|\mathrm{Aut}(\mathbb{Z}_m)|)=p_i$. So there exists nontrivial actions $\alpha:\mathbb{Z}_n\to\mathrm{Aut}(\mathbb{Z}_m)$ in this case. Moreover, if a nontrivial action $\alpha:\mathbb{Z}_n\to\mathrm{Aut}(\mathbb{Z}_m)$ exists, then $|\alpha(\mathbb{Z}_n)|$ must be a nonunit divisor of both $|\mathbb{Z}_n|$ and $|\mathrm{Aut}(\mathbb{Z}_m)|$. The only nonunit divisor of both $|\mathbb{Z}_n|$ and $|\mathrm{Aut}(\mathbb{Z}_m)|$ is p_i, so $|\alpha(\mathbb{Z}_n)|=p_i$. Reindex the prime divisors of k so that $n=p_1\cdots p_{j-1}$ and $m=p_j\cdots p_r$ with $p_1\mid(p_j-1)$. If the action α is trivial, we get that $G\cong\mathbb{Z}_k$ again. We will now prove the following claim:

Claim: If $\alpha_1,\alpha_2:\mathbb{Z}_n\to\mathrm{Aut}(\mathbb{Z}_m)$ are distinct nontrivial actions as described above (where $p_1|n$ and $p_j|m$ and $p_1|(p_j-1)$ is the only relation among primes), then $G\cong\mathbb{Z}_m\rtimes_{\alpha_1}\mathbb{Z}_n\cong\mathbb{Z}_m\rtimes_{\alpha_2}\mathbb{Z}_n$, in other words there is only one other possible isotype for G.

Proof of Claim: We will show that $\alpha_1(\mathbb{Z}_n)=\alpha_2(\mathbb{Z}_n)$ in $\mathrm{Aut}(\mathbb{Z}_m)$. Recall from above that $|\alpha_1(\mathbb{Z}_n)|=|\alpha_2(\mathbb{Z}_n)|=p_1$. We will first show that $\mathrm{Aut}(\mathbb{Z}_m)$ has a cyclic subgroup of order p_j-1. Note that $\mathrm{Aut}(\mathbb{Z}_m)\cong\mathrm{Aut}\left(\mathbb{Z}_{p_j}\times\cdots\times\mathbb{Z}_{p_r}\right)$. Choose g to be any generator of the cyclic group $\left(\mathbb{Z}_{p_j}\right)^\times$. Note that $p_j\neq2$ since $p_1\mid p_2-1$, so if $p_j=2$, then $p_1=1$, which is not prime. Since $p_j\neq2$ there exists nontrivial $\varphi\in\mathrm{Aut}\left(\mathbb{Z}_{p_j}\times\cdots\times\mathbb{Z}_{p_r}\right)$ defined by $\varphi(a_{p_j},a_{p_{j+1}},\ldots,a_{p_r})=(ga_{p_j},a_{p_{j+1}},\ldots,a_{p_r})$. We then have that $\varphi^k(a_{p_j},a_{p_{j+1}},\ldots,a_{p_r})=(g^ka_{p_j},a_{p_{j+1}},\ldots,a_{p_r})$. $\varphi^k=id$ if and only if $g^ka\equiv a\mod p_j$ for all $a\in\mathbb{Z}_{p_j}$ if and only if $a(g^k-1)\equiv0\mod p_j$. Since $\mathbb{Z}_{p_j}$ is an integral domain and a is not always 0, we have that $g^k\equiv1\mod p_j$. By the fact that g is a generator of $\left(\mathbb{Z}_{p_j}\right)^\times$, we have that the least value k so that $\varphi^k=id$ is $k=p_j-1$. Therefore, φ is an element of order p_j-1, so $\mathrm{Aut}\left(\mathbb{Z}_{p_j\cdots p_r}\right)$ has a cyclic subgroup of order p_j-1. Call this subgroup K.

Next, note that $p_1\mid p_j-1$ so we can consider the p_1-Sylow subgroup P of $\mathrm{Aut}\left(\mathbb{Z}_{p_j\cdots p_r}\right)$ (the Sylow subgroup is unique since the automorphism group is abelian). P has order p_1^k and we will show that $P\subset K$. Since $p_1\mid p_j-1$, by Cauchy's Theorem K has a subgroup of order p_1. This subgroup is contained in a Sylow p_1-subgroup, and hence contained in P, so $|P\cap K|\geq p_1$. Suppose $P\not\subset K$, then $|P\cap K|=p_1^a$, $1\leq a<k$. Consider the subgroup PK

of Aut $\left(\mathbb{Z}_{p_j\cdots p_r}\right)$. We have that

$$|PK| = \frac{|P||K|}{|P\cap K|} = (p_j - 1)p_1^{k-a}.$$

By Lagrange's Theorem, $(p_j-1)p_1^{k-a} \mid (p_j-1)\cdots(p_r-1)$, therefore $p_1^{k-a} \mid (p_{j+1}-1)\cdots(p_r-1)$. Since $1 \le k-a < k$ and p_1 is prime, $p_1 \mid (p_i-1)$ for some $j+1 \le i \le r$, which is a contradiction since this is a new relation on the primes. Thus, $P \subset K$. So P must be cyclic and therefore contains a unique cyclic subgroup of order p_1. Any other cyclic subgroup of Aut $\left(\mathbb{Z}_{p_j\cdots p_r}\right)$ of order p_1 would be contained in P. Thus, Aut $\left(\mathbb{Z}_{p_j\cdots p_r}\right)$ has a unique cyclic group of order p_1 so $\alpha_1(\mathbb{Z}_n) = \alpha_2(\mathbb{Z}_n)$. The original claim about semi-direct products then immediately follows from the result of Exercise 6 in Section 5.5 of Dummit and Foote. $\Box$Claim.

In all cases, the only possible isotypes for G were the cyclic group of order k or $\mathbb{Z}_m \rtimes_\alpha \mathbb{Z}_n$. Therefore, we have shown that (a) implies $\mathrm{Spec}_{\mathrm{Grp}}(k) = 2$.

Now suppose (b) holds. So $k = p_1\cdots p_r \cdot q^2$ with no relations. We claim that any group G with $|G| = k = p_1\cdots p_r\cdot q^2$ with no relations is abelian. We proceed by induction on r. If $r = 0$, then $k = q^2$, so G is abelian. Suppose now that for some arbitrary $r \ge 0$, we have that if k has r linear prime factors and exactly one square factor (k is of the form $k = p_1\cdots p_r\cdot q^2$) with no relations and G is a group with $|G| = k$, then G is abelian. Consider an arbitrary k of the form $k = p_1\cdots p_r\cdot p_{r+1}q^2$ and let G be a group of order k. Let P be a Sylow p_1-subgroup of G. We will show that P has a normal complement. Note first that $P \cong \mathbb{Z}_{p_1}$ is abelian. By Burnside's Normal Complement Theorem, it suffices to show that $N_G(P) = C_G(P)$. We know that $N_G(P)$ acts on P by conjugation. In other words, there exists a homomorphism $\alpha : N_G(P) \to \mathrm{Aut}(P) \cong \mathbb{Z}_{p_1-1}$ defined as $g \mapsto \alpha(g) : P \to P$ via $\alpha(g)(x) = g^{-1}xg$. Notice that $\ker(\alpha) = C_G(P)$ ($g \in \ker(\alpha) \Leftrightarrow \alpha(g)(x) = x$ for all $x \in P \Leftrightarrow g^{-1}xg = x$, $x \in P \Leftrightarrow gx = xg, x \in P \Leftrightarrow g \in C_G(P)$). Suppose for a contradiction that $N_G(P) \neq \ker(\alpha)$. So we can choose $g \in N_G(P)\backslash\ker(\alpha)$. So, $|\alpha(g)|$ divides p_1-1 and $|\alpha(g)| \neq 1$. But, $|\alpha(g)| \mid |g|$ and $|g| \mid k$ since $g \in G$. So $|\alpha(g)| \mid k$, hence $|\alpha(g)| = p_1^{a_1}\cdots p_r^{a_r}\cdot p_{r+1}^{a_{r+1}}\cdot q^b$ where $a_j \in \{0,1\}$ and $b \in \{0,1,2\}$. Since $|\alpha(g)| \mid (p_1-1)$, p_1 does not divide p_1-1, and $|\alpha(g)| \neq 1$, it must be the case that some $a_i = 1$ with $i \neq 1$ or $b \neq 0$. In either case since $|\alpha(g)| \mid (p_1-1)$, we then have that either some $p_i \mid (p_1-1)$ or $q \mid (p_1-1)$, which is a contradiction in either case to the fact that there are no relations among the primes. Therefore $N_G(P) = \ker(\alpha) = C_G(P)$. So by Burnside's Normal Complement Theorem, P has a normal complement which we will call N. So we have that $G \cong N \rtimes P$. Since N is a group of order $p_2\cdots p_r\cdot p_{r+1}q^2$ with no relations among the primes, by the inductive hypothesis N is abelian. So $N \cong \mathbb{Z}_{p_2\cdots p_{r+1}\cdot q^2}$ or $N \cong \mathbb{Z}_{p_2\cdots p_{r+1}\cdot q}\times\mathbb{Z}_q$. If $N \cong \mathbb{Z}_{p_2\cdots p_{r+1}\cdot q^2}$, then P can only act trivially on N since $|P| = p_1$ and $|\mathrm{Aut}(N)| = (p_2-1)\cdots(p_r-1)(p_{r+1}-1)q(q-1)$ so the existence of a nontrivial action would imply that p_1 divides some p_j-1 or $q-1$ (p_1 cannot divide q since q is prime and $p_1 \neq q$), which contradicts the assumption that there are no relations. If $N \cong \mathbb{Z}_{p_2\cdots p_{r+1}\cdot q}\times\mathbb{Z}_q$, then $\mathrm{Aut}(N) \cong \left(\mathbb{Z}_{p_2\cdots p_{r+1}}\right)^\times \times \mathrm{GL}_2(\mathbb{F}_q)$, so $|\mathrm{Aut}(N)| = (p_2-1)\cdots(p_{r+1}-1)\cdot(q^2-1)q(q-1)$. The existence of a nontrivial action of P on $\mathrm{Aut}(N)$ would imply that p_1 divides some p_j-1 or $q-1$ or q^2-1, which is a contradiction in all cases. Therefore, $G \cong N \times P$. So G is the product of two abelian groups and so G is abelian. By the principle of mathematical induction, we have shown that for any $r \ge 0$, if $k = p_1\cdots p_r\cdot q^2$ with no relations among the

Rebecca DeLand
Bob Kuo
Matt Watson

primes, then any group of order k is abelian. By the Structure Theorem for Abelian Groups, $\mathrm{Spec}_{\mathrm{Grp}}(k) = 2$ (the only possible isotypes for G are given by $\mathbb{Z}_k$ and $\mathbb{Z}_{k/q} \times \mathbb{Z}_q$). $\square$