Math 504, Fall 2013
HW 6

1. Let p be a prime number and G a non-abelian group with p^3 elements.

(a) Show that $Z(G) \cong \mathbb{Z}_p$ and that $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

(b) Show that every subgroup of G having p^2 elements contains $Z(G)$ and is a normal subgroup of G.

(c) Show that G has a normal subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ if $x^p = 1$ for all $p \in G$.

(a) By Corollary 4.38 of Knapp, $Z(G)$ is nontrivial. Since G is nonabelian, $|Z(G)| < p^3$. By Lagrange's theorem, $Z(G)$ must either be of order p or p^2. Suppose for contradiction that $|Z(G)| = p^2$. Choose $x \in G \setminus Z(G)$. Then $Z(x) := \{g \in G : gxg^{-1} = x\}$ is a subgroup of G that contains $Z(G)$, hence $Z(x) = G$, which contradicts the fact that $x \notin Z(G)$.

We conclude that $|Z(G)| = p$ and hence by Lagrange's theorem, $Z(G) \cong \mathbb{Z}_p$.

It follows that $H := G/Z(G)$ is a group of order p^2. But from Corollary 4.39 of Knapp (which is the same argument as the one we used to show that $|Z(G)| < p^2$), all such groups are abelian. By the fundamental theorem of abelian groups, either $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$ or $H \cong \mathbb{Z}_{p^2}$. Suppose for contradiction that $H \cong \mathbb{Z}_{p^2}$. Choose $x \in G \setminus Z(G)$ such that the image of x in $G/Z(G)$ generates $G/Z(G)$. Then

$$Z(G) \cup xZ(G) \cup x^2 Z(G) \cup \cdots \cup x^{p^2-1} Z(G)$$

is a partition of G. In other words every pair of elements $g, h \in G$ can be written as $g = x^j y$ and $h = x^i z$ for some integers i, j and some $y, z \in Z(G)$. Then $gh = x^{j+i} zy = hg$, so G is abelian, contradiction.

(b) Suppose $A \leq G$ is a subgroup with p^2 elements. By Proposition 4.36 of Knapp, A is normal, so the conjugation action of G on G restricts to an action of G on A. The fixed points of this action are precisely the elements of $Z(G) \cap A$. By the orbit-stabilizer theorem, the size of the orbit of each non-fixed point is a non-unit divisor of p^2. In particular it is a multiple of p. Thus $|A \setminus (Z(G) \cap A)|$ is divisible by p. Since $|A|$ is divisible by p it follows that $|Z(G) \cap A|$ is divisible by p. Since $|Z(G) \cap A| \neq 0$ and $|Z(G)| = p$ it follows that $|Z(G) \cap A| = p$ and hence $Z(G) \subset A$.

(c) By the Sylow theorems, G has a subgroup B of order p^2. So $B \cong \mathbb{Z}_p^2$ or $B \cong \mathbb{Z}_{p^2}$. But by assumption B cannot have an element of order p^2, so $B \cong \mathbb{Z}_p^2$.

∎

2. (Knapp, 4.42) Suppose that G is a nonabelian group of order 8 Prove that G has an element of order 4 but no elements of order 8.

The orders of non-trivial elements of G are in $\{2,4,8\}$. If 8 was attained, then G would be cyclic, a contradiction. If all elements had order 2, then $1 = x^2y^2 = (xy)^2$ implies $xy = yx$ after cancellation, so G would be abelian, contradiction. Thus G has an element of order 4, but no element of order 8. ■

3. (Knapp, 4.43) Let G be a nonabelian group of order 8, and let K be the copy of C_4 generated by some element of order 4. If G has some element of order 2 that is not in K, prove that $G \cong D_4$.

First note that K is normal in G because its index in G is 2, the smallest prime dividing the order of G. Now let $h \in G$ be an element of order 2 that is not in K. Then the product subgroup $\langle h \rangle$ must be all of G and, a priori, the two subgroups have trivial intersection. By the theorem on recognizing semidirect products, this is enough information to conclude that G is of the form $K \rtimes_\phi \langle h \rangle$ with ϕ some homomorphism from $\langle h \rangle$ to $\operatorname{Aut} K$. ■

4. (Knapp, 4.44) Let G be a nonabelian group of order 8, and let K be the copy of C_4 generated by some element of order 4. If G has no element of order 2 that is not in K, prove that $G \cong H_8$.

Let i be a generator of K. Then $i^2 =: -1$ has order 2, and $i^3 = -1 \cdot i^2 = i^2 \cdot (-1) =: -i$ also has order 4. Thus $K = \{1, i, -1, -i\} = \langle i \rangle$. By Problem 1a, $Z(G)$ is a two-element subgroup of K, and thus $Z(G) = \{1, -1\}$. Let $j \in G \backslash K$. Then by assumption j has order 4, and so $Z(G) \subset \langle j \rangle$ and we find as above that $\langle j \rangle = \{1, j, -1, -j\}$. Since $j \notin \langle i \rangle$, $i \notin \langle j \rangle$, and so $\langle i \rangle \cap \langle j \rangle = \{1, -1\}$. Define $k := ij$. Then $k \notin \langle i \rangle$ since $j \notin \langle i \rangle$, and similarly $k \notin \langle j \rangle$, and so k has order 4, $Z(G) \subset \langle k \rangle$, and thus $\langle k \rangle = \{1, k, -1, -k\}$. Similarly, $ji \notin \langle i \rangle$ and $ji \notin \langle j \rangle$, and so ji has order 4, showing $ji \in \{k, -k\}$. If $ji = k = ij$, then since $G = \langle i \rangle \cup j\langle i \rangle$, G would be commutative, and so $ji = -k$.

All the relationships in G are now determined. From $ij = k$ we see $ijk = k^2 = -1$, so

$$jk = (-i)ijk = (-i)(-1) = i$$

and by the commutativity argument $kj = -i$. Similarly, $jk = i$ implies $ki = j$ and $ik = -j$. We therefore see that the elements of $G = \langle i \rangle \cup \langle j \rangle \cup \langle k \rangle$ have precisely the same relationships as those of the quaternion group H_8, showing $G \cong H_8$.

■

In the following problems, p, q are two distinct prime numbers.

5. (Knapp, 4.50) If p^2 divides $q - 1$, exhibit three nonabelian groups of order p^2q that are mutually nonisomorphic.

We let $H \cong \mathbb{Z}_{p^2}$ and $K \cong \mathbb{Z}_q$. We let g generate H and b generate $\operatorname{Aut} K \cong Z_{q-1}$. Then we define an automorphism $\phi_1 : H \to \operatorname{Aut} K$ mapping $g \mapsto b^{(q-1)/p^2}$. Then we define the semidirect product $G_1 = K \rtimes_{\phi_1} H$. G_1 clearly has order p^2q, we show that G_1 is nonabelian group. First we notice that since $p^2|q-1$, then $(q-1)/p^2 < q-1$ so that $\phi_1(g) \neq Id$ because b has order $q-1$. Therefore for any nonidentity $k \in K$, $k^{\phi_1(g)} \neq k$. Then $(k,1)(1,g) = (k1^{\phi_1(g)}, g) = (k,g)$. But $(1,g)(k,1) = (k^{\phi_1(g)}, g) \neq (k,g)$, so G_1 is not abelian.

The next example is very similar to the last. We let $H \cong \mathbb{Z}_{p^2}$ and $K \cong \mathbb{Z}_p$. We let g generate H and b generate $\operatorname{Aut} K \cong Z_{q-1}$. Then we define an automorphism $\phi_2 : H \to \operatorname{Aut} K$ mapping $g \mapsto b^{(q-1)/p}$. Then we define the semidirect product $G_2 = K \rtimes_{\phi_2} H$. G_2 clearly has order p^2q, we show that G_2 is nonabelian group. First we notice that since $p|q-1$, then $(q-1)/p < q-1$ so that $\phi_2(g) \neq Id$ because b has order $q-1$. Therefore for any nonidentity $k \in K$, $k^{\phi_2(g)} \neq k$. Then $(k,1)(1,g) = (k1^{\phi_2(g)}, g) = (k,g)$. But $(1,g)(k,1) = (k^{\phi_2(g)}, g) \neq (k,g)$, so G_2 is not abelian.

We next show $G_1 \ncong G_2$. First we consider $k \in K$ and $h \in H$, where $h = g^t$ for some $t < p^2$. Thus $t(q-1)/p^2 < p^2(q-1)/p^2 = q-1$, so that $\phi_1(h) \neq Id$ and thus $k^{\phi_1(h)} \neq k$. Then $(k,1)(1,h) = (k,h)$. But $(1,h)(k,1) = (k^{\phi_1(h)}, h) \neq (k,h)$. So multiplying an element of order p or p^2 with one of order q in G_1 will never commute.

Since an isomorphism must preserve order and commutativity, if G_2 were isomorphic it would also have this property. But we will exhibit an element of order q and one of order p that do commute in G_2, thus showing these groups are not isomorphic. Let $h = g^p \in H$ and $k \in K$ with $k \neq 1$. Then $\phi_2(h) = b^{p(q-1)/p} = b^{q-1} = Id$. We see that $(k,1)(1,h) = (k,h)$ and also $(1,h)(k,1) = (k^{\phi_2(h)}, h) = (k,h)$. Therefore $G_1 \ncong G_2$.

The third example is also very similar to the last 2. We let $H \cong \mathbb{Z}_p \times \mathbb{Z}_p$ and $K \cong \mathbb{Z}_p$. We let $H = \langle g_1, g_2 \rangle$ and b generate $\operatorname{Aut} K \cong Z_{q-1}$. Then we define an automorphism $\phi_3 : H \to \operatorname{Aut} K$ mapping $g_i \mapsto b^{(q-1)/p}$ for $i = 1,2$. Then we define the semidirect product $G_3 = K \rtimes_{\phi_3} H$. G_3 clearly has order p^2q, we show that G_3 is nonabelian group. First we notice that since $p|q-1$, then $(q-1)/p < q-1$ so that $\phi_3(g_i) \neq Id$ for $i = 1,2$ because b has order $q-1$. Therefore for any nonidentity $k \in K$, $k^{\phi_2(g_i)} \neq k$. Then $(k,1)(1,g_i) = (k1^{\phi_2(g_i)}, g_i) = (k, g_i)$. But $(1,g_i)(k,1) = (k^{\phi_2(g_i)}, g) \neq (k, g_i)$, so G_3 is not abelian.

Moreover, G_3 is not isomorphic to either G_1 or G_2 because it has no elements of order p^2. ■

6. (Knapp, 4.51) If p divides $q-1$ but p^2 does not divide $q-1$, exhibit two nonabelian groups of order p^2q that are not isomorphic.

In fact, G_2 and G_3 from examples 0.2 and 0.3 never rely on the fact that $p^2|q$, just that p does, and therefore would also work in these cases. The construction, argument for them begin nonabelian, and the fact that they are not isomorphic is exactly the same. ■

7. (Knapp, 4.53) This problem is about constructing nonabelian groups of order 27.

(a) Show that multiplication by the elements $1, 4, 7 \bmod 9$ defines a nontrivial action of $\mathbb{Z}_3$ on $\mathbb{Z}_9$ by automorphisms.

(b) Show from (a) that there exists a nonabelian group of order 27.

(c) Show that the group in (b) is generated by elements a and b that satisfy

$$a^9 = b^3 = b^{-1}aba^{-4} = 1.$$

(a) Multiplication by 1 is the identity mapping on $\mathbb{Z}_9$, and the mappings $(1 \mapsto 4), (1 \mapsto 7)$ are automorphisms of $\mathbb{Z}_9$, because $\gcd(4,9) = \gcd(7,9) = 1$, so $4, 7$ are units mod 9 (in fact they are multiplicative inverses). Recall that $(1 \mapsto 4)(a) = 4a, (1 \mapsto 7)(a) = 7a$, so these automorphisms are, in fact multiplication by $1, 4, 9$.

Let $\phi : \mathbb{Z}_3 \to \operatorname{Aut}(\mathbb{Z}_9)$ be given by:

$$\phi(0) = (1 \mapsto 1), \qquad \phi(1) = (1 \mapsto 7), \qquad \phi(2) = (1 \mapsto 4)$$

It's clear that $\phi(0)$ is the identity mapping on $\operatorname{Aut}(\mathbb{Z}_9)$. Furthermore:

$$\phi(1)\phi(1) = (1 \mapsto 7)(1 \mapsto 7) = (1 \mapsto 49) \equiv (1 \mapsto 4) = \phi(2) = \phi(1+1)$$

$$\phi(1)\phi(2) = (1 \mapsto 7)(1 \mapsto 4) = (1 \mapsto 28) \equiv (1 \mapsto 1) = \phi(0) = \phi(1+2)$$

$$\phi(2)\phi(2) = (1 \mapsto 4)(1 \mapsto 4) = (1 \mapsto 16) \equiv (1 \mapsto 7) = \phi(1) = \phi(2+2)$$

Both groups are abelian, so this shows explicitly that the group operation is preserved. Thus, ϕ is a group homomorphism from $\mathbb{Z}_3$ to $\operatorname{Aut}(\mathbb{Z}_9)$, so multiplication by $1, 4, 7$ defines a nontrivial action of $\mathbb{Z}_3$ on $\mathbb{Z}_9$ by automorphisms.

(b) Let ϕ be as above, and let $G = \mathbb{Z}_9 \rtimes_\phi \mathbb{Z}_3$. Then $|G| = |\mathbb{Z}_9||\mathbb{Z}_3| = 9 \cdot 3 = 27$, and G is nonabelian since ϕ is not trivial.

(c) We can obviously take $a = (1,0)$, $b = (0,1)$, since $a^9 = b^3 = (0,0)$. It remains to show that $b^{-1}aba^{-4} = (0,0)$, or, alternatively, that $b^{-1}ab = a^4$. Compute:

$$\begin{aligned} b^{-1}ab &= (0,2)(1,0)(0,1) \\ &= (\Phi(2)(1), 2)(0,1) = (4,2)(0,1) \\ &= (4 + \Phi(2)(0), 3) = (4,0) = a^4 \end{aligned}$$

∎

8. (Knapp, 4.54) Show that any nonabelian group of order 27 having a subgroup H isomorphic to C_9 and an element of order 3 not lying in H is isomorphic to the group constructed in the previous problem.

Let G be any nonabelian group of order 27 and assume G has a subgroup H isomorphic to C_9 and an element of order 3 not lying in H. From problem 1(b), we have $C_9 \trianglelefteq G$, so we need only check that $N \cap H = \{e\}$, where N denotes the subgroup generated by the element $x \notin H$ of order 3. But this reduces to verifying that $y^2 \notin \langle x \rangle$. Since y has order 3, y^2 also has order 3. There are only two elements in C_9 of order 3: x^3 and x^6 since $9 = 3^2$. In either case, if $y^2 = x^3$, then multiplying both sides by y gives $1 = yx^3$, whence $y \in C_9$, a contradiction. Similarly, if $y^2 = x^6$, then $1 = yx^6$, and we again have a contradiction. Thus we are justified in forming the semi direct product $C_9 \rtimes_\varphi C_3$, where $\varphi : C_3 \to \text{Aut}\,(C_9)$ is a group homomorphism. We must have a nontrivial group homomorphism in order for the semi direct product to not be a direct product, and hence abelian, so we show first there are two possibilities and next that they result in isomorphic groups (both of which necessarily must be isomorphic to the group constructed in the previous problem). We know from elementary group theory that $\text{Aut}\,(C_9) \simeq (\mathbb{Z}/9\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z}$, so we just see what elements of order 3 are in $\mathbb{Z}/6\mathbb{Z}$ (or in $(\mathbb{Z}/9\mathbb{Z})^\times$). We therefore have two nontrivial homomorphisms, one sending the generator $1 \mapsto 4$ and the other sending $1 \mapsto 7$, where the maps are into the group of units of $\mathbb{Z}/9\mathbb{Z}$. These are the only elements with order 3, and they give rise to nontrivial homomorphisms by multiplication. But relabeling, we have two homomorphisms $\varphi_i : C_3 \to \text{Aut}\,(C_9), i = 1, 2$ where $\varphi_1(1) = \psi_4$ and $\varphi_2(1) = \psi_7$, which we recognize from the previous problem. But noting that $\varphi_1(2) = \psi_4^2 = \psi_7$ and that $\varphi_2(2) = \psi_7^2 = \psi_4$, we see that the two groups constructed are isomorphic by proposition 2.2 in the class notes (just take the automorphism of C_3 to be multiplication by 2). ∎