Math 30810 Honors Algebra 3
Homework 8

Andrei Jorza

Due at noon on Thursday, October 27

Do 8 of the following questions. Some questions are obligatory. Artin a.b.c means chapter a, section b, exercise c. You may use any problem to solve any other problem.

1. (You have to do this problem) A **short exact sequence** of groups is a sequence of group homomorphisms
$$1 \to N \xrightarrow{f} G \xrightarrow{g} K \to 1$$
such that $f : N \to G$ is injective, $g : G \to K$ is surjective, and $\operatorname{Im} f = \ker g$. A **section** of such an exact sequence is defined to be a group homomorphism $s : K \to G$ such that $g \circ s = \mathrm{id}_K$.

   (a) Show that in the short exact sequence above $N \cong f(N) \lhd G$ and $G/f(N) \cong K$.

   (b) Suppose that the exact sequence above admits a section $s : K \to G$. Show that for every $x \in G$ one can find $n \in N$ such that $x = f(n)s(g(x))$ and deduce that $G \cong N \rtimes K$ is a semidirect product.

   (c) (Extra credit) Show that if $G \cong N \rtimes K$ then one can find an exact sequence $1 \to N \to G \to K \to 1$ that admits a section $s : K \to G$.

   Proof. (a): Since f is injective we have $N \cong Nf(N)$. Since $f(N) = \ker g$ it follows that $f(N) = \ker g \lhd G$. Finally the 1st isomorphism theorem gives $K = \operatorname{Im} g \cong G/\ker g = G/f(N)$.

   (b): Note that $x = f(n)s(g(x))$ for some $n \in N$ if and only if $xs(g(x))^{-1} \in \operatorname{Im} f$. But $\operatorname{Im} f = \ker g$ so it's enough to check that $xs(g(x))^{-1} \in \ker g$: indeed $g(xs(g(x))^{-1}) = g(x)g(s(g(x)))^{-1} = g(x)g(x)^{-1} = 1$ as $g \circ s = \mathrm{id}_K$.

   Define $H = s(K)$ and $N' = f(N) \cong N$ as in part (a). Since $g \circ s = \mathrm{id}_K$ it follows that s is injective and so $H \cong K$ via s. We'll check that $G \cong N' \rtimes H \cong N \rtimes K$. From part (a) we know that $N' \lhd G$. If $x \in N' \cap H$ then $x = s(k)$ for some $k \in K$ and $x = f(n)$ for some $n \in N$. Thus $g(x) = g(f(n)) = 1$ but $g(x) = g(s(k)) = k$. We deduce that $k = 1$ and so $x = s(1) = 1$. Therefore $N' \cap H = 1$. Finally, we already know that $x = f(n)s(g(x))$ for some $n \in N$ and so $G = N'H$. The criterion from class now implies that $G \cong N' \rtimes H \cong N \rtimes K$ as desired.

   (c): If $G \cong N \rtimes K$ then from class the map $f(n) = (1, n)$ gives an injection $N \hookrightarrow G$ and the map $s(k) = (k, 1)$ gives an injection $K \hookrightarrow G$. Finally the map $g((k, n)) = k$, again from class, is a surjective homomorphism $G \to K$ with kernel $N = \operatorname{Im} f$. This means that $1 \to N \xrightarrow{f} G \xrightarrow{g} K \to 1$ is an exact sequence and visibly $g \circ s = \mathrm{id}_K$ so s is a section. □

2. Recall from class[1] that the matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ generate $\mathrm{SL}(2, \mathbb{Z})$.

[1] Actually in class I showed this with the inverse of the matrix S, but this is the more standard version of S

(a) Show that $\mathrm{SL}(2,\mathbb{Z}) = \langle S, ST\rangle$ and that the two generators S and ST have orders 4 respectively 6.

(b) (Do either this or the next part) Show that the only homomorphism $f : \mathrm{SL}(2,\mathbb{Z}) \to \mathbb{Z}/7\mathbb{Z}$ is the trivial homomorphism. [Hint: It's enough to see where the generators go.]

(c) (Do either this or the previous part) Show that every homomorphism $f : \mathrm{SL}(2,\mathbb{Z}) \to \mathbb{C}^\times$ has image $\operatorname{Im} f \subset \mu_{12} = \{z \in \mathbb{C}^\times \mid z^{12} = 1\}$.

Proof. (a): Let $R = ST$. Then $\langle S, R\rangle$ is clearly $\subset \langle S, T\rangle = \mathrm{SL}(2,\mathbb{Z})$. Viceversa, $T = S^{-1}R$ so again $\mathrm{SL}(2,\mathbb{Z}) = \langle S, T\rangle = \langle S, S^{-1}R\rangle \subset \langle S, R\rangle$. Finally, $S^2 = -I_2$ and $R = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, $R^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$, $R^3 = -I_2$ and so S has order 4 and R has order 6.

(b): If f is a homomorphism then $4f(S) = f(S^4) = 0$ and $6f(R) = f(R^6) = 0$ in $\mathbb{Z}/7\mathbb{Z}$. But 4 and 6 are invertible mod 7 so $f(R) = f(S) = 0$ and we conclude that $f = 0$.

(c): As above $f(S)^4 = 1$ and $f(R)^6 = 1$ and so $f(R), f(S) \in \mu_{12}$ which implies that $\operatorname{Im} f \subset \mu_{12}$. □

3. Let $\zeta = e^{2\pi i/3}$, $x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $y = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$. Let $G = \langle x, y\rangle \subset \mathrm{GL}(2,\mathbb{C})$ be the subgroups generated by x and y.

   (a) Show that x has order 4, y has order 3 and $xy = y^2 x$.

   (b) Show that G has order 12 with $G = \{y^b x^a \mid 0 \le a < 4, 0 \le b < 3\}$.

   (c) Show that $G \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z}$ for some $\phi : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$. [Hint: Use the criterion for when a group is a semidirect product.]

Proof. (a): Compute $x^2 = -I_2$, $y^3 = I_2$ to conclude that x has order 4 and y has order 3. Also $xy = \begin{pmatrix} & -\zeta^{-1} \\ \zeta & \end{pmatrix}$ and $y^2 x = \begin{pmatrix} & -\zeta^2 \\ \zeta^{-2} & \end{pmatrix} = xy$ as $\zeta^{-1} = \zeta^2$.

(b): Using $xy = y^2 x$, $x^{-1} = x^3$ and $y^{-1} = y^2$ one can write any product in $\langle x, y\rangle$ as a power $y^b x^a$ with $0 \le b < 3$ and $0 \le a < 4$, simply by putting all y-s on the left and all x-s on the right. It suffices to check that these are all distinct. But if $y^b x^a = y^{b'} x^{a'}$ then $y^{b-b'} = x^{a'-a}$ and this cannot be unless $b \equiv b' \pmod 3$ and $a \equiv a' \pmod 4$ as otherwise $b - b'$ is coprime to 3 so the LHS has order 3 while the RHS has order dividing 4.

(c): Let $N = \langle y\rangle \subset G$. Since $xyx^{-1} = y^2$ it follows that $N \lhd G$. Moreover, $H \cong \mathbb{Z}/3\mathbb{Z}$. Let $H = \langle x\rangle \subset G$, $H \cong \mathbb{Z}/4\mathbb{Z}$. As N and H have coprime orders, $N \cap H = 1$ and from part (b) $G = NH$. Thus $G \cong N \rtimes H \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$. □

4. Consider the homomorphism $\phi : S_3 \to \mathrm{Inn}(S_3) = \mathrm{Aut}(S_3)$ defined by $\phi_g(x) = gxg^{-1}$. Consider the groups $G_0 = S_3 \rtimes_\phi S_3$, $G_1 = S_3 \rtimes_\phi A_3$ and $G_2 = A_3 \rtimes_\phi A_3$.

   (a) Show that $G_2 \cong (\mathbb{Z}/3\mathbb{Z})^2$ [Hint: $A_3 \cong \mathbb{Z}/3\mathbb{Z}$],

   (b) Show that $G_2 \lhd G_1$ with $G_1/G_2 \cong \mathbb{Z}/2\mathbb{Z}$,

   (c) Show that $G_1 \lhd G_0$ with $G_0/G_1 \cong \mathbb{Z}/2\mathbb{Z}$.

   [Hint: To show normality you can use a criterion from a previous problem set. No need to do any conjugation.]

Proof. This problem looks harder than it is. Recall from a previous homework that if H is an index 2 subgroup of a group G then $H \lhd G$.

(a): We have $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ so $G_2 = A_3 \rtimes A_3 \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$. But in class we showed that $\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/n\mathbb{Z}$ when m is coprime to $\varphi(n)$ and the result follows by applying this to $m = n = 3$.

(b): Since A_3 has index 2 in S_3 it follows that $A_3 \rtimes A_3$ has index 2 in $S_3 \rtimes A_3$ so G_2 has index 2 in G_1 which implies normality. Then G_1/G_2 has order 2 so it is $\mathbb{Z}/2\mathbb{Z}$.

(c): Again $G_1 = S_3 \rtimes A_3$ has order 2 in $G_0 = S_3 \rtimes S_3$ so $G_1 \lhd G_0$ and the quotient is $\mathbb{Z}/2\mathbb{Z}$. $\square$

5. Show that S_n is generated by the transpositions (12), (23), …, $(n-1, n)$. [Hint: $(23)(12)(23) = (13)$. Recall that in class we showed that S_n is generated by all transpositions.]

Proof. It suffices to check that every transposition (ij) is in the group G generated by $(12), (23), (34), \ldots$ because S_n is generated by all transpositions. We'll prove this by induction on $j - i$. When $j - i = 1$ then $(ij) \in G$ by assumption, this is the base case. Now suppose $(ij) \in G$. Then so is

$$(j, j+1)(i, j)(j, j+1) = (i, j+1) \in G$$

$\square$

6. (a) Show that $(12 \ldots n)(i, i+1)(12 \ldots n)^{-1} = (i+1, i+2)$ for $i + 2 \leq n$.
   (b) Show that $(12 \ldots n)^k (12)(12 \ldots n)^{-k} = (k+1, k+2)$ for $k + 2 \leq n$.
   (c) Deduce that S_n is generated by (12) and $(12 \ldots n)$. [Hint: Use the previous problem.]

Proof. (a): Write τ for the cycle. $i+1$ is mapped to i by τ^{-1}, to $i+1$ by the transposition then to $i+2$ by τ. $i+2$ is mapped to $i+1$ by τ^{-1} then to i by the transposition then to $i+1$ by τ. Finally if $j \neq i+1, i+2$ then j is mapped to $j-1$ by τ^{-1}, is fixed by the transposition and is mapped back to j by τ.

(b): An immediate induction.

(c): The subgroup of S_n generated by (12) and $(12 \ldots n)$ contains, by part (b), all transpositions $(k, k+1)$ and so by the previous problem it is S_n. $\square$

7. Consider $\mathbb{Q}$ as a group with respect to $+$. Show that every finitely generated subgroup of $\mathbb{Q}$ is of the form $q\mathbb{Z}$ for some rational $q \in \mathbb{Q}$. In other words, every finitely generated subgroup is cyclic so generated by one single element.

Proof. If $G = \langle \frac{m_1}{n_1}, \ldots, \frac{m_k}{n_k} \rangle \subset \mathbb{Q}$ is finitely generated then $G = \{\frac{m_1 a_1}{n_1} + \cdots + \frac{m_k a_k}{n_k} \mid a_i \in \mathbb{Z}\}$ and so clearing denominators $G \subset \frac{1}{N}\mathbb{Z}$ where $N = [n_1, n_2, \ldots, n_k]$. As a group $\frac{1}{N}\mathbb{Z} \cong \mathbb{Z}$ and we know that every subgroup of $\mathbb{Z}$ is of the form $M\mathbb{Z}$ and so $G = \frac{M}{N}\mathbb{Z}$ as desired. $\square$

8. Let $G = \left\langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \subset \mathrm{GL}(2, \mathbb{R})$ and let $H < G$ be the subgroup of G consisting of those matrices with 1-s on the diagonal. Show that H is not finitely generated, i.e., there don't exist finitely many matrices $g_1, \ldots, g_n \in H$ such that $H = \langle g_1, g_2, \ldots, g_n \rangle$. [Hint: Show that H is a subgroup of $\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{Q} \right\} \cong \mathbb{Q}$, but H contains matrices where the upper right corner is a rational with arbitrarily large powers of 2 in the denominator. You may use Exercise 7.]

Proof. Note that H is a subgroup of $K = \{\begin{pmatrix} 1 & q \\ 0 & \end{pmatrix} \mid q \in \mathbb{Q}\}$ and that $K \cong \mathbb{Q}$ via the isomorphism $f : \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \mapsto q$ (this we did in class). Then $f(H)$ is a subgroup of $\mathbb{Q}$ and the previous problem would imply that if H (and therefore also $f(H)$) were finitely generated then $f(H) = m/n\mathbb{Z}$ for some integers m and n.

But $\begin{pmatrix} 2 & \\ & 1 \end{pmatrix}^k \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \begin{pmatrix} 2 & \\ & 1 \end{pmatrix}^{-k} = \begin{pmatrix} 1 & 2^{-k} \\ & 1 \end{pmatrix} \in H$ and so $2^{-k} \in f(H)$ for every $k \in \mathbb{Z}$. Now if H were finitely generated and $f(H) = m/n\mathbb{Z}$ then for $2^k > n$ it's clear that $2^{-k} \notin m/n\mathbb{Z}$ so we get a contradiction and thus H is not finitely generated. ☐

9. Let $n \geq 3$. Consider the dihedral group $D_{2n} = (\mathbb{Z}/n\mathbb{Z}) \rtimes_\phi (\mathbb{Z}/2\mathbb{Z})$ where $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ is defined by $\phi_0 = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$ and $\phi_1(x) = -x$. Recall from class that if $F = (1, 0)$ and $R = (0, 1)$ (the first coordinate in $\mathbb{Z}/2\mathbb{Z}$ and the second coordinate in $\mathbb{Z}/n\mathbb{Z}$) then F has order 2, R has order n and $FRF = R^{-1}$, and $D_{2n} = \langle F, R\rangle$. Suppose $a, b \in \mathbb{Z}/n\mathbb{Z}$. Show that R^a and FR^b generate D_{2n} (i.e., $D_{2n} = \langle R^a, FR^b\rangle$) if and only if $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. [Hint: Show that in an arbitrary product of R^a-s and FR^b-s and their inverses you can collect all the F-s on the left side.]

Proof. If $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ let k be such that $ak \equiv 1 \pmod{n}$. Writing $f = FR^b$ and $r = R^a$ then $R = R^{ka} = r^k \in \langle r, f\rangle$ and then $F = FR^bR^{-b} = fR^{-b} \in \langle r, f\rangle$. We conclude that $D_{2n} = \langle R, F\rangle \subset \langle r, f\rangle$ so D_{2n} is generated by R^a and FR^b.

Now suppose that R^a and FR^b do generated D_{2n}. Note that $\langle R^a, FR^b\rangle$ contains arbitrary products of R^a, R^{-a}, FR^b and $(FR^b)^{-1} = FR^b$ ($FR^bFR^b = R^{-b+b} = 1$). We'll show by induction on the number of terms in such a product that $\langle R^a, FR^b\rangle = \{R^{ka} \mid k \in \mathbb{Z}\} \cup \{FR^{b+ak} \mid k \in \mathbb{Z}\}$. This is clearly true if the product consists of a single factor. To show the inductive step it suffices to show that if we multiply an element of the RHS with either $R^{\pm a}$ or FR^b then we still get an element of the RHS. But $R^{ak} \cdot R^{\pm a} = R^{a(k\pm1)}$, $R^{ak}FR^b = FR^{b-ak}$, $FR^{b+ak}R^{\pm a} = FR^{b+a(k\pm1)}$ and $FR^{b+ak}FR^b = R^{-ak}$.

If the RHS is all of D_{2n} it follows that 1 is in the RHS and it can only be $1 = R^{ak}$ for some $k \in \mathbb{Z}$. But R has order n and so $ak \equiv 1 \pmod{n}$ which implies $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. ☐

10-11 (This counts as two problems) Let $n \geq 3$ be an odd number. Consider the group homomorphism $\phi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ given by $\phi_a(x) = ax$. Recall that the dihedral group $D_{2n} = \{F^uR^v \mid 0 \leq u \leq 1, 0 \leq v < n\}$.

(a) For $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $b \in \mathbb{Z}/n\mathbb{Z}$ define $\Psi_{a,b}(F^uR^v) := (FR^b)^u(R^a)^v$. Show that $\Psi_{a,b} \in \mathrm{Aut}(D_{2n})$. [Hint: Use the previous problem.]

(b) Show that $\Psi : (\mathbb{Z}/n\mathbb{Z}) \rtimes_\phi (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(D_{2n})$ is an injective group homomorphism.

(c) Show that Ψ is surjective, i.e., that every automorphism of D_{2n} is of the form $\Psi_{a,b}$ for some a and b and conclude that

$$\mathrm{Aut}(D_{2n}) \cong (\mathbb{Z}/n\mathbb{Z}) \rtimes_\phi (\mathbb{Z}/n\mathbb{Z})^\times$$

[Hint: Use part (a).]

(d) (Extra credit) For a group G the group of outer automorphisms is defined as $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$, a group since $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$ from a previous homework. Show that $\mathrm{Out}(D_{2n}) \cong (\mathbb{Z}/n\mathbb{Z})^\times/\{\pm1\}$.

Proof. (a): By construction $\Psi_{a,b} : D_{2n} \to D_{2n}$ and the previous problem shows that $\Psi_{a,b}$ is surjective. Since $\Psi_{a,b}$ is a surjective map between two sets of the same size it must also be injective. Finally, $\Psi_{a,b}$ is a homomorphism: $\Psi_{a,b}(F^uR^vF^eR^f) = \Psi_{a,b}(F^{u+e}R^{(-1)^ev+f}) = (FR^b)^{u+e}(R^a)^{(-1)^ev+f}$ while

$$\Psi_{a,b}(F^uR^v)\Psi_{a,b}(F^eR^f) = (FR^b)^u(R^a)^v(FR^b)^e(R^a)^f$$

and the homomorphism condition follows from the fact that for $e = 0, 1$ one has

$$(FR^b)^e (R^a)^v (FR^b)^e = (R^a)^{(-1)^e v}$$

(b): Suppose $(a, b), (c, d) \in \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ (with $a, c \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $b, d \in \mathbb{Z}/n\mathbb{Z}$). In this semidirect product one has $(a, b)(c, d) = (ac, b + ad)$. We compute

$$\begin{aligned}
\Psi_{a,b} \circ \Psi_{c,d}(F) &= \Psi_{a,b}(FR^d) = FR^{b+ad} = \Psi_{ac,b+ad}(F) \\
\Psi_{a,b} \circ \Psi_{c,d}(R) &= \Psi_{a,b}(R^c) = R^{ac} = \Psi_{ac,b+ad}(R)
\end{aligned}$$

Since $\Psi_{a,b} \circ \Psi_{c,d}$ and $\Psi_{ac,b+ad}$ agree on generators they are the same homomorphism and so $(a, b) \mapsto \Psi_{a,b}$ satisfies $\Psi_{a,b} \circ \Psi_{c,d} = \Psi_{(a,c)(b,d)}$ and so $\Psi : \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(D_{2n})$ is a group homomorphism.

(c): If $f \in \mathrm{Aut}(D_{2n})$ it follows that $f(F)$ has order 2 and $f(R)$ has order n, as the order of $f(x)$ is the same as the order of x for any injective f ($f(x)^k = 1$ iff $f(x^k = 1)$ iff $x^k = 1$). The order of FR^b is 2 for any b and the order of R^a is $n/(n, a)$. Since n is odd this can never be 2. Thus $f(F) = FR^b$ for some b and $f(R) = R^a$ for some a such that $n/(n, a) = n$, i.e., for $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. This means that $f = \Psi_{a,b}$ and we know from part (a) that every $\Psi_{a,b}$ is an automorphism. From part (b) we deduce the isomorphism $\mathrm{Aut}(D_{2n}) \cong (\mathbb{Z}/n\mathbb{Z}) \rtimes_\phi (\mathbb{Z}/n\mathbb{Z})^\times$.

(d): Since n is odd it follows that $FR^b R^a FR^b = R^{-a} \neq R^a$ for any exponent a (otherwise $R^{2a} = 1$ but then $a = 0$ as 2 is invertible mod n) and so $Z(D_{2n}) = 1$. This implies that $\mathrm{Inn}(D_{2n}) \cong D_{2n}/Z(D_{2n}) \cong D_{2n} = \mathbb{Z}/n\mathbb{Z} \rtimes \{\pm 1\}$. Thus

$$\mathrm{Out}(D_{2n}) = \mathrm{Aut}(D_{2n})/\,\mathrm{Inn}(D_{2n}) = \frac{\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times}{\mathbb{Z}/n\mathbb{Z} \rtimes \{\pm 1\}} \cong (\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\}$$

Here we used the 3rd isomorphism theorem as if $K \lhd H$ then

$$H/K \cong \frac{N \rtimes H/N}{N \rtimes K/N} \cong \frac{N \rtimes H}{N \rtimes K}$$

$\square$