Math 30810 Honors Algebra 3
Homework 4

Andrei Jorza

Due Thursday, September 22

Do any 8 of the following questions. Artin a.b.c means chapter a, section b, exercise c.

1. Artin 2.5.5

   Proof. Note that $\begin{pmatrix} A & B \\ & D \end{pmatrix}\begin{pmatrix} A' & B' \\ & D' \end{pmatrix} = \begin{pmatrix} AA' & AB' + BD' \\ & DD' \end{pmatrix}$ and $\begin{pmatrix} A & B \\ & D \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1} & -A^{-1}BD^{-1} \\ & D^{-1} \end{pmatrix}$. Therefore H is a subgroup. Let $f : M \to \mathrm{GL}_r(\mathbb{R})$ be the map sending M to A. By inspecting the formulas we immediately see that $f(M^{-1}) = f(M)^{-1}$ and $f(MM') = f(M)f(M')$ and so f is a homomorphism. It's kernel is the subgroup of matrices of the form $\begin{pmatrix} I_r & B \\ & D \end{pmatrix}$. □

2. Artin 2.6.7

   Proof. Note that if $x = gag^{-1}$ and $y = gbg^{-1}$ then $xy^{-1} = gag^{-1}(gbg^{-1})^{-1} = gag^{-1}gbg^{-1} = gabg^{-1} \in gHg^{-1}$ and so gHg^{-1} is closed under division which implies it is a subgroup. □

3. Artin 2.6.9

   Proof. Consider the map $f : G \to G^{\circ}$ given by $f(g) = g^{-1}$. It is a bijection of sets as $g^{-1} = 1$ iff $g = 1$ and $g^{-1} = h^{-1}$ iff $g = h$. Moreover,

   $$f(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1} * h^{-1} = f(g) * f(h)$$

   and so f is a homomorphism. □

4. Suppose H is a subgroup of a group G. Show that H is normal in G if and only if for all $g \in G$, $gHg^{-1} \subset H$. (In class we required $gHg^{-1} = H$.)

   Proof. We need to show that in fact $gHg^{-1} = H$. Pick $h \in H$. Then $g^{-1}hg \in g^{-1}Hg \subset H$ by assumption. But $h = g(g^{-1}hg)g^{-1} \in gHg^{-1}$ and so we conclude that $H \subset gHg^{-1}$. □

5. Let G be a group. Recall that $\mathrm{End}(G)$ is the set of homomorphisms $f : G \to G$ and $\mathrm{Aut}(G) \subset \mathrm{End}(G)$ is the subset of those homomorphisms which are isomorphisms.

   (a) Show that usual composition of functions yields an associative composition law on $\mathrm{End}(G)$ with identity given by the identity function. (There is something you need to check here!)

   (b) Show that $f \in \mathrm{End}(G)$ has an inverse with respect to the composition law iff $f \in \mathrm{Aut}(G)$ and conclude that $\mathrm{Aut}(G)$ is a group.

Proof. (a): Composition on functions on a set X is associative and has the identity map as an identity. What we need to check is that if we compose two homomorphisms we also get a homomorphism. But if $f, g \in \mathrm{End}(G)$ then $f(g(xy)) = f(g(x)g(y)) = f(g(x))f(g(y))$ as each of f and g is a homomorphism. Therefore $f \circ g$, which a priori is only a function, is also a homomorphism so composition yields a composition law on $\mathrm{End}(G)$.

(b): Suppose f admits a homomorphism inverse g. Then $f \circ g =_G$ and $g \circ f =_G$. From the former we deduce that f is surjective as $\mathrm{Im}\, f \circ g \subset \mathrm{Im}\, f$ and from the second we deduce that f is injective as $\ker f \subset \ker g \circ f$. Thus f is bijective and so f is an isomorphism. If, reciprocally, f is bijective then it has a set theoretic inverse f^{-1}. We need to show that this is an inverse in $\mathrm{End}(G)$, i.e., that f^{-1} is also a homomorphism. Pick $x, y \in G$. Since f is surjective there exist $a, b \in G$ such that $f(a) = x$ and $f(b) = y$. Then $f^{-1}(xy) = f^{-1}(f(a)f(b)) = f^{-1}(f(ab)) = ab = f^{-1}(x)f^{-1}(y)$ so f^{-1} is also a homomorphism.

Therefore $\mathrm{Aut}(G)$ is the set of elements in $\mathrm{End}(G)$ which have an inverse and so, by the previous homework, $\mathrm{Aut}(G)$ is a group. □

6. Let G be a group. Recall from class that if $g \in G$ then the map $\phi_g(x) = gxg^{-1}$ is a homomorphism $\phi_g \in \mathrm{End}(G)$.
   (a) Show that in fact $\phi_g \in \mathrm{Aut}(G)$.
   (b) Show that the map $\Phi : G \to \mathrm{Aut}(G)$ given by $\Phi(g) = \phi_g$ is a group homomorphism.
   (c) (Optional) Show that $\ker \Phi = Z(G)$, the center of the group G.

Proof. (a): In class we showed that ϕ_g is an endomorphism. Now $\ker \phi_g = \{x \mid gxg^{-1} = 1\} = 1$ and so ϕ_g is injective. Moreover, $\phi_g(g^{-1}xg) = x$ for every $x \in G$ and so ϕ_g is surjective. Thus ϕ_g is an isomorphism.

(b): We need to check that $\Phi(gh) = \Phi(g)\Phi(h)$, i.e., that $\phi_{gh} = \phi_g \circ \phi_h$. But $\phi_g \circ \phi_h(x) = \phi_g(hxh^{-1}) = ghxh^{-1}g^{-1} = \phi_{gh}(x)$ as $(gh)^{-1} = h^{-1}g^{-1}$.

(c): $\ker \Phi = \{g \in G \mid \phi_g =_G\}$ and $\phi_g =_G$ iff $gxg^{-1} = x$ for all $x \in G$, i.e., iff $gx = xg$ for all $x \in G$. But this is $Z(G)$ by definition. □

7. Show that $\mathrm{Inn}(G)$, defined as the set of all inner automorphism $\{\phi_g \mid g \in G\}$, is a normal subgroup of $\mathrm{Aut}(G)$. [Hint: Use the previous problem.]

Proof. By definition $\mathrm{Inn}(G) = \mathrm{Im}\, \Phi$ is the image of the homomorphism $\Phi : G \to \mathrm{Aut}(G)$ defined in the previous problem. Immediately we deduce that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$. We need to check that it is normal. Suppose $f \in \mathrm{Aut}(G)$ and $\phi_g \in \mathrm{Inn}(G)$. Let's compute $f\phi_g f^{-1}$. For $x \in G$

$$f\phi_g f^{-1}(x) = f(\phi_g(f^{-1}(x))) = f(gf^{-1}(x)g^{-1}) = f(g)xf(g)^{-1} = \phi_{f(g)}$$

and so $f\phi_g f^{-1} = \phi_{f(g)}$ which immediately shows that $f\,\mathrm{Inn}(G)f^{-1} \subset \mathrm{Inn}(G)$. We deduce that $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}(G)$. □

8. Show that if G is a group of order 4 then either it is cyclic or it is isomorphic to the Klein 4-group V.

Proof. G is a group so it contains 1, and let $x \in G - \{1\}$. If x has order 4 then $G = \langle x \rangle$ is cyclic from the proposition we proved in class.

Let's suppose this is not the case, which implies that $\mathrm{ord}(x) < 4$ as $\langle x \rangle \subset G$. Let $y \in G - \langle x \rangle$. If $\mathrm{ord}(x) = 3$ then $G = \{1, x, x^2, y\}$ and xy cannot be in G anymore as y is not in $\{1, x, x^2\}$. This is impossible and therefore $\mathrm{ord}(x) = 2$ (it cannot have order 1 as $x \neq 1$). Then G contains $1, x, y$ and therefore also xy. As x has order 2, $x^{-1} = x$ and so $xy \notin \{1, x, y\}$. This implies that $G = \{1, x, y, xy\}$.

Now the map $f : G \to V$ sending x to $\begin{pmatrix} -1 & \\ & 1 \end{pmatrix}$ and $y \mapsto \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}$ is an isomorphism between G and V simply by inspection. $\square$

9. Show that $\langle(123)\rangle$ is normal in S_3 but the subgroups $\langle(12)\rangle$, $\langle(13)\rangle$ and $\langle(23)\rangle$ are not normal in S_3.

Proof. $\langle(123)\rangle = A_3$ is normal in S_3 as A_n is always normal in S_n.

Now $(123)(12)(123)^{-1} = (13)$, $(123)^{-1}(13)(123) = (12)$ and $(123)(13)(123)^{-1} = (23)$ and so the subgroups generated by the three transposition are not normal in S_3. $\square$

10. Show that in S_n, $(i_1, \dots, i_k) = (i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k)$ for any cycle $(i_1, \dots, i_k)$.

Proof. Let $c = (i_1, \dots, i_k)$ and $\tau_s = (i_s, i_{s+1})$. To check that $c = \tau_1 \cdots \tau_{k-1}$ it suffices to check it on each integer r between 1 and n.

If $r \notin \{i_1, \dots, i_k\}$ then $c(r) = r$ and $\tau_s(r) = r$ for all s. Thus $c(r) = \prod \tau_s(r)$ as desired.

Suppose $r = i_m$. Then $\tau_s(i_m) = i_m$ if $s > m$, $\tau_m(i_m) = i_{m+1}$ and $\tau_s(i_m) = i_m$ if $s < m - 1$. This means that for $m \le k - 1$

$$\tau_1 \cdots \tau_{k-1}(i_m) = \tau_1 \cdots \tau_m(i_m) = \tau_1 \cdots \tau_{m-1}(i_{m+1}) = i_{m+1} = c(i_m)$$

and if $m = k$ then

$$\tau_1 \dots \tau_{k-1}(i_k) = \tau_1 \dots \tau_{k-2}(i_{k-1}) = \dots \tau_1(i_2) = i_1 = c(i_k)$$

$\square$

11. (This is a useful problem) For $1 \le i, j \le n$ consider the matrix $E_{ij} \in M_{n\times n}(\mathbb{C})$ with 1 in position ij and 0s everywhere else.

   (a) For $i \ne j$ show that $I_n + E_{ij} \in \mathrm{GL}_n(\mathbb{C})$.

   (b) For a general matrix $X \in \mathrm{GL}_n(\mathbb{C})$ compute XE_{ij} and $E_{ij}X$ and show that $Z(\mathrm{GL}_n(\mathbb{C})) = \mathbb{C}^\times I_n$.

Proof. (a): Since $i \ne j$ the matrix E_{ij} is either upper or lower triangular with 0s on the diagonal. Then homework 2 implies that E_{ij} is nilpotent and so $I_n + E_{ij}$ is invertible by homework 1.

(b): If $X = (x_{ij}) \in Z(\mathrm{GL}_n(\mathbb{R}))$ then $(I_n + E_{ij})X = X(I_n + E_{ij})$ as $In + E_{ij} \in \mathrm{GL}_n(\mathbb{R})$ from part (a). Breaking up parantheses we get $XE_{ij} = E_{ij}X$. But XE_{ij} is the matrix with 0s everywhere except on the j-th column where the entries are $x_{1i}, x_{2i}, \dots, x_{ni}$, and $E_{ij}X$ is the matrix with 0s everywhere except on the j-th row where the entries are $x_{1j}, x_{2j}, \dots, x_{nj}$. Since these two matrices must be equal we deduce that $x_{aj} = 0$ whenever $a \ne j$ and $x_{ib} = 0$ whenever $b \ne i$ and that $x_{ii} = x_{jj}$. Letting i and j be any two distinct indices implies that X must be a scalar matrix.

Clearly any scalar matrix commutes with any other matrix and so we deduce that $Z(\mathrm{GL}_n(\mathbb{C})) = \mathbb{C}^\times I_n$. $\square$