Algebra I - Homework 2

Pablo Sánchez Ocal

September 16th, 2016

Exercise 1

We prove that the subgroup of $\mathrm{GL}_2(\mathbb{C})$ generated by the matrices:

$$a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \, b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

is isomorphic to $\mathbb{H}$ the quaternion group. To do this, we will see that these two matrices generate three elements a, b, c that follow the characteristic multiplication of the quaternions:

$$a^2 = b^2 = c^2 = abc = -1.$$

Since having this information immediately defines the quaternion group, the isomorphism will be evident. First, note that:

$$a^2 = -1 = b^2,$$

then define:

$$c = ab = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$$

that also has $c^2 = -1$. Now:

$$abc = c^2 = -1,$$

and thus since $a^3 = a^{-1}$, $b^3 = b^{-1}$ and $c^3 = c^{-1}$, we found that the group we are working with is exactly:

$$\langle a, \, b\rangle = \langle -1, \, a, \, b, \, c | (-1)^2 = 1, \, a^2 = b^2 = c^2 = abc = -1\rangle = \mathbb{H}$$

the quaternion group.

To prove that the group of quaternions $\mathbb{H}$ cannot be isomorphic to D_4 the group of symmetries of the square, we can use the Exercise 1.5 from the Problem Set 1 of this same course. I here attach the same solution I gave to that one:

We cannot have $\mathbb{H} \cong D_4$ since $i \in \mathbb{H}$ is such that $i^2 = -1$, but there is no element in D_4 whose square is the identity element:

1. Any rotation r_α with $\alpha \in \{0, \pi/2, \pi, 3\pi/2\}$ has $r_\alpha^2 = r_{2\alpha}$ (obviously r_0 is the identity, different from $-r_0$, and we are working with α modulo a factor 2π), which are never $-r_0$.

2. Any mirror image along the diagonals or the edges m_β with $\beta \in \{1, 2, 3, 4\}$ has $d_\beta^2 = r_0$.

Exercise 2

The set $\mathrm{Aut}(G)$ of automorphisms of a group G is a group with respect to composition. Prove that:

1. $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$: consider $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ an isomorphism. We note that since f is a morphism, $f(0) = 0$ and f is completely determined by the image of 1. Thus for f to be an isomorphism we can only choose $f(1) = 1$ or $f(1) = -1$ (since if $f(1) = n$ with $n \in \mathbb{Z}$ then there doesn't exist any $m \in \mathbb{Z}$ with $f(m) = 1$, and thus f is not surjective). Thus $\mathrm{Aut}(\mathbb{Z}) = \{id, -id\}$ with the multiplication table:

	id	$-id$
id	id	$-id$
$-id$	$-id$	id

   which implies $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

2. $\mathrm{Aut}(\mathbb{Z}^n) \cong \mathrm{GL}_n(\mathbb{Z})$: that is, an isomorphism between the group of automorphisms $f : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ and the group of $n \times n$ invertible matrices with integer coefficients and inverse with integer coefficients.

   We first note that since $\mathbb{Z}$ is an Euclidean ring, by [1, p. 365 onwards], every element in the group $\mathrm{GL}_n(\mathbb{Z})$ can be obtained from the identity matrix by successive multiplication by the elementary matrices T_{ij} (which exchanges the i-th and j-th rows), D_i (which changes the sign of the i-th row) and $L_{ij}(m)$ (which adds $m \in \mathbb{Z}$ times the i-th row to the j-th row), namely:

$$\begin{pmatrix} 1 &&&&&& \\ & \ddots &&&&& \\ && 0 && 1 && \\ &&& \ddots &&& \\ && 1 && 0 && \\ &&&&& \ddots & \\ &&&&&& 1 \end{pmatrix}, \begin{pmatrix} 1 &&&& \\ & \ddots &&& \\ && -1 && \\ &&& \ddots & \\ &&&& 1 \end{pmatrix}, \begin{pmatrix} 1 &&&&&& \\ & \ddots &&&&& \\ && 1 &&&& \\ &&& \ddots &&& \\ && m && 1 && \\ &&&&& \ddots & \\ &&&&&& 1 \end{pmatrix}$$

   in their respective order. We note that D_i can only change the sign, and not multiply the whole row by an element of $\mathbb{Z}$, since (by [1]) we need that one such element be a unit, thus the only choices that we have are ± 1.

   We then note that since $f : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ must be an isomorphism, it must be invertible. Thus, since we do not have multiplicative inverses in $\mathbb{Z}$, each and every one of its components must be a linear combination of the original input. That is, when we write $f(m_1, \dots, m_n) = (f_1(m_1, \dots, m_n), \dots, f_n(m_1, \dots, m_n))$ we must have that $f_i(m_1 \dots, m_n) = \sum_{j=1}^{n} a_{ij} m_j$ for certain $a_{ij} \in \mathbb{Z}$ for every $i, j \in \{1, \dots, n\}$ (this is just a general expression to say that no divisions are allowed in the coefficients, but this is not the only restriction, as we treat below).

Define now the map:

$$\begin{array}{cccc} \varphi & : & \mathrm{Aut}(\mathbb{Z}^n) & \longrightarrow & \mathrm{GL}_n(\mathbb{Z}) \\ & & t_{ij} & \longmapsto & T_{ij} \\ & & d_i & \longmapsto & D_i \\ & & l_{ij}(m) & \longmapsto & L_{ij}(m) \end{array}$$

with t_{ij}, d_i and $l_{ij}(m)$ defined as follows:

$$\begin{aligned} t_{ij}(m_1,\ldots,m_n) &= (m_1,\ldots,m_j,\ldots,m_i,\ldots,m_n) \\ d_i(m_1,\ldots,m_n) &= (m_1,\ldots,-m_i,\ldots,m_n) \\ l_{ij}(m)(m_1,\ldots,m_n) &= (m_1,\ldots,m_i,\ldots,m_j+m\cdot m_i,\ldots,m_n) \end{aligned}$$

thus φ is a unequivocal and well defined relation between these kind of isomorphisms of $\mathbb{Z}^n$ and the correspondent matrices. By what we have discussed above, since any element of $\mathrm{GL}_n(\mathbb{Z})$ can be obtained from the elementary matrices (and thus the corresponding composition of isomorphisms determine one element that is mapped to the desired matrix), φ is surjective. Moreover, by definition, it preserves the group operation.

We now have to see that every element in $\mathrm{Aut}(\mathbb{Z}^n)$ can be also written composition of the isomorphisms t_{ij}, d_i and $l_{ij}(m)$, and thus φ will be completely well defined. To do so, take $f \in \mathrm{Aut}(\mathbb{Z}^n)$: $f(m_1,\ldots,m_n) = (f_1(m_1,\ldots,m_n),\ldots,f_2(m_1,\ldots,m_n))$. We note that by means of t_{ij}, we can start without loss of generality by first determining f_1, then determining f_2 and so on until finally determining f_n (permuting the variables and/or the components yields analogous situations). The possible linear combinations for f_1 do not allow having $k_{f_{1,1}}\cdot m_1$ for $k_{f_{1,1}} \neq \pm 1$ since that would make f not invertible, thus the only ones are $f_1(m_1,\ldots,m_n) = \pm m_1 + k_{f_{1,2}}\cdot m_2 + \cdots + k_{f_{1,n}}\cdot m_n$ with $k_{f_{1,j}} \in \mathbb{Z}$ for $1 \leq j \leq n$, $j \neq 1$. For the same reason, if we want f invertible we need $f_2(m_1,\ldots,m_n) = k_{f_{2,1}}\cdot f_1(m_1,\ldots,m_n) \pm m_2 + k_{f_{2,3}}\cdot m_3 + \cdots + k_{f_{2,n}}\cdot m_n$ with $k_{f_{2,j}} \in \mathbb{Z}$ for $1 \leq j \leq n$, $j \neq 2$, as since f_1 is already determined, we must deal with it as a whole. This argument can be readily generalized for f_j with $1 \leq j \leq n$, the final one being that we need $f_n(m_1,\ldots,m_n) = k_{f_{n,1}}\cdot f_1(m_1,\ldots,m_n) + \cdots + k_{f_{n,n-1}}\cdot f_{n-1}(m_1,\ldots,m_n) \pm m_n$ with $k_{f_{n,j}} \in \mathbb{Z}$ for $1 \leq j \leq n$, $j \neq n$, again because since f_j for $1 \leq j \leq n-1$ are already determined, we must deal with them as a whole. This clearly means that f has the desired form as composition of functions, and thus $\varphi(f)$ is well defined.

Now injectivity follows from the fact that φ is a morphism and determines a bijection of t_{ij}, d_i and $l_{ij}(m)$ to T_{ij}, D_i and $L_{ij}(m)$, meaning that φ is an isomorphism, as desired.

Exercise 3

Let M, N be subgroups of G of finite index, we want to prove that $M \cap N$ is a subgroup of finite index. We already know that the intersection of groups is a group, but the proof is easy:

1. Closed under multiplication: let $g, h \in M \cap N$, then $g, h \in M, N$ thus $gh \in M, N$ thus $gh \in M \cap N$.
2. Associativity: let $f, g, h \in M \cap N$, then then $f, g, h \in M, N$ thus $f(gh) = (fg)h$ in M, N thus in $M \cap N$.
3. Identity: $e \in M, N$ thus $e \in M \cap N$ and for every $g \in M \cap N$ we have $g \in M, N$ with $ge = g = eg$ in M, N thus in $M \cap N$.
4. Inverses: let $g \in M \cap N$, then $g \in M, N$ with $g^{-1} \in M, N$ so that $g^{-1} \in M \cap N$, with $gg^{-1} = e = g^{-1}g$ in M, N thus in $M \cap N$.

To prove that the index of $M \cap N$ is finite, we use that $M \cap N < M$ and $M \cap N < N$ so that by [2, p. 39] we have:

$$[G : M \cap N] = [G : M][M : M \cap N] \leq [G : M][G : N]$$

and $[G : M \cap N]$ is finite.

For an infinite group such that the intersection of all its subgroups of finite index is trivial, consider $\mathbb{Z}$ with $d\mathbb{Z}$ for $d \in \mathbb{N}^+$. We clearly have $[\mathbb{Z} : d\mathbb{Z}] = d$ for $d \in \mathbb{N}^+$. However, $\bigcap_{d \in \mathbb{N}^+} d\mathbb{Z} = \{0\}$, as desired.

Exercise 4

We want subgroups H and K of D_4 with $H \triangleleft K \triangleleft D_4$ but $H \ntriangleleft D_4$. We already know that D_4 has the special Klein group, so that will be our candidate for K. We will consider $D_4 < S_4$, thus the notation here used will be the one of permutations. Set $H = \langle (12)(34) \rangle = \{id, (12)(34)\}$ and $K = K_4 = \{id, (12)(34), (13)(24), (14)(23)\}$ the Klein group. Since $[D_4 : K] = 2$ and $[K : H] = 2$, it follows that $H \triangleleft K$, and $K \triangleleft D_4$.

However, we have that $H \ntriangleleft D_4$ since for $(1234) \in D_4$ and $(12)(34) \in H$ we have:

$$(1234)(12)(34)(1234)^{-1} = (1234)(12)(34)(1432) = (14)(23) \notin H.$$

Exercise 5

Suppose that $H \leq G$ and $N \triangleleft G$, we want to prove that $H \cap N \triangleleft H$. Take $h \in H$, $g \in H \cap N$. Since $g \in H$ we have $hg \in H$, since $g \in N$ we have that there exists $g' \in N$ with $hg = g'h$ by normality. Now $g' = hgh^{-1} \in H$, thus $g' \in H \cap N$ and $hg = g'h$ with $g, g' \in H \cap N$, meaning that $H \cap N \triangleleft H$.

Exercise 6

We want to find all normal subgroups of D_n for $n \in \mathbb{N}^+$. We begin with a few generalities. By [2, p. 50] we know that $D_n = \langle R, S | R^n = S^2 = (RS)^2 = 1, R^m \neq 1 \text{ if } 1 < m < n\rangle$, where R represents a rotation and S a symmetry. In particular, this means that any element of D_4 can be written as:

1. Rotation: R^m for $0 \leq m < n$.

2. Symmetry: $R^m S$ for $0 \leq m < n$.

The characterization of the normal subgroups that we will use is that a group is normal if and only if it is union of conjugacy classes.To prove this, let N be a subgroup of a group G and $[h] = \{ghg^{-1} | g \in G\}$. We know that N is normal if and only if when $n \in N$ then $gng^{-1} \in N$ for every $g \in G$, which happens if and only if $[n] \subset N$. Thus N normal implies $N = \bigcup_{n \in N} [n]$, and obviously if $N = \bigcup_{n \in N} [n]$ is a group then N is normal by definition of $[n]$. What we will now do is enumerate the conjugacy classes of D_n and use them to build all the possible normal subgroups.

1. $n = 2k + 1$, $k \in \mathbb{N}$: The conjugacy classes are:

   $$\{id\}, \{R, R^{n-1}\}, \ldots, \{R^k, R^{k+1}\}, \{R^m S | 0 \leq m < n\}.$$

   All but the last are clear, since we are taking R^m and $R^{-m} = R^{n-m}$ for $0 \leq m < n$. The last one is built from the single symmetry S by conjugation: $R^m S R^{-m} = R^{2m} S$ with $0 \leq m < n$, thus when $0 \leq m \leq k$ we obtain $\{S, R^2 S, \ldots, R^{2k}\}$ and when $k + 1 \leq m \leq 2k$ we obtain $\{RS, R^3 S, \ldots, R^{2k-1}\}$ in virtue of $(RS)^2 = 1$ (or $RS = R^{-1} S$) and $R^{2k+1} = 1$.

   However, $[S]$ is not a subgroup since $RS, S \in [S]$ with $RSS = R \notin [S]$. Thus if a normal subgroup N contains $[S]$ (or a single symmetry), it must be the whole D_n.

   Since $\langle R \rangle$ has index 2, it is automatically normal. Thus the remaining normal subgroups must be subgroups of $\langle R \rangle$. We note that $\langle R \rangle \cong S_n$, and thus the subgroups are $\langle R^d \rangle$ with d dividing n. In virtue of $RS = R^{-1} S$, we have that all those subgroups are normal: $(R^m S) R^{dq} (R^m S)^{-1} = R^m S S R^{-dq} R^{-m} = R^{-dq} \in \langle R \rangle$ for d dividing n and $q \in \mathbb{Z}$ (in particular for rotations it also works).

   We can then conclude that the normal subgroups are: $\{id\}$, $\langle R^d \rangle$ with d dividing n and D_n.

2. $n = 2k$, $k \in \mathbb{N}$: The conjugacy classes are:

   $$\{id\}, \{R, R^{n-1}\}, \ldots, \{R^k, R^{k+1}\}, \{R^k\}, \{R^{2m} S | 0 \leq m < k\}, \{R^{2m+1} S | 0 \leq m < k\}.$$

   Where by the same argument as before we obtain all but the last two. Those are $[S]$ (the even reflections) and $[RS]$ (the odd reflections) respectively, where now they are in disjoint classes because of the parity.

By the same argument as before, we still have as normal subgroups $\langle R^d \rangle$ with d dividing n.

Now say we want to include the even reflections in a subgroup N. Since $S, R^2S \in [S]$, we would need to have $R^2SS = R$ and thus include $[R^2]$, which in particular means including $\langle R^2 \rangle$ for N to be a group. Thus it must be $\langle R^2, S \rangle$.

Now say we want to include the odd reflections in a subgroup N. Since $RS, R^3S \in [RS]$, we would need to have $R^3SRS = R^2$ and thus include $[R^2]$, which in particular means including $\langle R^2 \rangle$ for N to be a group. Thus it must be $\langle R^2, RS \rangle$.

We can then conclude that the normal subgroups are: $\{id\}$, $\langle R^d \rangle$ with d dividing n, $\langle R^2, S \rangle$, $\langle R^2, RS \rangle$ and D_n.

Exercise 7

Let S be the subgroup of S_n of permutations for which 1 is invariant. By [2, p. 39] we have that $|S_n| = [S_n : S]|S|$ and since $S \cong S_{n-1}$ (this follows immediately from the fact that since $\sigma \in S$ must have $\sigma(1) = 1$, then σ can only be permutations of $\{2, \ldots, n\}$), we must have that $[S_n : S] = n$. We have $S \ntrianglelefteq S_n$ since taking $(12) \in S_n$ and $(23) \in S$ we have that $(12)(23)(12)^{-1} = (12)(23)(12) = (13) \notin S$.

References

[1] R. Elman, *Lectures on Abstract Algebra (Preliminary Version)*, [Available online at http://www.math.ucla.edu/∼rse/algebra_book.pdf.]

[2] T. W. Hungerford, *Algebra*.