Math 3140 - Assignment 4

Due February 14, 2024

(1) Let $\mathbb{C}$ be the set of complex numbers and

$$M = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;:\; a, b \in \mathbb{R} \right\}.$$

Show that $(\mathbb{C}, +) \cong (M, +)$ and $(\mathbb{C} \setminus \{0\}, \cdot) \cong (M \setminus \{0\}, \cdot)$.

Solution: We need to define the isomorphisms.

$$\varphi\colon \mathbb{C} \to M,\ a + ib \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

is clearly bijective.

(a) Check $\varphi([a+ib] + [c+id]) = \varphi(a+ib) + \varphi(c+id)$ for all $a+ib, c+id \in \mathbb{C}$.
Hence $\varphi\colon (\mathbb{C}, +) \to (M, +)$ is an isomorphism.

(b) Check $\varphi([a+ib] \cdot [c+id]) = \varphi(a+ib) \cdot \varphi(c+id)$ for all $a+ib, c+id \in \mathbb{C}$.
Hence $\varphi\colon (\mathbb{C} \setminus \{0\}, \cdot) \to (M \setminus \{0\}, \cdot)$ is an isomorphism. □

(2) Let G be a group. Show that Aut$G$ is group a under composition of functions.

Solution: Check the definition of a group:

(a) Aut$G \neq \emptyset$ since the identity map id is in Aut$G$.

(b) Composition is an operation on Aut$G$ since the composition of homomorphisms is a homomorphism and the composition of bijections is a bijection again.

(c) Composition of function is associative (recall from Discrete Math, Calculus).

(d) There is an identity element: $\mathrm{id} \circ \varphi = \varphi \circ \mathrm{id} = \varphi$ for all $\varphi \in \mathrm{Aut}G$.

(e) Every $\varphi \in \mathrm{Aut}G$ has an inverse $\varphi^{-1} \in \mathrm{Aut}G$.

Hence $(\mathrm{Aut}G, \circ)$ is a group. □

(3) For a group G and $g \in G$, define the inner automorphism

$$\varphi_g\colon G \to G,\ x \mapsto gxg^{-1}.$$

Show

(a) $\varphi_g \in \mathrm{Aut}G$.

(b) $\Phi\colon G \to \mathrm{Aut}G,\ g \mapsto \varphi_g$, is a homomorphism.

(c) $\ker\Phi = Z(G)$.

Solution: (a) φ_g is a homomorphism since for $x, y \in G$

$$\varphi_g(xy) = gxyx^{-1} = gxg^{-1}gyx^{-1} = \varphi_g(x)\varphi_g(y).$$

φ_g is bijective since it has an inverse $\varphi_g^{-1} = \varphi_{g^{-1}}$. Thus $\varphi_g \in \mathrm{Aut}G$.

(b) Φ is a homomorphism since for $g, h \in G$
$\Phi(gh) = \varphi_{gh}$ maps $x \mapsto ghx(gh)^{-1}$,
$\Phi(g)\Phi(h) = \varphi_g \circ \varphi_h$ maps $x \mapsto \varphi_g(\varphi_h(x)) = ghx(gh)^{-1}$.
Hence $\Phi(gh) = \Phi(g)\Phi(h)$.

(c)

$$\begin{aligned} g \in \ker\Phi &\text{ iff } \varphi_g = \mathrm{id} \\ &\text{ iff } gxg^{-1} = x \quad \forall x \in G \\ &\text{ iff } g \in Z(G). \end{aligned}$$

□

(4) Let $D_8 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$ be the dihedral group of order 8 generated by a rotation a and a reflection b.
(a) When are $\varphi_g = \varphi_h$ for $g, h \in D_8$?
(b) What is the order of $\mathrm{Inn}D_8$?
(c) List all distinct elements in $\mathrm{Inn}D_8$.

Solution: (a) For any group G and $g, h \in G$:

$$\begin{aligned} \varphi_g = \varphi_h &\text{ iff } \varphi_g(x) = \varphi_h(x) \quad \forall x \in G \\ &\text{ iff } gxg^{-1} = hxh^{-1} \quad \forall x \in G \\ &\text{ iff } xg^{-1}h = g^{-1}hx \quad \forall x \in G \\ &\text{ iff } g^{-1}h \in Z(G) \\ &\text{ iff } gZ(G) = hZ(G). \end{aligned}$$

Hence g, h give the same inner automorphism iff they are in the same left coset of the center of G.
(b) By (a)

$$|\mathrm{Inn}G| = \frac{|G|}{|Z(G)|}.$$

Since $Z(D_8) = \{1, a^2\}$, we get $|\mathrm{Inn}D_8| = 4$.
(b) By (a) we need to pick one representative from each coset of the center to get all distinct elements in $\mathrm{Inn}G$. So

$$\mathrm{Inn}D_8 = \{\varphi_1 = \varphi_{a^2},\ \varphi_a = \varphi_{a^3},\ \varphi_b = \varphi_{a^2b},\ \varphi_{ab} = \varphi_{a^3b}\}.$$

(5) Show that $|\mathrm{Aut}D_8| \leq 8$.

Hint: Explain why an automorphism is uniquely determined by what it does to the generators a and b. Where could these be mapped to?

Solution: Recall that D_8 is generated by a rotation a (order 4) and a reflection b (order 2),

$$D_8 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

If a homomorphism $\varphi\colon D_8 \to H$ satisfies $\varphi(a) = u$ and $\varphi(b) = v$, then the homomorphism property yields that $\varphi(a^i b^j) = u^i v^j$. Hence φ is uniquely determined on the whole group by what it does to its generators.

Now let $\varphi \in \mathrm{Aut}D_8$. Isomorphisms preserve the order of elements and map generators to generators. Since $\varphi(a)$ has order 4, it can only be a or a^3. Further $\varphi(b)$ has order 2, so could be a^2, b, ab, a^2b, a^3b. But $\varphi(b) = a^2$ is not possible since then $\langle \varphi(a), \varphi(b)\rangle = \langle a \rangle \neq D_8$. So it only remains that $\varphi(b) \in \{b, ab, a^2b, a^3b\}$.

Summing up there are 2 choices for $\varphi(a)$ and 4 choices for $\varphi(b)$. Hence at most 8 automorphism. (Note: It's not clear from this argument that every choice really yields an automorphism but it does.) □

(6) Find non-isomorphic groups G, H such that $\mathrm{Aut}G \cong \mathrm{Aut}H$.

Solution: We classified $\mathrm{Aut}\mathbb{Z}_n$ in class. So consider
$\mathrm{Aut}\mathbb{Z}_3 \cong (\mathbb{Z}_3^*, \cdot) = (\{1, 2\}, \cdot)$
$\mathrm{Aut}\mathbb{Z}_4 \cong (\mathbb{Z}_4^*, \cdot) = (\{1, 3\}, \cdot)$

Both groups have order 2, hence are isomorphic to $(\mathbb{Z}_2, +)$. □

(7) For the following subgroups H of G, find all the left cosets of H in G. Give one representative for each left coset. How many are there?

(a) $G = \mathbb{R}^2$ under addition, $H = \{(x, 0) \ : \ x \in \mathbb{R}\}$

Solution: H is the x-axis.
Translating H by $(a, b) \in \mathbb{R}^2$ yields the left coset

$$(a, b) + H = \{(x, b) \ : \ x \in \mathbb{R}\}.$$

Note this is just a parallel to the x-axis for $y = b$.
There are infinitely many such left cosets, all of the form $(0, b) + H$ for some $b \in \mathbb{R}$. E.g. $(0, b)$ is a representative for $(0, b) + H$. □

(b) $G = \langle a \rangle$ of order 12, $H = \langle a^4 \rangle$

Solution: $G = \langle a \rangle = \{1, a, a^2, \dots, a^{11}\}$
$H = \langle a^4 \rangle = \{1, a^4, a^8\}$
Translating H by elements from G yields

$$\begin{aligned} H &= \{1, a^4, a^8\} \\ aH &= \{a, a^5, a^9\} \\ a^2H &= \{a^2, a^6, a^{10}\} \\ a^3H &= \{a^3, a^7, a^{11}\} \end{aligned}$$

Note that the union of these 4 cosets is G. Hence we have found all cosets. Representatives are e.g. $1, a, a^2, a^3$, resp. □

(c) $G = \mathbb{R}^*$ under multiplication, $H = \mathbb{R}^+$ the subgroup of positive reals

Solution: Translating $\mathbb{R}^+$ by elements from $\mathbb{R}^*$ yields $\mathbb{R}^+$ and $(-1)\mathbb{R}^+ = R^-$ (the set of negative reals). Since $\mathbb{R} = \mathbb{R}^+ \cup \mathbb{R}^-$ we have found all cosets already. Representatives are e.g. $1, -1$. □

(8) For any integer $n > 1$, Euler's ϕ-function $\phi(n)$ yields the number of positive integers less than n that are coprime to n. Prove:

Euler's Theorem. If a is coprime to n, then $a^{\phi(n)} \equiv 1 \bmod n$.

Solution: Recall that $\mathbb{Z}_n^*$ is the set of elements in $\mathbb{Z}_n$ that have a multiplicative inverse, i.e. $\mathbb{Z}_n^* = \{[a] \ : \ \gcd(a, n) = 1\}$. In particular $|\mathbb{Z}_n^*| = \phi(n)$.

Assume a is coprime to n. Then $[a] \in \mathbb{Z}_n^*$ and Lagrange's Theorem yields $[a]^{|\mathbb{Z}_n^*|} = [1]$. Equivalently $a^{\phi(n)} \equiv 1 \bmod n$. □