MAS 4301, Abstract Algebra I

Notes of Krishna Alladi's Lecture on Wed, Mar 18, 2020.

Chapter 6: Isomorphisms cont'd.

Let us begin with

Problem 2, Ch. 6, p 132; Find $Aut(\mathbb{Z})$.

Solution: We know that $(\mathbb{Z}, +)$ is an infinite cyclic group and that it has precisely two generators 1 and -1. Every automorphism of $\mathbb{Z}$, denoted by α, is completely determined by its value $\alpha(1)$, since $\mathbb{Z} = \langle 1 \rangle$.

$$\alpha : \mathbb{Z} \underset{\text{auto}}{\rightarrow} \mathbb{Z}, \quad \alpha(1) = ?$$

We also know that $\alpha(1)$ must be a generator of $\mathbb{Z}$, because otherwise α will not be an onto map. Thus $\alpha(1) = 1$ or -1. So we have exactly two choices for $\alpha(1)$. Thus $Aut(\mathbb{Z})$ is in one-to-one correspondence with the two element group $\{1, -1\}$, which is isomorphic to $\mathbb{Z}_2$. Indeed, $Aut(\mathbb{Z})$ is isomorphic to $\{1, -1\}$, a group under multiplication, and thus is isomorphic to $\mathbb{Z}_2$, a group under addition (mod 2).

Let us denote the two members of $Aut(\mathbb{Z})$ by α_1 and α_{-1} where $\alpha_1(1) = 1$ & $\alpha_{-1}(1) = -1$. Then composition of α_1 and α_{-1} corresponds to multiplication of 1 and -1, and any composition of ~~any number~~ α_1 & α_{-1} corresponds to the corresponding multiplication of 1 and -1. For example $\alpha_1 \circ \alpha_1 \circ \alpha_{-1} \leftrightarrow 1.1.(-1)$. α_1 is the identity in $Aut(\mathbb{Z})$.

Simple as this example is, it is important, because every infinite cyclic group G is isomorphic to $\mathbb{Z}$. Thus for every infinite cyclic group, ~~we~~ G, we will have $Aut(G) \approx \mathbb{Z}_2$ (isomorphic to $\mathbb{Z}_2$).

It is of interest to determine the ~~isomor~~ automorphism group of a given group G. But this is not easy in general.

What about the automorphism group of a finite cyclic group? Since every finite cyclic group is isomorphic to $\mathbb{Z}_n$, for some $n \in \mathbb{Z}^+$ we need only determine $Aut(\mathbb{Z}_n)$. This is given by the next theorem.

Theorem 6.5 (in book). For each $n \in \mathbb{Z}^+$,

$$\mathrm{Aut}(\mathbb{Z}_n) \simeq U(n) = \mathbb{Z}_n^{\times}.$$

Proof: Let $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ be an automorphism. We view $\mathbb{Z}_n = \langle [1]_n \rangle$, and write 1 in place of $[1]_n$ (abuse of notation). Since α is an automorphism, its values are completely determined by $\alpha(1)$, because for an $[k]_n \in \mathbb{Z}_n$,

$$\alpha(k) = \alpha(\underbrace{1+1+\cdots+1}_{k \text{ times}}) = \underbrace{\alpha(1)+\alpha(1)+\cdots+\alpha(1)}_{k \text{ times}} = k\alpha(1) \quad (1)$$

where k is an integer – take it as one of $0, 1, 2, \dots, n-1$. In (1) we have used the property that α is operation preserving. However, since we want α to be a bijection, we want the values $k\alpha(1)$ as k runs through $0, 1, 2, \dots, n-1$, to generate all of $\mathbb{Z}_n$. This means we want $\alpha(1)$ to be a generator of $\mathbb{Z}_n$, which means $\alpha(1) \in U(n)$, since $(\alpha(1), n) = 1$. Also if $\alpha(1) \in U(n)$, the $[k\alpha(1)]_n$, for $k = 0, 1, 2, \dots, n-1$, will yield all values of $\mathbb{Z}_n$. Thus we can consider a map

$$\left.\begin{array}{rcl} T : \mathrm{Aut}(\mathbb{Z}_n) & \longrightarrow & U(n) \\ \alpha & \longrightarrow & [\alpha(1)]_n \end{array}\right\} \quad T(\alpha) = \alpha(1). \quad (2)$$

given by

The discussion above says this map is well defined, and all values of α are determined by the value $\alpha(1)$.

Next we prove that this map is one-to-one. Suppose α & $\beta \in \mathrm{Aut}(\mathbb{Z}_n)$, and $\alpha \neq \beta$. When two functions are not the same, but have the same domain (in this case $\mathbb{Z}_n$), what this implies is that $\exists$ some $k \in \mathbb{Z}_n$ for which $\alpha(k) \neq \beta(k)$. This is the same as saying

$$\alpha(k) = k\alpha(1) \not\equiv \beta(k) = k\beta(1)$$

This would yield $\alpha(1) \not\equiv \beta(1) \pmod n$ ie $\alpha(1) \neq \beta(1)$ (abuse of notation). Hence the map T is one-to-one. The map T is clearly onto, as per the discussion above. Thus T is a bijection.

Finally we need to confirm that T is operation preserving, where the operation in $\mathrm{Aut}(\mathbb{Z}_n)$ is composition, and on $U(n)$ is multiplication mod n.

Consider $\alpha, \beta \in Aut(Z_n)$. Then

$$T(\alpha \circ \beta) = \alpha \circ \beta(1) = \alpha(\beta(1)) = \alpha(\underbrace{1+1+\cdots+1}_{\beta(1) \text{ times}})$$

$$= \underbrace{\alpha(1) + \alpha(1) + \cdots + \alpha(1)}_{\beta(1) \text{ times}} \quad (\text{since } \alpha \text{ is operation preserving})$$

$$= \alpha(1) \cdot \beta(1). = T(\alpha) \cdot T(\beta).$$

Hence $T: Aut(Z_n) \to U(n)$ is an isomorphism and this proves the theorem.

Problems from Chapter 6.

Problems 4 & 5, p.132: Prove that $U(8) \not\simeq U(10)$ but $U(8) \simeq U(12)$.

Proof: $U(8) = \{1, 3, 5, 7\}$ (abuse of notation)

All elements x of $U(8)$ satisfy $x^2 \equiv 1 \pmod 8$ ie $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$.

On the other hand

$U(10) = \{1, 3, 7, 9\}$ but $|3| = 4$, because $3, 3^2 = 9, 3^3 = 27 \equiv 7, 3^4 = 81 \equiv 1$ ~~(mod~~

There are no elements of order 4 in $U(8)$. Thus $U(8) \not\simeq U(10)$, even though $|U(8)| = |U(10)|$.

Next note that

$U(12) = \{1, 5, 7, 11\}$ & $1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$.

ie all elements of $U(12)$ satisfy $x^2 \equiv 1 \pmod{12}$

Consider that map

$$\phi: U(8) \to U(12)$$

given by $[1]_8 \to [1]_{12}$, $[3]_8 \to [5]_{12}$, $[5]_8 \to [7]_{12}$ & $[7]_8 \to [11]_{12}$

This gives an isomorphism (check this)

Read Example 15 on p 130 as an illustration of Theorem 6.5.

Problem 12, p. 132: Let G be a group. Prove that $\alpha(g) = g^{-1}$ $\forall g \in G$ is an automorphism, if and only if G is Abelian.

Proof. We know that $\left.\begin{array}{l}\alpha: G \to G \\ g \to g^{-1}\end{array}\right\}$ $\alpha(g) = g^{-1}$ is a bijection and hence a permutation of G.

So we need only prove that it is operation preserving iff G is Abelian.

Suppose G is Abelian. Let $g, h \in G$. Then

$\alpha(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \alpha(g)\alpha(h)$.

So α is operation preserving.

Conversely if α is operation preserving, then for $\forall\, g, h \in G$, we have

$\alpha(gh) = (gh)^{-1} = h^{-1}g^{-1} = \alpha(g)\alpha(h) = g^{-1}h^{-1}$.

So we have

$$h^{-1}g^{-1} = g^{-1}h^{-1}, \quad \forall\, g, h \in G. \qquad (3)$$

Since g^{-1}, h^{-1} run through all elements of G as g, h range over G.

we see from (3) that

$$hg = gh \quad \forall\, g, h \in G.$$

Hence G is Abelian.

Problem 14, p 133: Find groups G and H such that $G \not\simeq H$ but $\mathrm{Aut}(G) \simeq \mathrm{Aut}(H)$.

Solution: Let $G = \mathbb{Z}$ and $H = \mathbb{Z}_3$. Then

$\mathrm{Aut}(G) = \mathrm{Aut}(\mathbb{Z}) \simeq \mathbb{Z}_2$ (by problem 2 worked out above)

& $\mathrm{Aut}(H) \simeq U(3) = \{1, 2 \pmod 3\}$ under multiplication mod 3

$\simeq \mathbb{Z}_2 = \{0, 1 \pmod 2\}$ under addition mod 2.

Thus

$$\mathrm{Aut}(G) \simeq \mathrm{Aut}(H).$$

Clearly $G \not\simeq H$ because $|G| = \infty$ & $|H| = 3$.
