Math 417 – Sixteenth Day – Class

Bruce Reznick
University of Illinois at Urbana-Champaign

September 30, 2020

I'll start again from the inbox, with answers to questions.

1. When you were talking about the isomorphisms of V, and the permutation $\{\pi(X), \pi(Y), \pi(Z)\}$, Permutation is just the reordering of the elements in a set, right?

Exactly. Two permutations are $\pi(X) = Y, \pi(Y) = X, \pi(Z) = Z$ and $\pi(X) = Y, \pi(Y) = Z, \pi(Z) = X$.

2. When we took into account u does not equal to v, why did we include a third element and compare the third element? Is it because u, v are already two elements of the set $\{X, Y, Z\}$?

This was because $X * Y = Z, Z * X = Y$, etc for all choices, so if the three elements are $\{u, v, w\}$, then $u * v = w$.

3. Is homomorphism the general concept and then isomorphism a special case of homomorphism and automorphism a special case of isomorphism?

Yes.

4. When we are proving that a function map is an automorphism, do we need to prove that it is a homomorphism first, then that it is injective to itself, and surjective to itself?

Not always. The order of proof doesn't matter. If you see that a map it isn't surjective, for example, then it can't be an automorphism, and you don't have to do anything else.

But an automorphism is a special kind of isomorphism, and the map in an isomorphism has to be a bijection, so at some point you have to prove that it is one-to-one and onto.

5. Why does $\phi(12) = 4$ and why did we do $\phi(11) = 11 - 1 = 10$? Is it related to the numbers that are relatively prime to n?

Yes, $\phi(n)$ is the number of integers less than n which are relatively prime to n. The formula is that if p is a prime, $\phi(p^k) = p^k - p^{k-1}$, and if n is given in terms of its prime factorization,

$$n = p_1^{k_1} \cdots p_r^{k_r} \implies$$
$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$$

We have $11 = 11^1$ and $\phi(11) = 11 - 1$; $12 = 2^2 \cdot 3$, so $\phi(12) = (2^2 - 2^1)(3 - 1) = (4 - 2)(3 - 1) = 2 \cdot 2 = 4$.

6. For the exam, what sections of the book should I focus my studying on?

The material is mostly from sections 4,5,6,8,9,10,11,13,14, but the main thing to do is to look at the sort of questions that have been on the homework and in the worksheet questions. I will have by Monday a list of vocabulary, ideas and theorems that you should know for the exam

Remember that $Aut(G)$, the set of automorphisms of G is a group. We gave one general construction of automorphisms, the conjugations: i_g given by $i_g(x) = gxg^{-1}$; these are called inner automorphisms. Let $Aut_I(G) = \{i_g \mid g \in G\}$.

As always, $Aut_I(G)$ is the *set* of all inner automorphisms, if $i_g = i_h$, then it's only counted once in the set; if G is abelian, we've already seen that $Aut_I(G)$ consists of the identity map

THEOREM The set of inner automorphisms $Aut_I(G)$ is a subgroup of $Aut(G)$.

PROOF The proof is pretty fast. We have

$$(i_g * i_h)(x) = i_g(i_h(x)) = i_g(hxh^{-1}) = g(hxh^{-1})g^{-1}$$
$$= (gh)x(h^{-1}g^{-1}) = (gh)x(gh)^{-1} = i_{gh}(x).$$

so $Aut_I(G)$ is closed under $*$. For all x, $i_e(x) = exe^{-1} = x$, so the identity element in $Aut(G)$ is contained in $Aut_I(G)$. And from the above $i_g * i_{g^{-1}} = i_e$, so it contains inverses as well. □

WORKSHEET PROBLEM

Let $G = S_3 \times (\mathbb{Z}/2\mathbb{Z}, \oplus)$. That is, the elements of G consist of the ordered pairs (g, h), where $g \in S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ and $h \in \{[0]_2, [1]_2\}$, with the respective operations on each component:

$$(\rho_1, [1]_2) * (\mu_1, [1]_2) = (\rho_1\mu_1, [1]_2 \oplus [1]_2) = (\mu_3, [0]_2), \quad \text{etc.}$$

1. Determine $H = \langle(\rho_1, [1]_2)\rangle$, explain (quickly!) why it is a normal subgroup, and give a homomorphism ϕ from H to $C_2 = \langle a\rangle, a^2 = e$ for which $Ker(\phi) = H$.

2. "Extra credit". Find a subgroup of S_5 which is isomorphic to H.

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Let's start by taking the powers of $x = (\rho_1, [1]_2)$

$$
\begin{aligned}
x^2 &= x * x = (\rho_1\rho_1, [1]_2 + [1]_2) = (\rho_2, [0]_2),\\
x^3 &= x * x^2 = (\rho_1\rho_2, [1]_2 + [0]_2) = (\rho_0, [1]_2),\\
x^4 &= x * x^3 = (\rho_1\rho_0, [1]_2 + [1]_2) = (\rho_1, [0]_2),\\
x^5 &= x * x^4 = (\rho_1\rho_1, [1]_2 + [0]_2) = (\rho_2, [1]_2),\\
x^6 &= x * x^5 = (\rho_1\rho_2, [1]_2 + [1]_2) = (\rho_0, [0]_2),
\end{aligned}
$$

So $x^6 = \mathrm{e}$ and $H = \langle x \rangle$ is a cyclic group of order 6. Since $|S_3 \times C_2| = 6 \times 2 = 12$, $[G : H] = 12/6 = 2$ and H is normal. Write $G = H \cup uH$, then ϕ would have to be defined as

$$
\begin{aligned}
\phi((g, h)) &= e, \quad \text{if } (g, h) \in H,\\
\phi((g, h)) &= a, \quad \text{if } (g, h) \in uH \qquad \text{or } (g, h) \notin H.
\end{aligned}
$$

2. Notice that the first and second component have nothing to do with each other, and I'd make the association $\Phi(x) = (123)(45)$, which has a cycle of order three and a cycle of order two that don't interact.

$$\Phi(x^0) = \Phi((\rho_0, [0]_2)) = (1)(2)(3)(4)(5),$$
$$\Phi(x^1) = \Phi((\rho_1, [1]_2)) = (123)(45),$$
$$\Phi(x^2) = \Phi((\rho_2, [0]_2)) = (132)(4)(5),$$
$$\Phi(x^3) = \Phi((\rho_0, [1]_2)) = (1)(2)(3)(45),$$
$$\Phi(x^4) = \Phi((\rho_1, [0]_2)) = (123)(4)(5),$$
$$\Phi(x^5) = \Phi((\rho_2, [1]_2)) = (132)(45).$$

You should check that Φ is an isomorphism from H to $\langle (123)(45) \rangle$; that is, from one cyclic group of order six to another one.

In the same way, H is isomorphic to $\langle (123456) \rangle \subset S_6$.