Math 417 – Eighth Day – Class

Bruce Reznick
University of Illinois at Urbana-Champaign

September 11, 2020

A few general remarks about homeworks.

I'm not very happy when I see an answer with no explanation. A good explanation can give substantial partial credit when the answer has a glitch. I can also help you understand better when I know what you are thinking.

As I've said, I encourage you to work together on the homework, but please check your work before you submit it. It's awkward for me to see the identical silly typo in several papers!

On HW 1, I will weight problem 5 less, but usually all problems have equal weight.

Just some quick review. Suppose you have a group $(G, *)$ and its multiplication table. For any $x \in G$, you can write down the powers from only looking at the table $x^2 = x * x, x^3 = x * (x^2)$.

In some cases, you are lucky and find that $e, x, x^2, \cdots, x^{m-1}$ are distinct and are the elements of G in some order and that $x^m = e$. In this case, $(G, *)$ is a cyclic group of order m.

So, for example, you showed in HW1 that $((\mathbb{Z}/14\mathbb{Z})^*, \odot)$ is a cyclic group of order 6 with generators $[3]_{14}$ or $[5]_{14}$. You can work out the powers just from looking at the table. You don't have to calculate 5^5 and reduce it mod 14.

$(\mathbb{Z}/14\mathbb{Z})^*$	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	15	3	1

Look at the powers: $5^2 = 5 * 5 = 11$, $5^3 = 5 * 5^2 = 5 * 11 = 13$, $5^4 = 5 * 5^3 = 5 * 13 = 9$, $5^5 = 5 * 5^4 = 5 * 9 = 3$, $5^6 = 5 * 3 = 1$.

Also, $11^2 = 11 * 11 = 9$, $11^3 = 11 * 11^2 = 9 * 11 = 1$, so $\langle\{[11]_{14}\rangle$ is a cyclic subgroup of order 3.

For fun, notice that $13 \equiv -1 \mod 14$, How do you make an isomorphism from a $G = \langle x \rangle$ that is cyclic with order m and generator x with the more familiar $C_m = \langle a \rangle$? It is very easy: define Φ so that

$$\Phi(a^k) = x^k.$$

Then $\Phi(a^k * a^j) = \Phi(a^{k+j}) = x^{k+j} = x^k * x^j$, $\Phi(a^m) = x^m = e$, etc. So to give an isomorphism from C_6 to $((\mathbb{Z}/14\mathbb{Z})^*, \odot)$, one is

$$\begin{aligned}
\Phi(e) &= [1]_{14}, \\
\Phi(a) &= [3]_{14}, \\
\Phi(a^2) &= [3^2]_{14} = [9]_{14}, \\
\Phi(a^3) &= [3^3]_{14} = [9 * 3]_{14} = [13]_{14}, \\
\Phi(a^4) &= [3^4]_{14} = [13 * 3]_{14} = [11]_{14}, \\
\Phi(a^5) &= [3^5]_{14} = [11 * 3]_{14} = [5]_{14}.
\end{aligned}$$

You could give a second isomorphism Φ' by $\Phi'(a) = [5]_{14}$, because $(\mathbb{Z}/14\mathbb{Z})^* = \langle [3]_{14} \rangle = \langle [5]_{14} \rangle$. Any generator will do.

How do you check that a subset H of a group $(G, *)$ is a subgroup? You check that it is closed under $*$, that it contains the identity and that it contains the inverses of every element in it.

One type of subgroup works for every group $(G, *)$. For $x \in G$ take $\langle x \rangle$. This will always be closed under $*$, it has the identity and inverses.

When G is a cyclic group, this is the only possible kind of subgroup: The subgroups of C_n are $\langle x^k \rangle$, where k divides n.

It is possible for G to be not a cyclic group and this is true for proper subgroups too: take V or S_3.

I think we already saw that the only subgroups of V are

$$\{e\}, \{e, X\}, \{e, Y\}, \{e, Z\}, \{e, X, Y, Z\}$$

Here's the multiplication table for S_3

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 find all the subgroups of S_3.

The identity ρ_0 is in every subgroup. Suppose H is a subgroup of G and $\rho_1 \in H$. Then $\rho_1 \circ \rho_1 = \rho_2 \in H$ and since $\rho_1^3 = \rho_0$, $\langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}$ is a subgroup of S_3.

You can also check that $\langle \rho_2 \rangle = \{\rho_0, \rho_1, \rho_2\}$. Suppose H is a subgroup that contains ρ_2. The same argument shows that H contains $\{\rho_0, \rho_1, \rho_2\}$.

Now suppose a subgroup H contains all the ρ_j's and one of the μ_i's. One look at the multiplication table shows that you get the other two μ_i's as well, so $H = S_3$.

So any other subgroup cannot have ρ_1 or ρ_2. If it has one μ_j, since $\mu_j \circ \mu_j = \rho_0$, we have the three subgroups $\langle \mu_j \rangle = \{\rho_0, \mu_j\}$.

Suppose a subgroup H has two different μ_j's, say μ_j and μ_k. Then it has $\mu_j \circ \mu_k$, which will be ρ_1 or ρ_2, so we get all of S_3.

This gets harder as the groups get larger.

WORKSHEET PROBLEM

1. Suppose α and β are two permutations in S_5 given by

$$\alpha = \begin{pmatrix} 12345 \\ 24135 \end{pmatrix} = (1243)(5), \qquad \beta = \begin{pmatrix} 12345 \\ 35124 \end{pmatrix},$$

a. Write β in cycle form.

b. Compute $\alpha \circ \beta$. (Remember that $(\alpha \circ \beta)(i) = \alpha(\beta(i))$.)

WORKSHEET PROBLEM SOLUTION

For reference:

$$\alpha = \begin{pmatrix} 12345 \\ 24135 \end{pmatrix}, \qquad \beta = \begin{pmatrix} 12345 \\ 35124 \end{pmatrix},$$

a. So $\alpha = (1243)(5)$ and $\beta = (13)(254)$ and $\alpha(\beta(i))$ is given by

$$\begin{aligned}
\alpha(1) = 2 \quad \beta(1) = 3 &\implies (\alpha \circ \beta)(1) = \alpha(3) = 1 \\
\alpha(2) = 4 \quad \beta(2) = 5 &\implies (\alpha \circ \beta)(2) = \alpha(5) = 5 \\
\alpha(3) = 1 \quad \beta(3) = 1 &\implies (\alpha \circ \beta)(3) = \alpha(1) = 2 \\
\alpha(4) = 3 \quad \beta(4) = 2 &\implies (\alpha \circ \beta)(4) = \alpha(2) = 4 \\
\alpha(5) = 5 \quad \beta(5) = 4 &\implies (\alpha \circ \beta)(5) = \alpha(4) = 3.
\end{aligned}$$

so

$$\alpha \circ \beta = \begin{pmatrix} 12345 \\ 15243 \end{pmatrix} = (1)(253)(4).$$

Have a good and safe weekend!