MATH 375.15

Class 15: Selected Answers

1. **a)** Gallian page 109 #38. **Solution:** Any two non-identical 2-cycles will work, e.g., $\alpha\beta = (12)(13) = (132)$. $|\alpha| = |\beta| = 2$ and $|\alpha\beta| = 3$.

b) Gallian p. 109 #32. **Solution:** $|\beta| = |(1357986)(2,4,10)| = \text{lcm}(7,3) = 21$. Then $\beta^n = \beta^{-5} \iff \beta^{n+5} = e \iff 21 \mid n+5$. The smallest such n is 16.

2. Let k be a *fixed* integer such that $1 \le k \le n$. Let $\text{stab}(k) = \{\alpha \in S_n \mid \alpha(k) = k\}$. That is, $\text{stab}(k)$ is the set of permutations that leaves k alone. Is $\text{stab}(k)$ a subgroup of S_n? **Solution:** Since S_n is finite, $\text{stab}(k)$ is finite. So we can apply the Finite Subgroup Test. We need to show that $\text{stab}(k)$ is closed. So let $\alpha, b \in \text{stab}(k)$. Then $\alpha(k) = k$ and $\beta(k) = k$. So $(\alpha\beta)(k) = \alpha(\beta(k)) = \alpha(k) = k$. That is, $\alpha\beta \in \text{stab}(k)$.

3. Let G be a group and let a be a *fixed* element of G. Let $\phi : G \to G$ by $\phi(g) = aga^{-1}$.

a) Show that ϕ is injective. **Solution:** Note that by cancellation.

$$\phi(g) = \phi(h) \iff aga^{-1} = aha^{-1} \iff g = h.$$

So ϕ is injective.

b) Show that ϕ is surjective. **Solution:** Let $b \in G$. We must find $g \in G$ so that $\phi(g) = b$. But

$$\phi(g) = b \iff aga^{-1} = b \iff g = a^{-1}ba.$$

Note that $g = a^{-1}ba \in G$ since G is a group and it closed and has inverses.

c) Show that ϕ is a group isomorphism. **Solution:** We've shown injectivity, and surjectivity, so all we need to do is show that ϕ is a homomorphism. Let $g, h \in G$. Then

$$\phi(g)\phi(h) = (aga^{-1})(aha^{-1}) = ag(a^{-1}a)ha^{-1} = a(gh)a^{-1} = \phi(gh).$$

4. **a)** The following is part of a theorem about homomorphisms that we stated in class, but did not prove. Suppose that $\phi : G_1 \to G_2$ is a group homomorphism. Prove by induction that $\phi(a^n)\phi = [\phi(a)]^n$. **Solution:** Base Case: Let $n = 0$. Then $f(a^0) = f(e_1) = e_2 = [f(a)]^0$ since we proved that any homomorphis does map the identity of the domain to the identity of the codomain. Inductive Step: Assume that $\phi(a^n)\phi = [\phi(a)]^n$. Prove that $\phi(a^{n+1}) = [\phi(a)]^{n+1}$. But by the inductive hypothesis and the definition of a group homomorphism

$$\phi(a^{n+1}) = \phi(aa^n) = \phi(a)\phi(a^n) = \phi(a)[\phi(a)]^n = [\phi(a)]^{n+1}.$$

Finally, consider negative integers. By what we have already shown and by the fact that group homomorphisms respect inverses, i.e., $f(a^{-1}) = (f(a))^{-1}$, then

$$f(a^{-n}) = f[(a^{-1})^n] = f[(a^{-1})]^n = [[f(a)]^{-1}]^n = [f(a)]^{-n}.$$

b) Use this (in its additive form) to show that if $\phi : \mathbf{Z}_n \to \mathbf{Z}$ is a homomorphism, then $\phi(j) = 0$ for all $j \in \mathbf{Z}_n$. **Solution:** Note that if $j \in \mathbf{Z}_n$, then $n \cdot j = 0$, while if $k \in \mathbf{Z}$, then $n \cdot k = 0 \Rightarrow k = 0$. So let $j \in \mathbf{Z}_n$. Then $\phi(nj) = \phi(0) = 0$ because any homommorphism maps the identity in the first group to the identity in the second. Next, because ϕ is a homomorphism, we just showed that $\phi(nj) = n \cdot \phi(j)$. So combining these two observations, $n \cdot \phi(j) = 0$ in $\mathbf{Z}$ which only happens if $\phi(j) = 0$ (since $\mathbf{Z}$ is infinite cyclic). Here's another solution. Since $j \in \mathbf{Z}_n$, by Sma's Theorem, $|j| \Big| n$. (So $|j|$ is finite.) On the other hand, Let $\phi(j) = k \in \mathbf{Z}$. $k \in \mathbf{Z}$, so

$$|k| = \begin{cases} \infty, & \text{if } k \neq 0 \\ 1, & \text{if } k = 0. \end{cases}$$

But one of the basic properties of a group homomorphism is that $|\phi(j)| \Big| |j|$. Since $|j|$ is finite, we must have $|\phi(j)| = |k|$ also finite. Therefore, $|\phi(j)| = 1$, and so $\phi(j) = 0$.

5. Recall that the natural log function is important in calculus. Show that $f : \mathbf{R}^+ \to \mathbf{R}$ by $f(x) = \ln x$ is an injective, surjective group homomorphism. Be careful! The two group operations are different. **Solution:** Injective: From Calculus, we know that

$$f(x) = f(y) \iff \ln x = \ln y \iff e^{\ln x} = e^{\ln y} \iff x = y.$$

Surjective: Let $y \in \mathbf{R}$. Then $f(x) = \ln x = y \iff x = e^y$. Note that $e^y \in \mathbf{R}^+$. Homomorpism: Note that the operation in $\mathbf{R}^+$ is multiplication and the operation in $\mathbf{R}$ is addition. But one of the basic log rules says that

$$\phi(xy) = \ln(xy) = \ln x + \ln y = \phi(x) + \phi(y).$$

6. Is the mapping $\phi : \mathbf{C}^* \to \mathbf{C}^*$ by $(a+bi)\phi = a - bi$ a group isomorphism? **Solution:** Let $a+bi, c+di \in \mathbf{C}^*$. Then

$$\phi(a+bi)\phi(c+di) = (a-bi)(c-di) = ac - bd - (ad+bc)i.$$

Compare this to

$$\phi((a+bi)(c+di)) = \phi(ac - bd + (ad+bc)i) = ac - bd - (ad+bc)i.$$

They are the same, so ϕ is a homomorphism.

7. The following is part of a theorem about isomorphisms that we stated in class, but did not prove. Let $\phi : G_1 \to G_2$ be a group isomorphism. Then:

a) Prove that if $a, b \in G_1$ commute, then $\phi(a), \phi(b) \in G_2$ commute. **Solution:** Assume $a, b \in G_1$ commute. Show that $\phi(a)\phi(b) = \phi(b)\phi(a)$. But we are given that $ab = ba$, so by the definition of a homomorphism,

$$\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a).$$

b) Prove that if G_1 is abelian, then G_2 is abelian. **Solution:** Let $c, d \in G_2$. We must show that $cd = dc$. But ϕ is onto since it is an isomorphism. Therefore, there exist $a, b \in G_2$ so that $\phi(a) = c$ and $\phi(b) = d$. By the previous part, since G_1 is abelian, then a and b commute, hence so do $\phi(a)$ and $\phi(b)$. Therefore,

$$cd = \phi(a)\phi(b) = \phi(b)\phi(a) = dc.$$

8. **a)** Notice that we can write the 5-cycle $(12345) = (145)(123)$ as a product of 3-cycles. Write (1234567) as a product of 3-cycles. Write $(a_1a_2a_3a_4a_5a_6a_7a_8a_9)$ as a product of 3-cycles. Write the 1-cycle $e = (1)$ as a product of 3-cycles (assuming that we are are in S_k with $k \geq 3$.) **Solution:** $(1234567) = (167)(145)(123)$.

$$(a_1a_2a_3a_4a_5a_6a_7a_8a_9) = (a_1a_8a_9)((a_1a_6a_7)(a_1a_4a_5)(a_1a_2a_3).$$

$(1) = (123)(321)$.

b) Ok, you should have the idea by now. Let $(a_1a_2a_3\ldots a_{2n}a_{2n+1})$ be any odd length cycle in S_k where $k \geq 3$. Prove *by induction* that such odd length cyles can be written as a 3-cycle or a product of 3-cycles. **Solution:** Base Case: For $n = 0$ this reduces to writing $(a_))= (1)$ as product of 3-cycles. This is done above. Inductive Step: Assume that $(a_1a_2a_3\ldots a_{2n}a_{2n+1})$ can be written as a product of 3-cycles. Show that $(a_1a_2a_3\ldots a_{2n}a_{2n+1}a_{2(n+1)}a_{2(n+1)+1})$ can be written as product of 3-cycles. But

$$(a_1a_2a_3\ldots a_{2n}a_{2n+1}a_{2(n+1)}a_{2(n+1)+1}) = (a_1a_{2(n+1)}a_{2(n+1)+1})(a_1a_2a_3\ldots a_{2n}a_{2n+1}),$$

where by assumption the second permutation is a product of 3-cycles.

9. Extra Credit: D_{12} has 24 elements (12 rotations which are generated by r_{30} the rotation of 30 degrees and 12 flips). S_4 also has 24 elements. Both groups are not cyclic and neither is abelian. Are they isomoprphic? Hint: what is the maximum order of an element in S_4? Is the same true about D_{12}?

10. Extra Credit: Is D_4 is isomorphic to Q_8? Compare their tables and see if you can match up the entries. If you can, that matching is the isomorphism.

11. Extra Credit: Page 128, #27. ($M^{\#}$ means that the zero matrix is not included.)

12. Extra Credit: Let a be a fixed element in $U(n)$. Let $\phi : \mathbf{Z}_n \to \mathbf{Z}_n$ by $b\phi = ab \bmod n$.

a) Show that ϕ is a homomorphism.

b) Show that ϕ is injective. Hint: Suppose that $b\phi = c\phi$. Write out what this means mod n. (Eculid's Lemma will be very useful here. If n, a and d are integers such that $n \mid ad$ and $\gcd(n, a) = 1$, then $n \mid d$.)

c) ϕ is surjective. Try to show it. There are lots of ways to do it. Some are easy and some are hard.