Math 3140 — Fall 2012
Assignment #2

Due Fri., Sept. 14. Remember to cite your sources.

Exercise 2. [Fra, §4, #9]. Let U be the set of complex numbers of absolute value 1.

(a) Show that U is a group under multiplication of complex numbers.

Solution. First we check that the group operation is well-defined: suppose that $|z| = |w| = 1$. Then $|zw| = |z| \cdot |w| = 1$. Therefore if $z, w \in U$, so is zw.

The identity element is $1 = 1 + 0i$. The inverse of $z = x + iy$ is $\overline{z} = x - iy$ since $z\overline{z} = |z|^2 = 1$. Finally, associativity comes from the associativity of complex multiplication. It's okay to treat this fact as known, but if you don't cite it you have to check:

$$((a + ib)(c + id))(e + if) = (a + ib)((c + id)(e + if)).$$

□

(b) Show that U is not isomorphic to $\mathbf{R}$ (with its additive group structure).

Solution. Consider $-1 \in U$. We have $(-1)^2 = 1$ in U. If $\varphi : U \to \mathbf{R}$ is a homomorphism then $\varphi(-1)$ is an element $x \in \mathbf{R}$ such that $2x = 0$. The only such element is $x = 0$. Therefore $\varphi(-1) = 0$. This proves that no homomorphism $U \to \mathbf{R}$ can be injective. In particular, there can be no isomorphism (bijective homomorphism) $U \to \mathbf{R}$. □

Solution. Now that we have the notion of a subgroup, a more efficient solution to this problem is possible: we show that U is a subgroup of $\mathbf{C}^*$. Since $1 \in U$, we know that $U \neq \varnothing$. If $z, w \in U$ then we check that $zw^{-1} \in U$. We have to check that $|zw^{-1}| = 1$ if $|z| = |w| = 1$. Remember that $|w^{-1}| = |w|^{-1}$ so that we have

$$\left|zw^{-1}\right| = \left|z\right|\left|w\right|^{-1} = 1 \cdot 1^{-1} = 1.$$

□

(c) Show that U is not isomorphic to $\mathbf{R}^*$ (with its multiplicative group structure).

Solution. Consider $i \in U$. We have $i^4 = 1$. Therefore if $\varphi : U \to \mathbf{R}^*$ is a homomorphism we will have $\varphi(i)^4 = 1$. The only solutions to this are $\varphi(1) = \pm 1$. But then we will have

$$\varphi(-1) = \varphi(i^2) = (\pm 1)^2 = 1$$

so φ cannot be injective. □

Hint: it might help to think about Exercise 13 while thinking about this one.

Comments. Several people seemed confused about the definition of multiplication of complex numbers. Remember:

$$(a + ib)(c + id) = ac + iad + ibc + i^2bd = (ac - bd) + i(ad + bc)$$

because $i^2 = -1$.

A frequent mistake was to forget to verify that the group operation is well-defined. You have to make sure that if $z, w \in U$ then $zw \in U$ as well. □

Exercise 13. Suppose that G is a group. An element $x \in G$ is said to have **order** n if $x^n = e$ but $x^k \neq e$ for $0 < k < n$. If no such n exists, we say that x has infinite order.

(a) What is the order of the identity element e?[1] $\leftarrow_1$

Solution. We have $e^1 = e$ and there is no integer k with $0 < k < 1$ so $\mathrm{ord}(e) = 1$. □

(b) Compute the orders of all of the elements of the symmetric group S_3.

Solution.

$$\begin{aligned} \mathrm{ord}(e) &= 1 & \mathrm{ord}((12)) &= 2 & \mathrm{ord}((13)) &= 2 \\ \mathrm{ord}((23)) &= 2 & \mathrm{ord}((123)) &= 3 & \mathrm{ord}((132)) &= 3. \end{aligned}$$

□

(c) Give an example of a group with more than one element where every element other than e has infinite order.

Solution. Let $G = \mathbf{R}$. If $x \in \mathbf{R}$ and x has finite order then $nx = 0$ for some $n \in \mathbf{Z}$ other than $n = 0$. But then $x = \frac{1}{n}0 = 0$. Therefore $x = 0$ is the only element of $\mathbf{R}$ of finite order. □

(d) Give an example of an infinite group where every element has finite order. (Hint: look for a subgroup of U.)

[1] clarification added; thanks Rachel Benefiel

Solution. The simplest example is probably $\mathbf{Q}/\mathbf{Z}$, but we haven't discussed quotient groups yet. Let G be the set of all elements of U of the form $e^{iq} = \cos(\theta) + i\sin(\theta)$ where $\theta = 2\pi q$ for some rational number q. These elements form a subgroup of U because they are a non-empty subset and if $x = e^{2\pi iq}$ and $y = e^{2\pi ir}$ are in G then $y^{-1} = e^{-ir}$ and

$$xy^{-1} = e^{2\pi iq}e^{-2\pi ir} = e^{2\pi i(q-r)}$$

is in G. If $q = a/b$ and $x = e^{2\pi iq}$ then $x^b = e^{2\pi iqb} = e^{2\pi ia} = 1$ because a is an integer. Therefore x has finite order (it might not actually have order b, but it has some order dividing b). □

Exercise 14. Prove that S_3 is not isomorphic to $\mathbf{Z}/6\mathbf{Z}$, the group of integers modulo 6.[2] $\leftarrow_2$

Solution. Here is one way: $\mathbf{Z}/6\mathbf{Z}$ is abelian because $a + b \pmod 6 = b + a \pmod 6$; on the other hand, $(12)(23) = (123)$ and $(23)(12) = (132)$ in S_3 so S_3 is not abelian. If $\varphi : S_3 \to \mathbf{Z}/6\mathbf{Z}$ were an isomorphism then

$$\varphi((123)) = \varphi((12)(23)) = \varphi((12))+\varphi((23)) = \varphi((23))+\varphi((12)) = \varphi((23)(12)) = \varphi((132))$$

so φ is not injective.

Here is another: $\mathbf{Z}/6\mathbf{Z}$ contains an element—1—whose order is 6, while we saw in the previous exercise that S_3 only contains elements of orders 1, 2, and 3. Since an isomorphism has to preserve the orders of elements, there is nowhere an isomorphism $\varphi : \mathbf{Z}/6\mathbf{Z} \to S_3$ could send 1: if φ were an isomorphism then $\varphi(1)$ would have order 6 and there is no element of order 6 in S_3.

Here is yet another: $\mathbf{Z}/6\mathbf{Z}$ contains one element of order 2—it's 3—while we have just seen S_3 has 3 elements of order 2. If $\varphi : S_3 \to \mathbf{Z}/6\mathbf{Z}$ were an isomorphism then it would send the set of elements of order 2 in S_3 to the set of elements of order 2 in $\mathbf{Z}/6\mathbf{Z}$. But the latter set has only 1 element while the former has 3. Therefore φ cannot be injective on the subset of elements of order 2 of S_3. In particular, φ takes two elements of S_3 to the same element of $\mathbf{Z}/6\mathbf{Z}$ so φ can't be injective, hence can't be an isomorphism. □

Comments. I saw many arguments of the following form: "S_3 is abelian and $\mathbf{Z}/6\mathbf{Z}$ is not abelian; this is a structural property so the groups are not isomorphic." This argument is totally correct, but it's dangerous to get in the habit of claiming properties are structural without doing some verification; invariably someone will identify a non-structural property and claim without proof that it is structural, then use it to conclude incorrectly that two groups can't be isomorphic. □

Exercise 15. Suppose that G is a group and x is an element of G. Prove that the function $\varphi : G \to G$ defined by

$$\varphi(y) = xyx^{-1}$$

[2]this is the set $\{0, 1, 2, 3, 4, 5\}$ with addition modulo six as the group operation

is an isomorphism from G to itself. An isomorphism from a group to itself is called an **automorphism**.

Solution. First we check φ is a homomorphism. We have

$$\varphi(y)\varphi(z) = xyx^{-1}xzx^{-1} = xyzx^{-1} = \varphi(yz)$$

so φ is a homomorphism. Also, φ is a bijection because the function $\psi(z) = x^{-1}yx$ is inverse to φ:

$$\begin{aligned}\psi(\varphi(y)) &= x^{-1}\varphi(y)x = x^{-1}xyx^{-1}x = y\\ \varphi(\psi(z)) &= x\psi(z)x^{-1} = xx^{-1}zxx^{-1} = z.\end{aligned}$$

□

Comments. Many people assumed that G was abelian (either implicitly or explicitly). If G is abelian then $\varphi(y) = xyx^{-1} = xx^{-1}y = y$ so φ is the identity function, which is obviously a homomorphism. The problem is only interesting when G is **not** abelian!

Do not assume multiplication is commutative unless there is a valid reason to! □

Exercise 16. Do not show your work on this problem. Consider the following permutations in S_6:

$$\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 1 & 4 & 5 & 6 & 2\end{pmatrix}$$
$$\tau = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 2 & 4 & 1 & 3 & 6 & 5\end{pmatrix}$$
$$\mu = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 5 & 2 & 4 & 3 & 1 & 6\end{pmatrix}$$

(a) [Fra, §8, #2]. Compute $\tau^2\sigma$.

Solution.
$$\tau^2\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 2 & 4 & 1 & 5 & 6 & 3\end{pmatrix} = (124563)$$

□

(b) [Fra, §8, #8]. Compute σ^{100}.

Solution. In cycle notation, $\sigma = (134562)$. Therefore $\sigma^{100} = \sigma^{6(16)+4} = (\sigma^6)^{16}\sigma^4 = \sigma^4$ since $\sigma^6 = e$. Therefore,

$$\sigma^{100} = \sigma^4 = (164)(253) = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 5 & 2 & 1 & 3 & 4\end{pmatrix}.$$

□

(c) Express μ in cycle notation.

Solution.

$$\mu = (15)(2)(34)(6) = (15)(34).$$

□

Exercise 17. Let σ be the permutaiton $(a_1 a_2 \cdots a_n)$ in cycle notation.

(a) Write σ^{-1} in cycle notation.

Solution.

$$\sigma^{-1} = (a_n a_{n-1} \cdots a_2 a_1)$$

□

(b) Write σ^2 in cycle notation. Hint: your answer may depend on n; try computing σ^2 for a few small values of n.

Solution. If n is even we get

$$\sigma^2 = (a_1 a_3 a_5 \cdots a_{n-1})(a_2 a_4 \cdots a_n).$$

If n is odd we get

$$\sigma^2 = (a_1 a_3 a_5 \cdots a_{n-2} a_n a_2 a_4 \cdots a_{n-3} a_{n-1}).$$

□

Exercise 18. Let A_4 be the subset of S_4 consisting of all permutations that are products of an **even number**[3] of transpositions. A transposition is a permutation that exchanges two things and leaves everything else stationary; in cycle notation, a transposition looks like (ab). Thus $(12)(13)$ and $(12)(24)(13)(24)$ are in A_4, but (23) and $(12)(23)(34)$ are not. ←3

Write down all of the elements of A_4 using cycle notation.[4] ←4

Solution. First of all, A_4 contains the identity and all the products of disjoint transpositions of the form $(ab)(cd)$. So A_4 contains $e, (12)(34), (13)(24), (14)(23)$. We also see that if we multiple $(ab)(bc)$ we get (abc) so A_4 also contains every 3-cycle. That is A_4 contains the eight 3-cycles,

$$(123), (124), (132), (134), (142), (143), (234), (243).$$

In fact, these are all of the elements of A_4, because the other elements of S_4 are the transpositions (ab) and the 4-cycles $(abcd) = (ab)(bc)(cd)$, each of which is a product of an odd number of transpositions. □

[3] correction: accidentally left this out before!

[4] I reworded this problem; note that you **do not** have to write down the multiplication table!

Exercise 19. [Fra, §8, #18]. List all of the subgroups of S_3.

Solution.

$$\begin{tikzcd}
 & & S_3 \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{e,(12)\} \arrow[drr, dash] & \{e,(13)\} \arrow[dr, dash] & \{e,(23)\} \arrow[d, dash] & \{e,(123),(132)\} \arrow[dl, dash] \\
 & & \{e\} &
\end{tikzcd}$$

□

Exercise 20. Suppose that G is a group. How would you define a symmetry of G?

Solution. A symmetry of G is an automorphism of G (an isomorphism from G to itself). □

Comments. This question was extra credit, since it did not have a precise answer and was merely asking for a reasonable definition. Many said that a symmetry of G would be a symmetry of the underlying set of G—that is, a bijection from this set to itself. This answer is reasonable in a sense, but it takes no account of the group structure. The correct answer is a bijection from G to itself that respects the group structure—that is, an automorphism. □

References

[Fra] John B. Fraleigh. *A first course in abstract algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., seventh edition edition, 2002. ISBN-10: 0201763907, ISBN-13: 978-0201763904.