Math 3140 — Fall 2012
Assignment #3

Due Fri., Sept. 21. Remember to cite your sources, including the people you talk to.

My solutions will repeatedly use the following proposition from class:

Proposition 1. *Let G be a group and $H \subset G$ a subset. If H is non-empty and for every $x, y \in H$ we have $xy^{-1} \in H$ as well then H is a subgroup of G.*

Exercise 12. Suppose that G is a group with 5 elements.

(a) Show that G is isomorphic to $\mathbf{Z}/5\mathbf{Z}$, the group of integers modulo 5. (Hint: Let x be a non-zero element of G and consider the permutation L_x of G induced by left multiplication by x. What could the orbits of this action look like?)

Solution. Let x be an element of G other than the identity. Then $\mathrm{ord}(x)$ divides the size of G, which is 5. Since the only divisors of 5 are 1 and 5 this means that x has order either 1 or 5. But the only element with order 1 is the identity, so this means the order of x is 5. That means that the elements of G must be $1, x, x^2, x^3, x^4$. (Indeed, if $x^a = x^b$ for $a, b < 5$ then $x^{a-b} = 1$ so $\mathrm{ord}(x)$ must divide $a - b$, which impossible becuase $|a - b| < 5$ and $\mathrm{ord}(x) = 5$.)

Now consider the function $\varphi : \mathbf{Z}/5\mathbf{Z} \to G$ defined by $\varphi(n) = x^n$. This is well-defined because if $n \equiv m \pmod 5$ we have $n - m = 5k$ for some integer k, so $x^m = x^{n+5k} = x^n(x^5)^k = x^n$ since $x^5 = 1$. Furthermore, this is a homomorphism because $\varphi(n + m) = x^{n+m} = x^n x^m = \varphi(n)\varphi(m)$. Finally, this is a bijection because if $\varphi(n) = \varphi(m)$ then $x^n = x^m$ so $x^{n-m} = 1$ so $n - m$ is a multiple of 5 so $n \equiv m \pmod 5$. $\square$

(b) Suppose p is a prime number. Up to isomorphism, how many groups are there with p elements? (You do not have to prove your answer is correct, but try to give a sentence or two of justification.)

Solution. All of the reasoning of the solution above works equally well if 5 is replaced by any prime number p. Therefore all groups with p elements are isomorphic to $\mathbf{Z}/p\mathbf{Z}$. $\square$

Exercise 21. Justify your answers below.

(a) Is $[0, 1] \subset \mathbf{R}$ a subgroup? (Recall that $[0, 1]$ is the interval of all real numbers x such that $0 \le x \le 1$.)

Solution. No: $1 \in [0,1]$ but its inverse -1 is not in $[0,1]$. $\square$

(b) Is $3\mathbf{Z} \subset \mathbf{R}$ a subgroup? (Here $3\mathbf{Z}$ is the set of integers that are multiples of 3.)

Solution. Yes: $3\mathbf{Z}$ is not empty (it contains 0, for example) and if $a, b \in 3\mathbf{Z}$ then $a = 3x$ and $b = 3y$ so $a - b = 3(x - y)$ is also in $3\mathbf{Z}$. Therefore by Proposition 1, $3\mathbf{Z}$ is a subgroup of $\mathbf{R}$. $\square$

(c) Is $\mathbf{Q} \subset \mathbf{C}$ a subgroup?

Solution. Yes: it's non-empty because $0 \in \mathbf{Q}$ and if x and y are rational numbers then so is $x - y$. Therefore by Proposition 1, $\mathbf{Q}$ is a subgroup of $\mathbf{C}$. $\square$

(d) Is $\mathbf{R} \smallsetminus \mathbf{Q} \subset \mathbf{R}$ a subgroup? (Note that $\mathbf{R} \smallsetminus \mathbf{Q}$ is the set of all irrational real numbers.)

Solution. No: $\mathbf{R} \smallsetminus \mathbf{Q}$ doesn't contain the identity! $\square$

(e) Let $A \subset D_n$ be the subset consisting of all reflections and the identity. Is A a subgroup?

Solution. If $n = 2$ then yes, this is a group: D_2 consists of two elements, a reflection and the identity. If $n > 2$ then D_n contains two different reflections τ and σ. Each of τ and σ fixed a different line. Let θ be the angle between the lines fixed by τ and σ. Then I claim $\tau\sigma$ has the effect of rotating by an angle of 2θ.

To prove this, select a ray S fixed by σ and a ray T fixed by τ such that the angle from S to T is θ. If the angle from S to a ray R is ϕ then the angle from S to $\sigma(R)$ is $-\phi$. Therefore the angle from T to $\sigma(R)$ makes an angle $-\theta - \phi$. Then the angle from T to $\tau(\sigma(R))$ will be $\theta + \phi$. The angle from S to $\tau\sigma(R)$ is therefore $2\theta + \phi$. Thus acting by $\tau\sigma$ has the effect of rotation by 2θ. $\square$

(f) Let $B \subset D_n$ be the subset of all rotations (including the identity). Is B a subgroup?

Solution. Yes. B is non-empty (contains the identity) and if σ and τ are rotations by angles θ and ϕ, respectively, then $\sigma\tau^{-1}$ is rotation by $\theta - \phi$. Therefore B is a subgroup. $\square$

Exercise 22. Suppose that $\varphi : A \to B$ is a homomorphism of groups. Let $K \subset A$ be the set of all elements $a \in A$ such that $\varphi(a) = 1$. Symbolically,

$$K = \big\{a \in A \big| \varphi(a) = 1\big\}.$$

Show that K is a subgroup of A.

Solution. We know that $\varphi(1) = 1$ by an earlier exercise so $1 \in K$. Therefore $K \neq \varnothing$. Also, if $a, b \in K$ then $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = 1 \cdot 1^{-1} = 1$ so $ab^{-1} \in K$. Therefore K is a subgroup by Proposition 1. $\square$

Exercise 23. [Arm, Exercise 5.1].

(a) Find all subgroups of $\mathbf{Z}/12\mathbf{Z}$.

Solution. The subgroups are

$$\begin{tikzcd}[arrows=dash]
& \mathbf{Z}/12\mathbf{Z} \arrow[dl] \arrow[dr] & \\
2\mathbf{Z}/12\mathbf{Z} \arrow[d] \arrow[drr] & & 3\mathbf{Z}/12\mathbf{Z} \arrow[d] \\
4\mathbf{Z}/12\mathbf{Z} \arrow[dr] & & 6\mathbf{Z}/12\mathbf{Z} \arrow[dl] \\
& \{0\}. &
\end{tikzcd}$$

The lines indicate which groups are contained in which others: if X and Y are connected by a line and X appears above Y then X contains Y. $\square$

(b) Find all subgroups of D_5.

Solution. There are 10 elements in D_5. Let ρ be a rotation by $72^\circ = \frac{2\pi}{5}$ and let τ be a reflection in D_5. Then the elements of D_5 are

$$1, \rho, \rho^2, \rho^3, \rho^4,$$
$$\tau, \tau\rho, \tau\rho^2, \tau\rho^3, \tau\rho^4.$$

The elements in the first line are reflections and the elements in the second line are rotations. Suppose that $G \subset D_5$ is a subgroup. If it contains a rotation other than the identity then it contains all rotations (since every element of $\mathbf{Z}/5\mathbf{Z}$ has order 5!) and the collection of reflections is a subgroup of D_5. Each reflection generates a subgroup with 2 elements. If a subgroup contains a non-trivial rotation and a non-trivial reflection then it must be all of D_5. Therefore we have named all of the subgroups already:

$$\begin{tikzcd}[arrows=dash]
& & D_5 \arrow[dll] \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr] \arrow[drrr] & & & \\
\langle \rho \rangle \arrow[drrr] & \langle \tau \rangle \arrow[drr] & \langle \tau\rho \rangle \arrow[dr] & \langle \tau\rho^2 \rangle \arrow[d] & \langle \tau\rho^3 \rangle \arrow[dl] & \langle \tau\rho^4 \rangle \arrow[dll] \\
& & & \{e\} & &
\end{tikzcd}$$

$\square$

Exercise 24. Suppose that G is a group and A and B are subgroups of G.

(a) Show that $A \cap B$ is also a subgroup.

Solution. If A and B are subgroups then both contain the identity $e \in G$. Therefore $e \in A \cap B$ so $A \cap B \neq \varnothing$. Also, if $a, b \in A \cap B$ then $a, b \in A$ and $a, b \in B$ so $ab^{-1} \in A$ and $ab^{-1} \in B$ so $ab^{-1} \in A \cap B$. Therefore $A \cap B$ is a subgroup by Proposition 1. $\square$

(b) Assume that G is abelian. Let $C = \{ab \big| a \in A, b \in B\}$. Show that C is a subgroup of G.

Solution. We know that C is non-empty because $e \in A$ and $e \in B$ so $e = ee \in C$. Also, if we have two elements $x, y \in C$ then $x = ab$ with $a \in A$ and $b \in B$ and $y = cd$ with $c \in A$ and $d \in B$. We have $xy^{-1} = ab(cd)^{-1} = ac^{-1}bd^{-1}$ (because G is abelian!). Furthermore, $ac^{-1} \in A$ and $bd^{-1} \in B$ because A and B are subgroups of G. Therefore their product $ac^{-1}bd^{-1} = xy^{-1}$ is in C. Therefore C is a subgroup of G by Proposition 1. $\square$

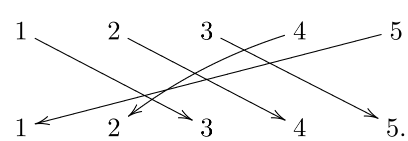
(c) Show that in the last part, the assumption G be abelian is essential by giving an example of a non-abelian group G and subgroups A and B such that if C is defined as above then C is not a subgroup of G.

Solution. Consider $G = S_3$, let $A = \{e, (12)\}$ and $B = \{e, (23)\}$. These are both subgroups but C consists of five elements: $\{e, (12), (23), (123), (132)\}$ and this is not a subgroup (it does not contain $(23)(123) = (13)$). $\square$

Exercise 25. Compute the sign of each of the following permutations:

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$

Solution. We can count the number of crossings in



There are 7 crossings so the permutation is odd. Its sign is -1.

We can also compute by writing it in cycle notation: $(135)(24) = (13)(35)(24)$. This is a product of an odd number of transpositions so its sign is -1. $\square$

(b) (1364)(25)

Solution. We can write this as a product of transpositions

$$(13)(36)(64)(25).$$

There is an even number of transpositions, so the permutation is even. Its sign is $+1$. $\square$

(c) $(a_1a_2\cdots a_n)$.

Solution. Write this as a product of transpositions:

$$(a_1a_2)(a_2a_3)\cdots(a_{n-1}a_n).$$

There are $n-1$ transpositions above, so the sign is $(-1)^{n-1}$. $\square$

Exercise 26. The first 3 parts of this problem are meant to give you ideas for the last part. It is also permissible to use the last part to solve the first 3 parts.

(a) Compute the order of the permutation $(12)(345) \in S_5$.

Solution.

$$\operatorname{ord}((12)(345)) = 6$$

$\square$

(b) Compute the order of $(123)(4567) \in S_7$.

Solution.

$$\operatorname{ord}((123)(4567)) = 12$$

$\square$

(c) Compute the order of $(12)(34)(567) \in S_7$.

Solution.

$$\operatorname{ord}((12)(34)(567)) = 6$$

$\square$

(d) Suppose that $\sigma = \sigma_1 \cdots \sigma_k$ is a product of **disjoint** cycles in S_n. Prove that

$$\operatorname{ord}(\sigma) = \operatorname{lcm}\big\{\operatorname{ord}(\sigma_1), \ldots, \operatorname{ord}(\sigma_k)\big\}.$$

Solution. Because disjoint cycles commute, we have

$$\sigma^\ell = \sigma_1^\ell \cdots \sigma_k^\ell.$$

Therefore the order of σ is the smallest value of ℓ such that $\sigma_i^\ell = e$ for all i. But $\sigma_i^\ell = e$ if and only if ℓ is a multiple of the order of σ_i. Therefore the smallest ℓ such that $\sigma_i^\ell = e$ for all i is precisely the least common multiple of the orders of all of the σ_i. □

Exercise 28. Let A be a group. Let be the set of automorphisms of A:

$$G = \big\{ f : A \to A \big| f \text{ is an isomorphism of groups} \big\}.$$

Show that G is a group where the operation is composition of functions. (Hint: show that G is a subgroup of S_A.)

Solution. Since every isomorphism of groups is a bijection, G is a subset of S_A. To show it is a subgroup we have to show that it is non-empty and that if $f, g \in G$ then $fg^{-1} \in G$ (by Proposition 1). We certainly have the identity function $\mathrm{id}_A \in G$ because the identity is definitely a automorphism of A. Furthermore, we can check that if f and g are automorphisms of G then so is fg^{-1}:

We have to check that fg^{-1} is a bijective homomorphism. It is a bijection because it is the composition of the bijections f and g^{-1}. It is a homomorphism because both f and g^{-1} are homomorphisms, which implies that

$$\begin{aligned} fg^{-1}(xy) &= f(g^{-1}(xy)) \\ &= f(g^{-1}(x)g^{-1}(y)) && \text{because } g^{-1} \text{ is a homomorphism} \\ &= f(g^{-1}(x))f(g^{-1}(y)) && \text{because } f \text{ is a homomorphism} \\ &= fg^{-1}(x)fg^{-1}(y). \end{aligned}$$

Thus fg^{-1} is a homomorphism. It follows now that G is a subgroup of S_A and is in particular therefore a group. □

Exercise 29. Let G be the set of all **surjective** functions from $\mathbf{N}$ (the set of natural numbers) to itself. Is G a group with the operation being composition of functions? If so, prove it. If not, say which axioms of a group fail.

Solution. This is not a group. Composition of functions is associative, so G has an associative composition law; the identity function serves as an identity element. And if $f : \mathbf{N} \to \mathbf{N}$ is a surjection then for each $y \in \mathbf{N}$ there is some $x \in \mathbf{N}$ such that $f(x) = y$. If we choose such an x for each $y \in \mathbf{N}$ then we can define a function $g : \mathbf{N} \to \mathbf{N}$ such that $f(g(y)) = y$.

However, g is only a right-sided inverse to f. It is possible to find a surjection $f : \mathbf{N} \to \mathbf{N}$ that has no left-sided inverse. For example, let

$$f(x) = \begin{cases} 0 & x = 0 \\ x - 1 & x > 0 \end{cases}.$$

This function is surjective but not injective, so it cannot have an inverse. However, the function

$$g(y) = y + 1$$

is a right-sided inverse for f: we have, $fg(y) = y$ but $gf(0) = 1 \neq 0$ so g is not a left-sided inverse for f. $\square$

References

[Arm] M. A. Armstrong. *Groups and symmetry*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1988.