Margaret Bilu
Office 604
Fall 2019
bilu@cims.nyu.edu

Algebra homework 4
Laws of composition, groups, subgroups

Due October 9th, 2019

Please hand in your homework stapled, with your name written on it. All answers have to be justified.

Exercise 1. We define a law of composition $*$ on $\mathbf{R}$ by $x * y = x^2 + y^2$.

(a) Is it associative?

Solution. We compute, for $x, y, z \in \mathbf{R}$,

$$(x * y) * z = (x^2 + y^2) * z = (x^2 + y^2)^2 + z^2 = x^4 + 2x^2y^2 + y^4 + z^2.$$

and

$$x * (y * z) = x * (y^2 + z^2) = x^2 + y^4 + 2y^2z^2 + z^4.$$

These two expressions are easily seen to be not equal, by taking for example $x = y = 0$ and $z = 2$. So $*$ is not associative.

(b) Is it commutative?

Solution. We have, for all $x, y \in \mathbf{R}$, $x * y = x^2 + y^2 = y^2 + x^2 = y * x$, so the law is commutative.

(c) Does it have an identity?

Solution. Assume we have an identity e. Then it should satisfy, for all $x \in \mathbf{R}$, $x * e = x$, that is, $x^2 + e^2 = x$. For $x = 0$, this implies $e = 0$, and for $x = 2$, it implies $e^2 = 2^2 - 2 = 2$. This gives us a contradiction, so there is no identity element.

Exercise 2. We consider the set $\mathcal{F}(\mathbf{R}, \mathbf{R})$ of functions from $\mathbf{R}$ to $\mathbf{R}$. We saw in lectures that composition of functions $\circ$ is an associative law of composition on this set, with identity the function $\mathrm{id} : \mathbf{R} \to \mathbf{R}$ defined by $\mathrm{id}(x) = x$. For the following elements of $\mathcal{F}(\mathbf{R}, \mathbf{R})$, determine if they have an inverse for $\circ$, and if yes, give it.

(a) The function $f : \mathbf{R} \to \mathbf{R}$ given by $f(x) = 5x + 2$.

Solution. Recall that we saw in lectures that an element of $\mathcal{F}(\mathbf{R}, \mathbf{R})$ is invertible if and only if the corresponding function has an inverse, that is, if and only if it is bijective. We therefore only need to check bijectivity of the given functions. The function f is bijective, with inverse given by $f^{-1}(x) = \frac{1}{5}(x - 2)$.

(b) The function $g : \mathbf{R} \to \mathbf{R}$ given by $g(x) = x^2 - 3$.

Solution. This function is not invertible, because it is not bijective. For example, injectivity fails because $f(1) = f(-1) = -2$.

(c) The function $h : \mathbf{R} \to \mathbf{R}$ given by $h(x) = 2e^x$.

Solution. This function is not surjective, because its image contains only positive real numbers, therefore it is not bijective and not invertible.

Exercise 3. Let G be a group. Show that

$$Z(G) = \{x \in G,\ xg = gx \text{ for all } g \in G\}$$

is a subgroup of G. It is called the *center* of G.

Solution. To show it is a subgroup, we are going to check all the axioms one by one. For closure, start with $x, y \in Z(G)$: then for all $g \in G$, using associativity, we have

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy),$$

so $xy \in Z(G)$. By definition, the identity element e satisfies $eg = ge = e$ for all $g \in G$, so $e \in Z(G)$. Finally, for $x \in Z(G)$, starting from $xg = gx$ and multiplying by x^{-1} both on the right and on the left, we get

$$x^{-1}xgx^{-1} = x^{-1}gxx^{-1}$$

which, using the definition of the inverse, gives $gx^{-1} = x^{-1}g$ for all $g \in G$. So $x^{-1} \in Z(G)$. We may conclude that $Z(G)$ is indeed a subgroup of G.

Exercise 4. Let G be a group such that for every $x \in G$ we have $x^2 = e$, where e is the identity element of g. Show that G must be abelian.

Solution. Let $a, b \in G$. Our aim is to show that $ab = ba$. First of all, remark that since for all $x \in G$, $x^2 = x \cdot x = e$, we have that every x is its own inverse. In particular, we have $ab = (ab)^{-1}$. On the other hand, we know from lectures that $(ab)^{-1} = b^{-1}a^{-1}$, so that we get the equality $ab = b^{-1}a^{-1}$. Using that a and b are their own inverses, we get the result.

Exercise 5. Prove that

$$G = \{a + b\sqrt{3},\quad a, b \in \mathbf{Q},\ a, b \text{ not both zero}\}$$

is a subgroup of the group $(\mathbf{R}^\times, \cdot)$.

Solution. Closure: For all elements $x = a + b\sqrt{3}$ and $y = c + d\sqrt{3}$ of G, we have

$$xy = (a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}.$$

Since $a, b, c, d \in \mathbf{Q}$, be have $ac + 3bd \in \mathbf{Q}$ and $ad + bc = \mathbf{Q}$. We must moreover check that $ac + 3bd$ and $ad + bc$ are not both zero. Indeed, if they were, we would have $ac = -3bd$ and $ad = -bc$. To go further, we need to consider several cases.

Assume first that a is non-zero. Then we have $c = -\frac{3bd}{a}$ from the first equation, and substituting it into the second equation, we get

$$ad = \frac{3b^2 d}{a},$$

or, multiplying by a, $a^2 d = 3b^2 d$. Since a is non-zero, if d were zero, the equation $ac = -3bd$ would force c to be zero, which is impossible since c and d cannot be both zero. Therefore, $d \neq 0$, and simplifying by d on both sides, we get $a^2 = 3b^2$, which in turn gives

$$(a + b\sqrt{3})(a - b\sqrt{3}) = 0.$$

This equation means that either $a + b\sqrt{3} = 0$ or $a - b\sqrt{3} = 0$. Since $a \neq 0$, we necessarily have $b \neq 0$ (otherwise any of these equations would imply $a = 0$), and therefore either $\sqrt{3} = -\frac{a}{b}$ or $\sqrt{3} = \frac{a}{b}$, both of which are impossible since this would mean $\sqrt{3} \in \mathbf{Q}$, which is known to be false.
Assume now that $a = 0$. Since a and b are not both zero, we have $b \neq 0$, so the equation $0 = ac = -3bd$ implies that d must be zero. On the other hand, the equation $0 = ad = -bc$ implies $c = 0$, since $b \neq 0$. We therefore get $c = d = 0$, which is a contradiction.
From this, we may conclude that $ac + 3bd$ and $ad + bc$ are not both zero, so that xy is indeed an element of G.
We have $1 = 1 + 0 \cdot \sqrt{3}$, so G contains the identity element 1 of $(\mathbf{R}^\times, \cdot)$.
Let $x = a + b\sqrt{3} \in G$. We want to show that x^{-1} is also an element of G. We have

$$x^{-1} = \frac{1}{a + b\sqrt{3}}.$$

Multiplying the numerator and the denominator by $a - b\sqrt{3}$ (remember this trick, it is often very useful!), which, as noted previously, is non-zero because $\sqrt{3} \notin \mathbf{Q}$, we get

$$x^{-1} = \frac{a - b\sqrt{3}}{(a + b\sqrt{3})(a - b\sqrt{3})} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} = \frac{a}{a^2 - 3b^2} - \frac{b}{a^2 - 3b^2}\sqrt{3}.$$

Since $a, b \in \mathbf{Q}$, we have $\frac{a}{a^2 - 3b^2} \in \mathbf{Q}$ and $-\frac{b}{a^2 - 3b^2} \in \mathbf{Q}$. Moreover, they are not both zero because if they were, this would force a and b to be both zero. Therefore we may conclude that $x^{-1} \in G$.
As a conclusion, G is indeed a subgroup of $(\mathbf{R}^\times, \cdot)$.

Exercise 6.

1. Let $O_n(\mathbf{R})$ be the set of matrices $A \in M_n(\mathbf{R})$ satisfying ${}^tAA = I_n$, where ${}^tA$ denotes the transpose of A and I_n denotes the identity matrix. Show that any $A \in O_n(\mathbf{R})$ is an invertible matrix.

   Solution. For any $A \in O_n(\mathbf{R})$, we have ${}^tAA = I_n$. Taking transposes, we also have $A{}^tA = I_n$. Thus, A is invertible with inverse $A^{-1} = {}^tA$.

2. Show that $O_n(\mathbf{R})$ is a subgroup of $(GL_n(\mathbf{R}), \cdot)$.

Solution. Closure: Let A and B be two matrices in $O_n(\mathbf{R})$. Then

$$^t(AB)(AB) = {}^tB\,{}^tAAB = {}^tBI_nB = {}^tBB = I_n,$$

so $AB \in O_n(\mathbf{R})$.

Identity: We have ${}^tI_nI_n = I_nI_n = I_n$, so $I_n \in O_n(\mathbf{R})$.

Inverses: Let $A \in O_n(\mathbf{R})$. We know that $A^{-1} = {}^tA$. Thus,

$$^t(A^{-1})A^{-1} = {}^t({}^tA){}^tA = A\,{}^tA = I_n$$

(using the identity in the proof of the first question). So $A^{-1} \in O_n(\mathbf{R})$.