Solution Set 8: Part A

Benjamin Bakker
Mathematics 25a
Prof. Berger

November 14, 2003

A.1. *In each of the following exercises, you are given a set G and a composition law $(x, y) \mapsto x \otimes y$. Determine whether $(G, \otimes)$ is a group, and if it is, find the unit element, give a formula for the inverse of an element, and determine whether G is abelian.*

(1) $G = \mathbb{R}$ *and* $x \otimes y = x + y + xy$.

Solution. If G were a group, then 0 must be the identity, since $0 \otimes x = x \otimes 0 = x + 0 + 0 \cdot x = x$. But -1 cannot have an inverse since

$$(-1) \otimes x = -1 + x + (-1)x = -1 \neq 0$$

Thus, G is not a group. □

(2) $G = (\mathbb{R} \setminus \{0\}) \times \mathbb{R}$ *and* $(x, u) \otimes (y, v) = (xy, xv + u)$.

Solution. G is a group. Multiplication is associative since

$$(x, u) \otimes [(y, v) \otimes (z, w)] = (x, u) \otimes (yz, yw + v) = (xyz, xyw + xv + u)$$
$$[(x, u) \otimes (y, v)] \otimes (z, w) = (xy, xv + u) \otimes (z, w) = (xyz, xyw + xv + u)$$

The unit is $(1, 0)$, for

$$(1, 0) \otimes (x, u) = (x, u + 0) = (x, u) = (x, x \cdot 0 + u) = (x, u) \otimes (1, 0)$$

For a given (x, y), the inverse is $(x, y)^{-1} = (1/x, -y/x)$ $(x \neq 0\ )$, since

$$(x, y) \otimes (1/x, -y/x) = (1, -y + y) = (1, 0) = (1, y/x - y/x) = (1/x, -y/x) \otimes (x, y)$$

The group is nonabelian since

$$(1, 2) \otimes (2, 1) = (2, 3) \neq (2, 5) = (2, 1) \otimes (1, 2)$$

A much easier way to show G is a group would have been to identify

$$(x, u) \leftrightarrow \begin{pmatrix} x & u \\ 0 & 1 \end{pmatrix}$$

and then noting that $\otimes$ is just matrix multiplication, that the identity has the above form, and that the inverse of any matrix of the above form has the above form. □

(3) $G = \{(x, y) \in \mathbb{R}^2 | x^2 + y^2 = 1\}$ *and* $(x_1, y_1) \otimes (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$.

Solution. The multiplication here is identical to the multiplication law of complex numbers $(x, y) = x + yi$, and G is just the unit circle in the complex plane, $S^1 = \{z \in \mathbb{C} | |z| = 1\}$.

I did the last one out in gory detail, so here I'll just use the trick that I mentioned at the end of (2). If we identify

$$(x, y) \leftrightarrow \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \tag{1}$$

then $\otimes$ is matrix multiplication, since

$$\begin{pmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_2 & -y_2 \\ y_2 & x_2 \end{pmatrix} = \begin{pmatrix} x_1x_2 - y_1y_2 & -x_1y_2 - x_2y_1 \\ x_1y_2 + x_2y_1 & x_1x_2 - y_1y_2 \end{pmatrix} \tag{2}$$

We can then consider G as the set of all matrices of the form (1) with determinant 1 (this is the condition that $x^2 + y^2 = 1$). G is closed under multiplication, for by (2) the product of the matrices corresponding to $(x_1, y_1), (x_2, y_2)$ has the form of (1), and the determinant is the product of the determinants of the factors—namely, 1. The identity matrix is in G, corresponding to $(1, 0)$, and every matrix (x, y) has determinant 1 and therefore is invertible; explicitly, the inverse is

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix}^{-1} = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \Rightarrow (x, y)^{-1} = (x, -y)$$

which is clearly in G. G is in fact abelian, since

$$\begin{pmatrix} x_2 & -y_2 \\ y_2 & x_2 \end{pmatrix} \begin{pmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{pmatrix} = \begin{pmatrix} x_1x_2 - y_1y_2 & -x_1y_2 - x_2y_1 \\ x_1y_2 + x_2y_1 & x_1x_2 - y_1y_2 \end{pmatrix}$$

A.2. *Let G be a finite group and let $a, b \in G$ be such that $(ab)^m = e$ for some $m \geq 1$. Prove that $(ba)^m = e$.*

Solution.

$$e = beb^{-1} = b(ab)^m b^{-1} = b\left[\underbrace{(ab)(ab)\cdots(ab)(ab)}_{m\text{ times}}\right]b^{-1} = (ba)^m$$

A.3. *Let G be a group such that for every $a \in G$, we have $a^2 = e$. Prove that G is abelian.*

Solution. Note first that in an arbitrary group G, if an element $x \in G$ has two inverse y, y', then because inverses are required to be both-sided,

$$y = ye = y(xy') = (yx)y' = ey' = y'$$

and therefore the inverse is unique.

For any $a, b \in G$ we have $(ab)(ba) = ab^2a = a^2 = e$, so $(ab)^{-1} = ba$. But by hypothesis, any element is its own inverse, so $ab = ba$.

A.4.

(1) *Find all groups G which have no non-trivial automorphisms.*

Solution. Conjugation by an element $x \in G$, $f : a \mapsto xax^{-1}$, is an automorphism since: $f(a)f(b) = (xax^{-1})(xbx^{-1}) = xabx^{-1} = f(ab)$; $a \in \ker f \Rightarrow xax^{-1} = e \Rightarrow a = e$; for any $a \in G$, $f(x^{-1}ax) = a$. For any $x \in G$, conjugation by x is trivial, so for all $a \in G$, $xax^{-1} = a \Rightarrow xa = ax$, and G must be abelian. We showed in lecture that for any abelian group, $x \mapsto x^{-1}$ is an automorphism; if it is trivial, then for every $x \in G$, $x = x^{-1} \Rightarrow x^2 = e$.

Suppose there are two non-unit elements $a, b \in G$. Let $H = (e, a, b, ab)$, and pick representatives x_i of the nontrivial cosets. Let K be the subgroup generated by the x_i. Note that if $x_i \neq x_j$ then we can't have $x_ix_j \in H$, or else $x_iH = x_jH$. Since $x_i^2 = e$, it follows that $H \cap K = (e)$. The map $H \times K \to G$, $(h, k) \mapsto hk$ is an isomorphism; it is surjective by construction, and injective by the above ($H \cap K = (e)$, so if $hk = e \Rightarrow h^{-1} = k \in H \cap K$). The map $f : H \to H$, that switches a, b is a nontrivial automorphism as can be readily checked by computation, so we have an induced nontrivial automorphism $g : H \times K \to H \times K$, $g(h, k) = (f(h), k)$. Therefore, there cannot be two non-unit elements in G.

Only (e) and $\mathbb{Z}/2\mathbb{Z}$ can have no nontrivial automorphisms. Since an automorphism must fix e, both of these groups do, in fact, have no nontrivial automorphisms.

(2) *Find all groups G which have no non-trivial subgroups.*

Solution. Certainly, the identity group (e) has no nontrivial subgroups. If $G \neq (e)$, then there is some $x \in G$ not equal to e. The subgroup generated by x (i.e., the set of powers of x, negative, positive, and zero) cannot be (e) and therefore must be the whole group, so G is cyclic—$\mathbb{Z}/n\mathbb{Z} \cong G$ for some $n \neq 1$ (the isomorphism is given by the map $\bar{1} \mapsto x$). $\mathbb{Z}$ has nontrivial subgroup $2\mathbb{Z}$, so $n \neq 0$. If n is not prime, then there is some $p \neq 1, n$ dividing n, in which case the subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by p is nontrivial. If n is prime, however, then for any nonzero $x \in \mathbb{Z}/n\mathbb{Z}$, the subgroup generated by x must have order d greater than 1 and dividing n, and is therefore the whole group. Thus, the only groups (up to isomorphism) with no nontrivial subgroups are (e) and $\mathbb{Z}/p\mathbb{Z}$ for p prime.

A.5. *Find all continuous homomorphisms* $f : (\mathbb{R}, +) \to (\mathbb{R}, +)$.

Solution. For any homomorphism $f : G_1 \to G_2$, and any $x \in G_1$, $f(x) = f(e_1 x) = f(e_1)f(x) \Rightarrow f(e_1) = e_2$. Thus, for homomorphisms of $\mathbb{R}$ into $\mathbb{R}$, $f(0) = 0$. $f = 0$ is one possible continuous homomorphism.

Suppose $f(a) \neq 0$ for some $a \in \mathbb{R}$ (note that $a \neq 0$). Then for any $n \in \mathbb{Z}$,

$$f(na) = f(\underbrace{a + \cdots + a}_{n \text{ times}}) = nf(a)$$

Similarly, for any nonzero $m \in \mathbb{Z}$, $f(a) = f(m(a/m)) = mf(a/m)$, so $f(a/m) = f(a)/m$. More generally, for any $n/m \in \mathbb{Q}$, $f(na/m) = nf(a)/m$.

We claim that $f(x) = f(a)x/a$. By the above, this is true for the rational multiples $a\mathbb{Q}$ of a. $a\mathbb{Q}$ is dense in $\mathbb{R}$, so for every $x \in \mathbb{R}$, there is a sequence $x_n \in a\mathbb{Q}$ converging to x. f is continuous, so

$$f(x) = \lim f(x_n) = \lim f(a)x_n/a = \frac{f(a)}{a} \lim x_n = f(a)x/a$$

as claimed. In particular, if $f(1) = f(a)/a = b$, then $f(x) = f(a)x/a = bx$, and thus f is simply multiplication by $f(1)$. This clearly is, in fact, a continuous homomorphism, so the only continuous homomorphism are multiplication by a real number (including 0).