KMB, 15/10/13

M2PM2 Algebra II Solutions to Sheet 2

1. (a) Say g is an isometry that fixes two points v and $w \neq v$. Say x is a general point in $\mathbb{R}^2$. Then $d(g(x), v) = d(x, v) = a$ say (as $g(v) = v$), and similarly $d(g(x), w) = d(x, w) = b$. Let σ denote the reflection about the line L through v and w. Now convince yourself either by doing the algebra or drawing two circles, that the circles centre v radius a and centre w radius b meet at at most two points, and that if they meet at x (which they do) then the only other point where they can meet is at $\sigma(x)$. We conclude that for each $x \in \mathbb{R}^2$, $g(x)$ is either x or $\sigma(x)$ (and in particular $g(x) = x$ for all $x \in L$).

Now if $g(x) = \sigma(x)$ for all x, then $g = \sigma$ and we're done. So let's say $g(x) = x$ for some $x \notin L$ and let's prove that g must be the identity. If y is a point in $\mathbb{R}^2$ on the same side of L as x then $d(x, y) < d(x, \sigma(y)) = d(g(x), \sigma(y))$, so we can't have $g(y) = \sigma(y)$ and hence $g(y) = y$. A similar argument works for points on the opposite side of L. Hence g must be the identity.

(b) If g fixes three non-collinear points v, w, x then by (a) g is either the identity or the reflection about the line through v and w – but this reflection moves x. So g must be the identity.

2. We must show three things: (i) $G \cong G$, (ii) $G \cong H \Rightarrow H \cong G$, and (iii) $G \cong H$, $H \cong K \Rightarrow G \cong K$.

For (i), observe that the identity function $f(x) = x$ ($x \in G$) is an isomorphism from G to G.

For (ii), let $\phi : G \to H$ be an isomorphism. We claim ϕ^{-1} is an isomorphism $H \to G$. It is a bijection (by M1F). And for $a, b \in H$, we have $a = \phi(c), b = \phi(d)$ for some $c, d \in G$, hence $\phi^{-1}(ab) = \phi^{-1}(\phi(c)\phi(d)) = \phi^{-1}(\phi(cd)) = cd = \phi^{-1}(a)\phi^{-1}(b)$. Hence $\phi^{-1} : H \to G$ is an isomorphism, so $H \cong G$.

For (iii), let $\phi : G \to H$ and $\psi : H \to K$ be isomorphisms. Then $\psi \circ \phi : G \to K$ is a bijection (M1F again), and is an isomorphism since for all $x, y \in G$,

$$(\psi \circ \phi)(xy) = \psi(\phi(xy)) = \psi(\phi(x)\phi(y)) = \psi(\phi(x))\,\psi(\phi(y)) = (\psi \circ \phi)(x)\,(\psi \circ \phi)(y).$$

Hence $G \cong K$.

3. (a) $\phi(e_G) = e_H$ as shown in lectures, so $e_H = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$ hence $\phi(g^{-1}) = \phi(g)^{-1}$. (b) Say $\phi(g)$ had finite order. Then $\phi(g)^n = e_H$ for some positive integer n, and hence $\phi(g^n) = e_H = \phi(e_G)$. Because ϕ is a bijection, this implies $g^n = e_G$, so g has finite order, a contradiction.

4. Call these groups $G_1, \ldots, G_6$ in the order they are listed. Then $G_2 = (\mathbb{Z}, +) \cong \langle \pi \rangle = G_5$ as they are both infinite cyclic. Also $G_3 = (\mathbb{Q}^*, \times) \cong G_6$, an isomorphism being $a \mapsto a - 1$ (one has to check that $(a-1) * (b-1) = ab - 1$ to check that this map is an isomorphism, but this is easy). There are no further isomorphisms between these groups: G_2 is not isomorphic to any of G_1, G_3, G_4 as it is cyclic and the others aren't (what could a generator be?); G_3 is not isom to G_1, G_4 as it has an element of order 2 (namely -1) and the others don't; and finally $G_1 \ncong G_4$ – this is tricky, here's the argument. Spose $\phi : \mathbb{Q} \to \mathbb{Q}_{>0}$ is an isomorphism, sending 1 to f say. Then $f \neq 1$ (as $\phi(0) = 1$), and for any $n \in \mathbb{N}$, ϕ must send $1/n$ to the n^{th} root of f; this cannot lie in $\mathbb{Q}$ for all n.

5. (a) D_{120} has elements of order 60, whereas S_5 does not, so $S_5 \ncong D_{120}$ by Prop 2.1 of lectures. And C_{120} is not isomorphic to either of these groups as it is abelian and the others are not.

(b) Isomorphism $\phi : D_6 \to S_3$ is given by sending each element of D_6 to the corresponding permutation of the corners of the triangle.

(c) Isomorphism $x \to e^x$ shows $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \times)$. But $(\mathbb{Q}, +) \ncong (\mathbb{Q}_{>0}, \times)$ by Q3.

(d) One subgroup of size 4 is $\langle \rho \rangle$, the subgroup consisting of all rotations. Another is the

subgroup consisting of the symmetries $e, \rho^2, \sigma, \sigma\rho^2$. These subgroups are not isomorphic as one is cyclic and the other is not.

6. (a) Let $x, y \in G$. Then $x^2 = y^2 = (xy)^2 = e$. So $e = xxyy = xyxy$. Multiply on left by x^{-1} and on right by y^{-1}, to get $xy = yx$. Hence G is abelian.

(b) Suppose $|G| > 2$. Pick non-identity $x, y \in G$, $x \neq y$. Then check $\{e, x, y, xy\}$ is a subgroup (closure - write down mult table; inverses - each element is its own inverse). Hence 4 divides $|G|$ by Lagrange.

7. (i) The trick I explained in lectures (there are infinitely many groups of size 1) easily generalises.

(ii) As we are considering groups up to isomorphism, we can assume that our group elements are a fixed set, say $\{a_1, \ldots, a_n\}$. Clearly there are only finitely many possible mult tables for this set, hence only finitely many possible groups with these elements.

Note: the function sending a positive integer n to the number of groups of order n up to isomorphism is quite interesting. It is sequence A000001 (the first one!) in the online encyclopedia of integer sequences (`oeis.org`). No closed form for it is known and unless I'm out of date, we don't know how many groups there are of order 2048. The number of groups of order 1024 is 49487365422 and I believe the proof of this was a brute force computer calculation.

8. (a) Both +1 (because there are an even number of even cycles in both cases – it doesn't matter that the cycles aren't disjoint).

(b) $e, (3)$ (i.e. "a 3-cycle"),$(5), (7), (2,2), (2,4), (3,3), (2,2,3)$.

(c) Elements of order 2 are those of cycle-shape $(2,2)$. The number of these is $\binom{7}{2} \times \binom{5}{2} \times \frac{1}{2} = 105$.

9. As g has odd order, it is a product of disjoint cycles, all of odd length. These are all even perms., therefore g is even.

Alternatively argue by contradiction: if g has order m, odd, and $\mathrm{sgn}(g) = -1$, then $g^m = e$ gives $-1 = (-1)^m = \mathrm{sgn}(e) = +1$, a contradiction.