Name: Adam Frank **August 21, 2020**

Math 437: Homework Section 1

1. (1.1.20)
For an element x in G show that x and x^{-1} have the same order.

Proof. If $x^n = \mathbb{1}$ then by multiplying both sides by x^{-n} we get that $\mathbb{1} = x^{-n}$. Thus the order of x is at most the order of x^{-1}. But then that is already enough to see that the order of x^{-1} is at most the order of $(x^{-1})^{-1} = x$ so the orders are equal. □

2. (1.2.4)
If $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}.

Proof. That the order of z is 2 is obvious. $z^2 = r^{2k} = e$ and since $z^1 \neq e$ we're done.

To show that it commutes with everything, first note that it's a rotation and all rotates commute with each other. So it only remains to show that z commutes with any reflection. We use the fact that $sr^i = r^{n-i}s$ for each integer i. If sr^i is any reflection we need to show

$$(sr^i)z = z(sr^i)$$

We can simply chase the equation from left to right,

$$\begin{aligned}(sr^i)z = sr^{i+k} = sr^k r^i = \\ r^{n-k}sr^i = r^{2k-k}sr^i = \\ r^k sr^i = z(sr^i)\end{aligned}$$

□

3. (1.2.5)
If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all of D_{2n}.

Proof. The identity always commutes with everything so we don't need to show this. For any other element, we need to show that it cannot commute with everything. First we show that no other rotation commutes with s. For $r^i s = sr^i$ then

$$r^i s = sr^{-i} = sr^i$$

which entails $(r^i)^{-1} = r^i$. Then $r^{2i} = \mathbb{1}$ and we must have $2i$ equal to some multiple of n. Since 2 does not divide n then i must, but then $r^i = \mathbb{1}$.

Next we show that no reflection commutes with r. For if $(sr^i)r = r(sr^i)$ then

$$sr^{i+1} = sr^{i-1}$$

and then $r^{i+2} = r^i$. This is not true for any integer i when $n \geq 3$. □

4. (1.3.9(a))
Let σ be the 12-cycle (1 2 3 4 5 6 7 8 9 10 11 12). For which positive integers i is σ^i also a 12-cycle?

Proof. All the integers $i < 12$ coprime with 12, so $i = 5, 7, 11$. Any integer congruent with these modulo 12 will also give a 12-cycle. □

5. (1.3.15)
Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition.

Proof. It's clear that the order divides the LCM: Let $\sigma = \tau_1 \cdots \tau_p$ where τ_i is a cycle of length ℓ_i for each $i = 1 \dots p$, each disjoint from all the others. Note that for cycles, the length is the order. Call $\ell = LCM(\ell_1, \dots, \ell_p)$. Since the cycles are disjoint they commute and we can write

$$\sigma^\ell = \prod_{i=1}^{p} \tau_i^\ell = \mathbb{1}$$

And so we have that $|\sigma|$ divides ℓ.

However, from here we can even say more. If any two cycles α, β are disjoint and $\alpha\beta = \mathbb{1}$ then it must be that $\alpha = \beta = \mathbb{1}$. Hence the equation above shows that

$$\tau_i^\ell = \mathbb{1}$$

for each i. Hence the order of each cycle divides ℓ.

What we've proven then is that $\sigma^\ell = \mathbb{1}$ if and only if ℓ is a multiple of each ℓ_i. Then $|\sigma|$ is a multiple of each ℓ_i and is the least such, therefore $|\sigma| = \ell$. □

6. (1.4.3)
Show that $GL_n(F)$ is a finite group if and only if F has a finite number of elements.

Proof. If F has finitely many elements then clearly $|GL_n(F)| \leq |F|^{n^2}$.

For the converse, we prove that if F is infinite then $|GL_n(F)|$ is. In particular, since F is a field it must contain a copy of $\mathbb{Q}$, up to isomorphism. Then we can build an infinite subset of elements in $GL_n(F)$.

With I_n the $n \times n$ identity matrix, $(aI_n)^{-1} = \frac{1}{a} I_n$ clearly, for each $a \in \mathbb{Z} \setminus \{0\}$. □

7. (1.4.10)
Let $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} | a, b, c \in \mathbb{R}, a \neq 0, c \neq 0 \right\}$.

(a) Compute the product of $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$ and $\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$ to show that G is closed under matrix multiplication.

(b) Find the matrix inverse of $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and deduce that G is closed under inverses.

(c) Deduce that G is a subgroup of $GL_2(\mathbb{R})$.

(d) Prove that the set of elements of G whose two diagonal entries are equal is also a subgroup of $GL_2(\mathbb{R})$.

Proof. (a.)

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix} \in G$$

(b.) Since we are selecting from $GL_n(F)$ then we are already assured that each matrix is invertible, so all that remains is to show that the inverse is again in G.

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \frac{1}{ac} \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix} \in G$$

(c.) Subsets of a group closed under multiplication and inverses are always groups.

(d.) Call this subset H. Then for closure under multiplication,

$$\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1a_2 \\ 0 & a_1a_2 \end{pmatrix} \in H$$

And for inverses

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} = \frac{1}{a^2} \begin{pmatrix} a & -b \\ 0 & a \end{pmatrix} \in H$$

□

8. (1.5.3)
Find a set of generators and relations for Q_8.

Proof.

$$Q_8 = \langle i, j : i^2 = j^2 = (ij)^2 = -1; ij = -ji \rangle$$

□

9. (1.6.14)
Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Prove that the kernel is a subgroup. Prove that φ is injective if and only if the kernel is the trivial subgroup.

Proof. First we show closure under multiplication: if $x, y \in G$ such that $\varphi(x) = \varphi(y) = \mathbb{1}$ then $\varphi(xy) = \varphi(x)\varphi(y) = \mathbb{1}$.

Next we show closure under inverses. $\varphi(x^{-1}) = (\varphi(x))^{-1} = \mathbb{1}$

Hence we have that the kernel is a subgroup.

Next we show that injectivity implies the kernel is the trivial subgroup. But $\varphi(\mathbb{1}) = \mathbb{1}$ so if φ is injective nothing else also maps to $\mathbb{1}$. Hence the kernel is just $\{\mathbb{1}\}$.

Finally we show that if the kernel is trivial then φ is injective. Suppose that the kernel is the trivial subgroup and suppose $\varphi(x) = \varphi(y)$. Then $\varphi(xy^{-1}) = \mathbb{1}$ so that $xy^{-1} = \mathbb{1}$. Of course then $x = y$ so that φ is injective. □

10. (1.6.17)
Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Proof. Suppose the map is a homomorphism, call it φ and let $a, b \in G$. Before starting the proof let's note that the map is injective and therefore the inverse is a function. It is injective because if $\varphi(a) = \varphi(b) = a^{-1} = b^{-1}$ then multiplying by ab gives $a = b$. In particular we will use, for any $a \in G$ that $a = \varphi(a^{-1})$. Then

$$ab = \varphi(a^{-1})\varphi(b^{-1}) = \varphi(a^{-1}b^{-1}) = \varphi((ba)^{-1}) = ba$$

The converse is the easy direction:

$$\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} = \varphi(b)\varphi(a) = \varphi(a)\varphi(b)$$

□

11. (1.7.3)
Show that the additive group $\mathbb{R}$ acts on the x, y plane $\mathbb{R} \times \mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$.

Proof. First we show that the identity element, which here is 0, acts trivially.

$$0 \cdot (x, y) = (x + 0y, y) = (x, y)$$

and then that the action associates

$$\begin{aligned} r \cdot s \cdot (x, y) &= r \cdot (x + sy, y) = \\ &= (x + sy + ry, y) = (x + (r + s)y, y) = \\ &= (r + s) \cdot (x, y) \end{aligned}$$

□

12. (1.7.16)
Let G be any group and let $A = G$. Show that the maps defined by $a = gag^{-1}$ for all $g, a \in G$ are left group actions.

Proof. That the identity acts trivially: $a = \mathbb{1}a\mathbb{1}^{-1} = a$.

That the operation associates:

$$\begin{aligned} g_1 \cdot g_2 \cdot a = g_1 g_2 a g_2^{-1} g_1^{-1} = \\ (g_1 g_2) a (g_1 g_2)^{-1} = (g_1 g_2) \cdot a \end{aligned}$$

□