

GROUPS AND RINGS (MA22017)
SOLUTIONS TO PROBLEM SHEET 2

1 W In each of the following cases say what the order $|G|$ of G is.

- (a) $G = S_5$, the symmetric group on 5 letters.
- (b) The alternating group A_5 .
- (c) \mathbb{Z}/n .
- (d) The subgroup $n\mathbb{Z}$ of \mathbb{Z} .

Solution:

- (a) $5!$, which is 120.
- (b) 60, namely $\frac{5!}{2}$ because $S_5 = A_5 \cup (12)A_5$ and the union must be disjoint because different cosets don't meet.
- (c) n . Note that if p is a prime then $(\mathbb{Z}/p)^*$ is also a group, under multiplication this time, and is of order $p - 1$. Don't confuse these two!
- (d) ∞ .

2 H In each of the following cases say what the order $o(g)$ of g is. Verify that $o(g)$ divides $|G|$.

- (a) $G = S_5$ and $g = (13)(245)$.
- (b) $G = \text{SL}(2, \mathbb{F}_2)$ and $g = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. (By \mathbb{F}_2 we mean $\mathbb{Z}/2$ considered as a field, i.e. with both addition and multiplication mod 2.)

Solution:

- (a) g has order 6: either because you know that the order of a permutation is the lowest common multiple of its cycle lengths or just by computing g^2, g^3 and so on, and 6 does indeed divide 120.
- (b) We can simply compute that $g^2 = \text{id}$ so $o(g) = 2$. The harder part is finding the order of $\text{SL}(2, \mathbb{F}_2)$, which is most simply done by simply writing down the six elements. They are the identity along with

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

In other words: $\text{SL}(2, \mathbb{F}_2) = \text{GL}(2, \mathbb{F}_2)$ (if the determinant is not 0, it is 1) and the columns form an ordered basis, so the first column may be any nonzero vector in \mathbb{F}_2 (three possibilities) and the second column may be either of the other two.

3 W Suppose that G is a cyclic group of finite order n and that g generates G (in this case, we say that g is a generator). Is g^2 a generator? Which other elements of G are generators? How many of them are there?

Solution: g^2 is a generator if n is odd but not if n is even. More generally, g^k generates G if and only if $\text{hcf}(k, n) = 1$. So the number of generators is $\phi(n) = \prod_{p|n} n(1 - \frac{1}{p})$ (where p is prime), the Euler ϕ function.

4 W By considering left and right cosets, show that if $H < G$ and $|G : H| = 2$ then $H \triangleleft G$. Give an example of a group G and a non-normal subgroup of index 3.

Solution: There are two left cosets of H and one of them is H : call the other gH . Then $Hg \subset G = H \cup gH$, but $g \notin H$ since otherwise $gH = H$ (see II.2 in the lecture notes) so $Hg \cap H = \emptyset$ (otherwise $gh = h'$ for some $h, h' \in H$ and then $g = h'h^{-1} \in H$). So $Hg \subseteq gH$. Similarly, $gH \subseteq Hg$ so $gH = Hg$ so $H \triangleleft G$. The subgroup H generated by (12) is non-normal of index 3 in S_3 , since $(132)(12)(123) = (13) \notin H$.

5 H Suppose that G is a group and H is a subgroup.

- Verify that there is no such thing as “left index” and “right index”: the number of left cosets of H in G is equal to the number of right cosets. You may wish to consider the map $gH \mapsto Hg^{-1}$.
- Suppose that every non-identity element of G has order 2. Show that G is abelian.
- Show that the alternating group A_4 , which is of order 12, does not have a subgroup of order 6: hence the converse of Lagrange’s Theorem is false in general.

Solution:

- The map given is a bijection between the set of left cosets and the set of right cosets. To show this it is only necessary to check that it is well defined. If $g_1H = gH$ then $g_1 = gh$ for some $h \in H$ and then $Hg_1^{-1} = Hh^{-1}g^{-1} = Hg^{-1}$, which is all that we need. Once we know that the map is defined, we can see that it is a bijection because its inverse is $Hg \mapsto g^{-1}H$.
- Suppose $a, b \in G$. Then we claim that $ab = ba$, i.e. that $aba^{-1}b^{-1} = 1$. But $a^{-1} = a$ and $b^{-1} = b$ since $a^2 = b^2 = 1$, so $aba^{-1}b^{-1} = abab = (ab)(ab) = 1$ because ab also has order 2 (or order 1).
- One way to see this is as follows: A_4 contains the identity, three elements of order 2 such as $(12)(34)$ and eight elements of order 3 such as (123) . A subgroup H of order 6 would have to contain the identity and if it contains an element of order 3 it must also contain its inverse. So it

contains an odd number of elements of order 2, either just one or all of them. If it contains all of them then it contains (12)(34) and a 3-cycle, say (123), and its inverse, but no more; but (12)(34)(123) = (243). If it contains only one, say (12)(34), then it also contains a 3-cycle, say (123), and its inverse: but (321)(12)(34)(123) = (13)(24).

6 E Verify the assertion made in 2.20(iv): the group $\text{Aff}(\mathbb{R}^2)$ of affine linear transformations of a plane has a normal subgroup consisting of the translations. The quotient is isomorphic to $\text{GL}(2, \mathbb{R})$, but although $\text{GL}(2, \mathbb{R})$ is a subgroup of $\text{Aff}(\mathbb{R}^2)$, it is not a normal subgroup.

Solution: If $M \in \text{GL}(2, \mathbb{R})$ and $\mathbf{a} \in \mathbb{R}^2$, let us denote by $T(M, \mathbf{a})$ the element of $\text{Aff}(\mathbb{R}^2)$ that sends $\mathbf{x} \in \mathbb{R}^2$ to $M\mathbf{x} + \mathbf{a}$. (Think of \mathbf{x} and \mathbf{a} as column vectors.) The translation subgroup is the subgroup $T = \{T(I, \mathbf{a} \mid \mathbf{a} \in \mathbb{R}^2\}$ and $\text{GL}(2, \mathbb{R})$ is identified with $\{T(M, 0) \mid M \in \text{GL}(2, \mathbb{R})\}$.

The best way to check that T is a normal subgroup is to consider the map $\varphi: \text{Aff}(\mathbb{R}^2) \rightarrow \text{GL}(2, \mathbb{Z})$ given by $\varphi(T(M, \mathbf{a})) = M$. This is obviously surjective and $\text{Ker } \varphi = T$ by definition, but we need to check that φ is a group homomorphism: then the First Isomorphism Theorem tells us the result. However

$$\begin{aligned} (T(M_1, \mathbf{a}_1)T(M_2, \mathbf{a}_2))(\mathbf{x}) &= T(M_1, \mathbf{a}_1)(M_2\mathbf{x} + \mathbf{a}_2) \\ &= M_1M_2\mathbf{x} + M_1\mathbf{a}_2 + \mathbf{a}_1 \\ &= T(M_1M_2, M_1\mathbf{a}_2 + \mathbf{a}_1)(\mathbf{x}). \end{aligned}$$

So $T(M_1, \mathbf{a}_1)T(M_2, \mathbf{a}_2) = T(M_1M_2, M_1\mathbf{a}_2 + \mathbf{a}_1)$, so

$$\varphi(T(M_1, \mathbf{a}_1)T(M_2, \mathbf{a}_2)) = M_1M_2 = \varphi(T(M_1M_2, M_1\mathbf{a}_2 + \mathbf{a}_1)).$$

On the other hand, if we take $\mathbf{a} = (1, 0)^T$ and $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ then

$$T(0, -\mathbf{a})T(M, 0)T(0, \mathbf{a})(\mathbf{x}) = M(\mathbf{x} + \mathbf{a}) - \mathbf{a},$$

which sends the origin to $(1, -1)$ so it does not belong to $\text{GL}(2, \mathbb{R})$.

GKS, 13/2/25