Queen Mary
University of London

MTHM024/MTH714U Group Theory

Problem Sheet 6 Solutions

1 (a) We can map 0 to b by the map $x \mapsto x+b$ (that is, $x \mapsto (1x+b)/(0x+1)$), and 0 to ∞ by $x \mapsto 1/x$. So the orbit containing 0 is the whole of $F \cup \{\infty\}$.

(b) The map $x \mapsto (ax+b)/(cx+d)$ maps ∞ to a/c. If this is to be ∞, we must have $c = 0$, so that $x \mapsto (ax+b)/d = (a/d)x + (b/d)$. Nothing is affected if we take $d = 1$, giving the form stated.

This group is transitive on F (we saw this implicitly in (a)), so the result follows from:

Fact *Suppose that G is transitive on Ω, and the stabiliser of a point $\omega \in \Omega$ is transitive on $\Omega \setminus \{\omega\}$. Then G is doubly transitive on Ω.*

Proof Suppose that we want to map (α, β) to $(\gamma, delta)$, where $\alpha \neq \beta$ and $\gamma \neq \delta$. Choose $g \in G$ mapping α to ω, and $g' \in G$ mapping γ to ω. Then βg and $\delta g'$ are both different from Ω; so choose $h \in \mathrm{Stab}(\omega)$ mapping βg to $\delta g'$. Then check that $gh(g')^{-1}$ is the element we are looking for.

(c) If $x \mapsto ax+b$ fixes 0, then $b = 0$, so the stabiliser of ∞ and 0 is the group $x \mapsto ax$ for $a \in F^\times$. Clearly it is transitive on $F \setminus \{0\}$: we can map 1 to a by multiplying by a.

Now a result similar to the Fact above shows that, if G is doubly transitive and the stabiliser of two points is transitive on the remaining points then G is triply transitive.

Since G is triply transitive, all three-point stabilisers are conjugate; and the stabiliser of ∞, 0 and 1 is the identity. (The map $x \mapsto ax$ maps 1 to 1 if and only if $a = 1$.)

2 Suppose that G is a simple group of order pqr, where $p > q > r$. The number of Sylow p-subgroups is congruent to 1 mod p and divides qr; it cannot be 1 (since G is simple), q or r (since it is at least $p+1$), so must be qr.

Now the Sylow p-subgroups between them contain the identity and $qr(p-1)$ elements of order p (since any two intersect only in the identity).

Similarly, the number of Sylow q-subgroups is congruent to 1 mod q and divides pr, so must be either p or pr, giving us at least $p(q-1)$ elements of order q. Similarly, there are at least $q(r-1)$ elements of order r. So

$$1+qr(p-1)+p(q-1)+q(r-1)\leq pqr,$$

which is obviously false.

3 The proof that G is a group is all straightforward except for the associative law, which requires a lot of case-by-case analysis. Then the proof that it is an elementary abelian 2-group is straightforward.

For the associative law, the cases where one or more of the three terms is 0 are all trivial. The case where the first and second, or second and third, are equal are also trivial. The case where the first and last elements are equal holds since $x+(y+x)=(x+y)+x$ by commutativity. I reckon that the following cases need to be considered:

- $\{a,b\}$, $\{a,c\}$, $\{a,d\}$;
- $\{a,b\}$, $\{a,c\}$, $\{b,c\}$;
- $\{a,b\}$, $\{a,c\}$, $\{b,d\}$;
- $\{a,b\}$, $\{a,c\}$, $\{c,d\}$;
- $\{a,b\}$, $\{a,c\}$, $\{d,e\}$;
- $\{a,b\}$, $\{c,d\}$, $\{a,e\}$;
- $\{a,b\}$, $\{c,d\}$, $\{c,e\}$;
- $\{a,b\}$, $\{c,d\}$, $\{e,f\}$.

Here is a different argument avoiding cases.

Step 1: The set of all subsets of $\{1,\ldots,n\}$, with the operation of symmetric difference, is an elementary abelian 2-group. (Mapping each subset A to the n-tuple of 0s and 1s having 1s in the positions of A and 0s elsewhere is a bijection to $(\mathbb{Z}_2)^n$, and it is easy to see that it is a group isomorphism.)

Step 2: The set of subsets of even cardinality is a subgroup W, and the set $\{\emptyset,\{1,\ldots,n\}\}$ is a subgroup U.

Step 3: If n is even, then $U\leq W$, and so W/U is an elementary abelian 2-group of order 2^{n-2}.

Step 4: If $n = 6$, then every coset of U apart from U itself has the form $\{\{a,b\},\{c,d,e,f\}\}$. Choose $\{a,b\}$ as the coset representative, and check that the group operation takes exactly the form given in the question (where 0 denotes the coset U).

An elementary abelian 2-group is the additive group of a vector space over $\mathbb{F}_2$, where scalar multiplication is given by $0v = 0$ and $1v = v$. Any group automorphism is a vector space automorphism. So the automorphism group of $(V,\oplus)$ is $\mathrm{GL}(4,2)$. But clearly S_6, acting by permuting the elements of the sets (so that $0g = 0$ and $\{a,b\}g = \{ag,bg\}$) is a group of automorphisms.

The index is $(2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3)/6! = 28$.

Remark In fact, $\mathrm{GL}(4,2)$ is isomorphic to the alternating group A_8. The embedding of S_6 into A_8 is given by the following map:

$$g \in S_6 \mapsto \begin{cases} g & \text{if } g \text{ is an even permutation;} \\ g(7,8) & \text{if } g \text{ is an odd permutation.} \end{cases}$$

If you are interested in classical groups, I will mention that S_6 is isomorphic to the symplectic group $\mathrm{Sp}(4,2)$, which naturally occurs as a subgroup of $\mathrm{GL}(4,2)$.

4 (a) Immediate from Sylow's Theorem.

(b) G acts on the set of eight Sylow 7-subgroups; the stabiliser of one such subgroup P is its normaliser $N(P)$. Now P is cyclic of order 7; we can take it to be generated by the map $x \mapsto x+1$ of $\mathbb{Z}_7$. The normaliser of this subgroup in S_7 can be shown to be the group of maps $x \mapsto ax+b$ where $a,b \in \mathbb{Z}_7$ and $a \neq 0$, of order 42. A subgroup of order 21 must contain P, and must consist of maps $x \mapsto ax+b$ where a runs through a subgroup of order 3 of the multiplicative group of $\mathbb{Z}_7$, necessarily $\{1,2,4\}$.

G is doubly transitive by the fact proved in Question 1.

The maps $x \mapsto ax$ for $a = 1,2,4$ form a subgroup of order 3, necessarily a Sylow 3-subgroup Q.

(c,d) By double transitivity there is an element t interchanging ∞ and 0; it must normalise Q, since Q is the two-point stabiliser, and must consist of four 2-cycles (the only alternative is 3, and then it would be an odd permutation). If it were to fix the two orbits of Q it would fix a point in each and have only three 2-cycles.

(e) There are not too many possibilities for t; laborious calculation show that, in all cases except that given, we can obtain a non-identity permutation fixing three points from the ones we are given.

(f) The group H generated by N and t is transitive, and contains N, the stabiliser of ∞; so it must be equal to G. (Both G and H contain N as a subgroup of index 8, so they are equal.)

(g) As noted, we have shown that $G \leq \mathrm{PSL}(2,7)$. Both groups have order 168, so they are equal.

5 This can be done by hard work using the Fundamental Theorem of Finite Abelian Groups. Here is a trick which makes it easier.

Let A be a finite abelian group of order n. Let A^* be the set of all homomorphisms from A to the multiplicative group of nth roots of unity in the complex numbers. Then the operation of multiplication (that is, $a(\phi\psi) = (a\phi)(a\psi)$) makes A^* a group. By using the FTFAG, we can see that A^* is a group isomorphic to A.

Now if $B \leq A$, let $B^\dagger$ be the set of elements of A^* which are the identity on B. Then $B^\dagger$ is the kernel of a homomorphism from A^* to B^*, whose image is B^*; so $A^*/B^\dagger \cong B$. Thus A has a subgroup C with $A/C \cong B$; and $C \cong A/B$, by considering $(A^*)^*$, which is isomorphic to A.

The infinite cyclic group $\mathbb{Z}$ has the property that all its subgroups are infinite cyclic groups (the groups $n\mathbb{Z}$ for positive integers n) and all its quotients are finite cyclic groups $\mathbb{Z}/n\mathbb{Z}$. Clearly it doesn't have this property the other way round.

The quaternion group of order 8 has four non-trivial subgroups (all normal), once C_2 and three C_4s. but $Q_8/C_2 \cong V_4$, which is not in the list of subgroups.