1a Groups

Thomas Forster

November 25, 2017

Sheet 1

Do not allow yourself to confuse '$G \setminus H$' and 'G/H'.

Question 1

A chance to write '$h_1 \in H_1 \setminus H_2$'.

Can you have three subgroups forming an antichain under $\subseteq$ whose union is a subgroup?

Question 2

Question 3

Observe the symmetry in the definition of $x * y$. This tells you that the group is abelian.

Suppose n is odd and we have a homomorphism f from D_{2n} to C_n. Every element of C_n is of odd order, but the reflections in D_{2n} are of even order. What can f possibly send them to? For any g the order of $f(g)$ must divide the order of g. So f must send every reflection to $\mathbb{1}$. But every element of D_{2n} is a product of two reflections.

Question 4

Question 5

Question 6

Question 7

Question 8

Question 9

Question 10

Question 11

Question 12

Question 13

Question 14

Suppose that every element is of order 2. Then $abab = \mathbb{1}$. So $abab \cdot ba = ba$. Do some cancelling on the LHS to get $ab = ba$.

You might wonder if you get anything nice from every element of a group being of order 3. No! 2 is special in this respect.

The starred part is a riff on things called **boolean rings**. Given a collection $X \subseteq G$, we can think about the subgroup generated by those elements. If that subgroup is the whole of G then we say X is a *set of generators* of G. Because every element is of order 2 each element is its own inverse, so we don't have to write things like $aba^{-1}b^{-1}$, we can merely write $abab$, and not worry about the exponents. Since $a^2 = \mathbb{1}$ we don't have to worry about higher powers. Because the group is abelian we can not only ignore the exponents we can even ignore order, so we can uniquely identify any element witha set of generators. How many such sets are there? Find a $\subseteq$-minimal set X of generators. Then $|G| = 2^{|X|}$. I did mention boolean rings didn't i. You don't need to know about them yet, but one can at this stage make the point that the power set $\mathcal{P}(X)$ of X becomes a group of this kind (every element is of order 2—we say it is a group of exponent 2) if we take the group operation to be. . . can you guess. . . ?[1] Answer in the footnote.

Sheet 2

Question 1

30 is the LCM of 6 and 10. Lagrange tells you that not only must the order of the group be at least as big as 30, it must be a *multiple* of 30.

[1] The group operation is `XOR`, exclusive OR, and the unit is X.

Question 2

Every element is of order 2 so it can't be C_4.

Question 3

Question 4

You want to say "send gH to Hg", don't you? But it doesn't work, because lots of different gs can give you the same left coset gH but different right cosets! Try prove $gH = g'H \to Hg = Hg'$; it doesn't work. (In fact one can find counterexamples; Dr Wadsley suggests taking $G = D_6$ and H a subgroup of order 2). Annoying.

Something that looks as if it might work is $gH \mapsto Hg^{-1}$.
Want: $gH = g'H \to Hg^{-1} = Hg'^{-1}$.
$g_1H = g_2H$ so
for all a in H there is b in H s.t. $g_1a = g_2b$, which is to say
$(g_1a)^{-1} = (g_2b)^{-1}$
which is to say
$a^{-1}g_1^{-1} = b^{-1}g_2^{-1}$.
In full:

$$(\forall a \in H)(\exists b \in H)(a^{-1}g_1^{-1} = b^{-1}g_2^{-1}).$$

But H is a group, so is closed under inverse so this is

$$(\forall a \in H)(\exists b \in H)(ag_1^{-1} = bg_2^{-1}),$$

which says that

$$Hg^{-1} = Hg'^{-1}.$$

The upshot is that $gH = g'H \to Hg^{-1} = Hg'^{-1}$ as desired. Thus we can send gH to Hg^{-1} since it really doesn't matter which of g and g' we choose.

Notice that this bijection is **natural**. This is a concept to get straight in supervision!

Question 5

The order is obviously 4; it fixes 0 and ∞.
Apparently $g(z) = -((i-1)z - (1-i))/((i-1)z - (1+i))$

Question 6

Unless i am much mistaken each orbit is a hyperbola. None of you picked this up, and i'm not sure why, co's it's not difficult. Perhaps unfamiliar so you get wrongfooted into thinking about differential equations for e^t. Every orbit is a solution of whatever-the-differential-equation-is-for-a-conic.

Question 7

I like to think this is obvious, and i'm not sure what to say.

Question 8

Question 9

The fact that a group acts on itself by conjugation is standard. For any subgroup H one wants to know: "how big is its orbit?". How many different subgroups can you find that are conjugate copies of H, things of the form gHg^{-1}? In principle there might be $|G|$-many, but it might happen that $g_1Hg_1^{-1} = g_2Hg_2^{-1}$ for some $g_1 \neq g_2$. Let us say $g_1 \sim g_2$ iff $g_1Hg_1^{-1} = g_2Hg_2^{-1}$. Certainly $g_1 \sim g_2$ if $g_1g_2^{-1} \in H$! So the answer to "how many ...?" will be : $|G|$ divided by the size of the equivalence classes, aka the index of $\sim$.

Question 10

Think polygons. If the polygon has an odd number of sides then every reflection is about a line through a vertex and the midpoint of the opposite side; if it has an even number of sides then there are two kind of relections. One kind is about lines that go through opposite vertices ("diameters"), and the other is about lines that connect midpoints of opposite sides.

In all three cases any two reflections of any one flavour can be conjugated by rotations.

I really should fire up geogebra and draw some pictures.

Question 11

Question 12

Suppose $|G| = 2p$. Every nonidentity element of G must be of order 2, p or $2p$. If it has a nonidentity element of order $2p$ then it is C_{2p}. So suppose it has nonidentity elements or order 2 and p only. Then it had better turn out to be D_{2p}.

Let C be the cyclic group generated by one of the elements of order p. This was obviously intended by the gods to be the cyclic group of the rotations. It has two cosets. What does the other coset (call it C') consist of? We hope that it consists entirely of involutions.

Question 13

All the stabilisers of elements of X are conjugate copies of one another. Since the group is abelian they must all the same: in an abelian group all subgroups are normal (identical to any conjugate copy). The action is faithful by assumption, which is to say that the intersection of the stabilisers is the trivial group. (No nonidentity element fixes everything). But if they are all the same then the only way their intersection can be the trivial group is if every single one of them is the trivial group. So, for any $x \in X$, no two $g, h \in G$ send x to different things. But if the action is transitive, then for every $y \in X$ there must be g with $gx = y$. One and only one. So $|G| = |X|$.

Question 14

Let G be a group of order p^2, p prime. It acts on itself by conjugation. Think about the kernel of this action, the centraliser of G. It's a subgroup, and so has order 1 or p or p^2 by Lagrange. If it has order p^2 it's the whole of G, so G is abelian. It is has order p then it's C_p so G is going to have to be $C_p \times C_p$ which is also abelian. Finally we have to show that the centraliser cannot be the trivial group.

Sheet 3

Question 1

If H is of index 2 then it has only two cosets. Cosets? Only two left cosets, one of which is H, and only two right cosets, one of which—again—is H. Since the two left cosets (and the two right cosets) partition G it must be that the left coset that isn't H must be the same set as the right coset that isn't H. But then G is clearly normal.

Question 3

Why all the fuss about *normal* subgroups? Here's why .... If G is a subgroup of H then it induces an equivalence relation on (the members of) H, and it can do this in at least three ways. The partition of H into left cosets is the set of equivalence classes of one of them (what is this equivalence relation?); the partition of H into right cosets is the set of equivalence classes of another of them (what is this equivalence relation?); there is a third defined by $h_1 \sim_G h_2$ if $h_1 \cdot (h_2)^{-1} \in G$. (Check that that really is an equivalence relation(!)). In each case the *quotient* is the set of equivalence classes. Is the quotient a group? Might be. How would we define a group operation on the equivalence classes. Well, to multiply two equivalence classes together, take a member of the one and a member of the other, multiply them together and take the equivalence class of the result. Does this work? Might it make a difference which representatives you take? If it does make a difference then that avenue of putting a group structure on the quotient (at least) is not open to you. Might you not need special conditions on G to ensure that it doesn't matter which representatives you take? You might indeed: and i suppose in principle the special conditions might be different for the three equivalence relations we consider. However if G is a **normal** subgroup of H then we can show that it doesn't matter which representative we take. In fact if G is normal then the two equivalence relations "...belong to same left coset" and "...belong to same right coset" are the same equivalence relation, and that simplifies matters enormously. In fact G being normal makes all three equivalence relations the same.

Specifically (and this was question 7, which we might as well deal with here) we want to show that if H is a normal subgroup of G we can define a group operation on the left H-cosets by taking representatives from two cosets, multiplying them togther using the group operations of G and then presenting the coset of the product as the output of our new group operation on the cosets. *It doesn't matter which representatives we pick from the cosets.* What we have to show is that if a' belongs to the same coset as a and b' belongs to the same coset as b then $a'b'$ belongs to the same coset as ab. (A language point: we want to say that the equivalence relation of belonging-to-the-same-left-coset **is a congruence relation for** the multiplication of G.) Two things belong to the same left H coset if you can get one from the other by multiplying it on the right by an element of H. So let us multiply ah_1 (which belongs to the same left-coset as a) by bh_2 (which belongs to the same left-coset as b) and hope that ah_1bh_2 will belong to the same left-coset as ab. ($h_1, h_2 \in H$ of course). We want to tweak the word ah_1bh_2 into something of the form abh_3. Observe that $h_1b = bb^{-1}h_1b$ and we can bracket this as $b(b^{-1}h_1b)$ so we can rewrite ah_1bh_2 as $ab(b^{-1}h_1b)h_2$. Now, **since H is normal** (and therefore a union of conjugacy classes) $b^{-1}h_1b$ is also in H, whence $(b^{-1}h_1b)h_2$ is in H and we can call it h_3, so that $ah_1bh_2 = abh_3$ as desired.

Where were we? H has got to be the kernel of a homomorphism. Now that the normality of H has ensured that the obvious candidate for a group structure on the set of cosets is indeed a group structure, we can send elements of G to their cosets and find that this is a group homomorphism. (Check it!) The kernel of this homomorphism is the normal subgroup H.

Question 4

The quaternion group is a counterexample as it happens, but i'm not sure how you are supposed to know that. I suppose it's one of the things you pick up behind the bike sheds. I think the point of this question is for you to attempt to prove that if every subgroup is normal then the group is abelian, and find the failure instructive and illuminating.

Question 5

I don't know about you, Dear Reader, but for your humble correspondent this question usefully illustrates the fact that, on the whole, G is **not** reliably isomorphic to $(G/H) \times H$. In the case we are considering here G is a cyclic group (as it might be: C_{25}) and H, being a subgroup of a cyclic group, is cyclic itself (in this case let it be C_5). Then the quotient is obviously C_5 again. But $C_5 \times C_5$ is not C_{25}. I think they say that C_{25} "*is an extension of*" C_5 "*by*" C_5. (When explaining this to Wilfrid i incautiously used C_{15} as my illustration, forgetting that $C_3 \times C_5$ really is C_{15}, beco's 3 and 5 are coprime. He picked me up on it.)

Question 6

I find myself thinking of this quotient group as the rational interval $[0, 1)$ (yes i think i *do* mean the half-open interval) with addition mod 1.

Question 8

This object is apparently called the *Heisenberg Group* and it is something to do with Quantum Mechanics. It's a simple diagram chase to verify that G is a subgroup of $GL_3(\mathbb{R})$ and that H is a normal subgroup of G.

Consider the function that sends the displayed matrix (i'll try to draw a picture) to $x + iy \ldots$

Question 10

The image of θ is the set of linear combinations of a and b. I think they want you to say that it's the set of all integer multiples of HCF(a, b).

Question 11

Apparently this is a routine technique in the study of finite groups. G acts on the quotient (the set of cosets) G/H. This action gives us a homomorphism from G to the ("symmetric") group of all permutations of G/H. The hypothesis we are given is that $|G|$ does not divide the cardinality of this symmetric group. The effect of this is that the homomorphism cannot be injective: if it were the G would be iso to a subgroup of the symmetric group and its size would divide the cardinality of the symmetric group (by Lagrange). This draws our attention to the kernel of the homomorphism, which must therefore be a normal subgroup of G. [Do i need to explain why it's a subgroup of H?]

Question 12

It has a normal subgroup of order 4, so the quotient is of order 7 and must be C_7. The normal subgroup is abelian and the quotient is abelian. Is that enuff to make the original group abelian? No, as Gareth points out to me, the rotations in a dihedral group are a normal subgroup (abelian) and the quotient is abelian but dihedral groups are not abelian.

Question 13

$\mathbb{Z}/n\mathbb{Z}$ is the integers mod n (think of it as the regular n-gon). So think how the isometries of $\mathbb{Z}$ act on the regular n-gon. Well, what are these isometries anyway? Translations and reflections. Clearly translations are going to give rise to rotations of the regular n-gon and reflections will give rise to, well, reflections! So we have a homomorphism from the group of isometries of $\mathbb{Z}$ to D_{2n}. So: what is the kernel of this homomorphism? Clearly any translation of $\mathbb{Z}$ by a multiple of n is going to do nothing and will therefore be in the kernel.

Sheet 4