# ALGEBRA I. PROBLEM SET 5.

SOLUTIONS.

Here are solutions to the set 5 problems. Questions #8, #9 and #10 are substantial extensions from what we covered, so well done if you made sense of them.

**#1** [Q8, §5.1.] In each of (a) to (e) give an example of a group with the specified properties:

(a) an infinite group in which every element has order 1 or 2

(b) an infinite group in which every element has finite order but for each positive integer $n$ there is an element of order $n$

(c) a group with an element of infinite order and an element of order 2

(d) a group $G$ such that every finite group is isomorphic to some subgroup of $G$

(e) a nontrivial group $G$ such that $G \cong G \times G$.

**Solution:** For (a) use the group $G = Z_2 \times Z_2 \times \cdots$. For (b) the obvious $\prod_{i \in \mathbb{Z}_{\geqslant 1}} Z_i$ doesn't quite work since the element with $i$th component equal to a generator of $Z_i$ has infinite order. Take the subgroup where all but finitely many components are 1. This is called the *restricted direct product* or the *direct sum* and denoted

$$\bigoplus_{i \in \mathbb{Z}_{\geqslant 1}} Z_i.$$

For (c), (d), (e) you can use $\mathbb{Z} \times Z_2$, $\prod_{i \in \mathbb{Z}_{\geqslant 1}} S_i$ and $G$ from (a) respectively.

**#2** How many non-isomorphic abelian groups are there of order one million?

**Solution:** From the Elementary Divisor Decomposition, the number of non-isomorphic abelian groups of order $2^6 5^6$ is $p(6) \cdot p(6)$. Check that the number of partitions of 6 is 11, so the answer is 121. (Note that the cyclic group of order one million is counted since it's $\cong Z_{2^6} \times Z_{5^6}$.)

**#3** [Q11, §5.5.] Classify groups of order 28 (there are 4 isomorphism types).

**Solution:** From the classification theorem, two distinct abelian groups of order 28 are $Z_4 \times Z_7$ and $Z_2 \times Z_2 \times Z_7$. Two non-abelian groups of this order are $Z_2 \times D_{14}$ and $D_{28}$. Since all are non-isomorphic, this accounts for the 4 isomorphism types.

Taking the "(there are 4 isomorphism types)" as more of a hint than a statement, we can use semidirect products to carry out the classification. Let $G$ be a group with order 28. From the Sylow theorems we see that $n_2 = 1$ or 7 and $n_7 = 1$, meaning that $G$ has a unique Sylow 7-subgroup, $H$, and at least one Sylow 2-subgroup, $K$. Since $H \trianglelefteq G$ we have $HK \leqslant G$. Also $H \cap K = 1$ because 4 and 7 are relatively prime. It follows from the semidirect product recognition theorem that $HK = H \rtimes K$. Further $|HK| = |H||K|/|H \cap K| = |H||K| = |G|$ so that $G = H \rtimes K$.

It remains to list all the semidirect products $H \rtimes K$ that are possible. Since $|K| = 4$ we must have $K = Z_4$ or $Z_2 \times Z_2$. The only option for $H$ is $Z_7$. Each semidirect product requires a homomorphism $\phi : K \to \operatorname{Aut} H$. We can see that $\operatorname{Aut} H \cong Z_6$ by examining the 6 possibilities for where an automorphism of $H$ sends its generator (or noting that $\operatorname{Aut} Z_7 \cong (\mathbb{Z}/7\mathbb{Z})^\times \cong Z_6$ as we saw in problem set 4).

*Case (i).* For $K = Z_4 = \langle x \rangle$ and $Z_6 = \langle y \rangle$ we see the only possible homomorphisms $Z_4 \to Z_6$ have (a) $x \mapsto 1$ or (b) $x \mapsto y^3$. In option (a) the semidirect product reduces to the direct product $Z_4 \times Z_7$. In option (b) we get a different group $Z_7 \rtimes Z_4$.

*Date*: Nov 1, 2012.

*Case (ii).* For $K = Z_2 \times Z_2 = \langle a, b \mid a^2 = b^2 = (ab)^2 = 1\rangle$ and $Z_6 = \langle y\rangle$ we see the only possible homomorphisms $Z_2 \times Z_2 \to Z_6$ have (a) $a, b \mapsto 1$, (b) $a \mapsto y^3, b \mapsto 1$, (c) $a \mapsto 1, b \mapsto y^3$ or (d) $a \mapsto y^3, b \mapsto y^3$. In option (a) the semidirect product reduces to the direct product $Z_2 \times Z_2 \times Z_7$. Options (b), (c), (d) can be shown to yield isomorphic results which we may call $Z_7 \rtimes (Z_2 \times Z_2)$.

**#4** [Q1, 14, 17, §6.1.] A subgroup $H \leqslant G$ is *characteristic* in $G$ if every automorphism of $G$ maps $H$ to itself (see page 135 of the text). Since conjugation is an automorphism, this implies that characteristic subgroups are normal. Prove one of the following (all are true):
(a) $Z_i(G)$ is a characteristic subgroup of $G$
(b) $G^i$ is a characteristic subgroup of $G$
(c) $G^{(i)}$ is a characteristic subgroup of $G$.

**Solution to (a):** Let $\phi : G \to G$ be an automorphism. If an element $g$ of $G$ commutes with all elements of $G$ then $\phi(g)$ commutes with all elements of $G$ also. Therefore $Z_1 = Z(G)$ is characteristic in $G$ (as is $Z_0 = 1$). Recall the defining relation for $Z_{i+1}$:

$$Z_{i+1}/Z_i = Z(G/Z_i) \tag{0.1}$$

Note that if $N \trianglelefteq G$ and $\phi(N) = N$ then we get a well defined automorphism $\phi : G/N \to G/N$ given by $gN \mapsto \phi(g)N$. Hence, for $i = 1$ in (0.1),

$$\phi(Z_2/Z_1) = \phi(Z(G/Z_1)) = Z(G/Z_1) = Z_2/Z_1$$

and it follows that $\phi(Z_2) = Z_2$. Repeating this argument, induction shows $\phi(Z_i) = Z_i$ and $Z_i(G)$ is a characteristic subgroup of $G$ for all $i$.

**Solution to (b):** Let $\phi : G \to G_1$ be a homomorphism. Check that $\phi([g, h]) = [\phi(g), \phi(h)]$. It follows that for any two subgroups $H, K \leqslant G$, the commutator subgroup they generate, $[H, K]$, satisfies

$$\phi([H, K]) = [\phi(H), \phi(K)]. \tag{0.2}$$

Hence, for $\phi : G \to G$ an automorphism, we have

$$\begin{aligned}\phi(G^0) &= \phi(G) = G = G^0,\\ \phi(G^1) &= \phi([G, G^0]) = [\phi(G), \phi(G^0)] = [G, G^0] = G^1.\end{aligned}$$

Continuing, an obvious induction shows that $\phi(G^i) = G^i$ for all $i$ and hence $G^i$ is characteristic in $G$ for all $i$.

**Solution to (c):** Very similar to (b).

**#5** Show that the Heisenberg group $H(F)$ (over a field $F$) is nilpotent and find its nilpotence class.

**Solution:** Use the lower central series $H(F)^i$. We have $H(F)^1 = [H(F), H(F)]$ generated by all the commutators $[x, y] = x^{-1}y^{-1}xy$ for $x, y \in H(F)$. A calculation shows

$$\left[\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}, \begin{pmatrix}1 & d & e\\ 0 & 1 & f\\ 0 & 0 & 1\end{pmatrix}\right] = \begin{pmatrix}1 & 0 & af - dc\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$$

so that

$$H(F)^1 = \left\{ \begin{pmatrix}1 & 0 & b\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} \middle| \, b \in F \right\} \neq 1.$$

Continuing, we have $H(F)^2 = [H(F), H(F)^1] = 1$ and so $H(F)$ is nilpotent with nilpotency class 2.

**#6** [Q5, §3.4.] Prove that subgroups and quotient groups of a solvable group are solvable.

**Solution:** There are a quite a few ways to do this question. Here are the simplest.

*Subgroups solvable.* Let $G$ be a group with subgroup $H$. An easy way to check that $H$ is solvable is to compare its commutator series with that of $G$. We have $H^{(0)} = H \leqslant G = G^{(0)}$. Also $H^{(1)} = [H, H] \leqslant [G, G] = G^{(1)}$. Continuing with induction we see $H^{(i)} \leqslant G^{(i)}$ for all $i \in \mathbb{Z}_{\geqslant 0}$. If $G$ is solvable then $G^{(i)} = 1$ for some $i$. This implies $H^{(i)} = 1$ and so $H$ is solvable.

*Quotient groups solvable.* Let $G$ be a group with normal subgroup $N$. Let $\phi : G \to G/N$ be the projection map. Suppose we have a series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

with all $G_{i+1}/G_i$ abelian, demonstrating that $G$ is solvable. To see that $G/N$ is also solvable look at the series

$$1 = \phi(G_0) \leqslant \phi(G_1) \leqslant \cdots \leqslant \phi(G_{n-1}) \leqslant \phi(G_n) = G/N. \tag{0.3}$$

It is straightforward to verify that for any homomorphism $\phi : B \to C$

$$A \trianglelefteq B \implies \phi(A) \trianglelefteq \phi(B),$$
$$A/B \text{ abelian } \implies \phi(A)/\phi(B) \text{ abelian.}$$

It now follows from (0.3) that

$$1 = \phi(G_0) \trianglelefteq \phi(G_1) \trianglelefteq \cdots \trianglelefteq \phi(G_{n-1}) \trianglelefteq \phi(G_n) = G/N$$

with all quotients $\phi(G_{i+1})/\phi(G_i)$ abelian, proving that $G/N$ is solvable.

With the above notation, an even quicker way to check that $G/N$ is solvable is to use (0.2):

$$(G/N)^{(1)} = \phi(G)^{(1)} = [\phi(G), \phi(G)] = \phi([G, G]) = \phi(G^{(1)}).$$

Repeating this proves $(G/N)^{(i)} = \phi(G^{(i)})$ and then $G^{(n)} = 1$ implies $(G/N)^{(n)} = 1$. See Proposition 10 in §6.1 of the text.

**#7** [Q8, §3.4.] Show that a group is solvable if and only if all its composition factors are of prime order by using the steps outlined in this question - see the text.

**Solution:** One direction is easy: if all composition factors of a group $G$ are of prime order then they are abelian and so $G$ is solvable.

In the other direction, suppose $G$ is solvable:

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G \tag{0.4}$$

with $G_{i+1}/G_i$ abelian. We want to add more groups to the series (0.4) to ensure that all the successive quotients are of prime order (ie we want a *refinement* of (0.4)).

What can we add between $G_i$ and $G_{i+1}$? By the Jordan-Holder theorem we know that $G_{i+1}/G_i$ has a composition series:

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_r = G_{i+1}/G_i. \tag{0.5}$$

Since the quotients $N_{j+1}/N_j$ are simple and abelian (since $G_{i+1}/G_i$ is abelian) they must be of prime order. Let $\pi : G_{i+1} \to G_{i+1}/G_i$ be the projection map. Let

$$H_j = \pi^{-1}(N_j) \quad \text{so that} \quad H_j/G_i = N_j.$$

Check that $N_j \trianglelefteq N_{j+1} \implies H_j \trianglelefteq H_{j+1}$ (it follows from the Lattice Isomorphism Theorem). Then we see (with the Third Isomorphism Theorem) that

$$H_{j+1}/H_j \cong (H_{j+1}/G_i)/(H_j/G_i) \cong N_{j+1}/N_j$$

implying $H_{j+1}/H_j$ has prime power order. Thus we can fill in

$$G_i = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_r = G_{i+1}$$

and similarly between the other groups in the series (0.4). All the successive quotients are of prime order and therefore simple, so this gives the desired composition series for $G$.

**#8** [Q6, §6.1.] Show that if $G/Z(G)$ is nilpotent then $G$ is nilpotent.

**Solution:** Consider the upper central series for $G$:

$$1 = Z_0 \trianglelefteq Z_1 \trianglelefteq Z_2 \trianglelefteq \cdots \trianglelefteq G \tag{0.6}$$

where we have the defining relation for $Z_{i+1}$:

$$Z_{i+1}/Z_i = Z(G/Z_i) \tag{0.7}$$

and $G$ is nilpotent if $Z_n = G$ for some $n$. We have $Z_1 = Z(G)$, the center of $G$. We want to compare (0.6) to the upper central series for $G/Z_1$. Recall that $Z_1 \trianglelefteq G$ so we may take the quotients of everything except the first term in (0.6) by $Z_1$:

$$1 = Z_1/Z_1 \trianglelefteq Z_2/Z_1 \trianglelefteq \cdots \trianglelefteq G/Z_1. \tag{0.8}$$

In fact (0.8) is the upper central series for $G/Z_1$. To check this we need to prove the analog of (0.7):

$$(Z_{i+1}/Z_1)/(Z_i/Z_1) = Z\Big((G/Z_1)/(Z_i/Z_1)\Big). \tag{0.9}$$

But (0.7) and the Third Isomorphism Theorem show that the two sides of (0.9) are isomorphic. We get the equality in (0.9) since the center $Z\Big((G/Z_1)/(Z_i/Z_1)\Big)$ is characteristic in $(G/Z_1)/(Z_i/Z_1)$, see question **#4**.

So we have proved a formula for the upper central series for $G/Z_1$:

$$Z_i(G/Z_1) = Z_{i+1}/Z_1.$$

If $G/Z_1$ is nilpotent then $Z_n(G/Z_1) = G/Z_1$ for some $n$. Therefore $Z_{n+1} = G$ and hence $G$ is nilpotent (with nilpotency class at most one more than $G/Z_1$).

A similar proof shows the more general formula

$$Z_i(G/Z_j) = Z_{i+j}/Z_j.$$

**#9** [Q1, §6.3.] Let $F_1$ and $F_2$ be free groups of finite rank. Prove that $F_1 \cong F_2$ if and only if they have the same rank. What facts do you need to extend your proof to infinite ranks (where the result is also true)?

**Solution:** This question is a bit misleading, since we haven't shown that the rank of a free group is well defined. A group $G$ is free if there is a subset $S$ of $G$ so that $G = F(S)$. But, until we can show otherwise, there could be another subset $T$ of $G$ (with a different cardinality) so that $G = F(T)$ also.

• Suppose $F_1$ and $F_2$ are free groups with $F_1 = F(S)$ and $F_2 = F(T)$. If $S$ and $T$ have the same cardinality (possibly infinite) then we can prove $F_1 \cong F_2$ as follows: Let $\lambda : S \to T$ be a bijection. Consider the composite map from $S$ to $F(T)$ given by

$$S \xrightarrow{\lambda} T \hookrightarrow F(T).$$

By the universal property, it extends to a homomorphism $\alpha : F(S) \to F(T)$. Similarly, the map

$$T \xrightarrow{\lambda^{-1}} S \hookrightarrow F(S)$$

extends to a homomorphism $\beta : F(T) \to F(S)$. Then $\beta \circ \alpha : F(S) \to F(S)$ fixes $S$ and so, by uniqueness, must be the identity map. Also $\alpha \circ \beta : F(T) \to F(T)$ fixes $T$ and must be the identity map. We have shown that $\alpha$ and $\beta$ are isomorphisms between $S$ and $T$.

• In the other direction we want to show that for two isomorphic free groups, $F_1 \cong F_2$, that if $F_1 = F(S)$ and $F_2 = F(T)$ then $S$ and $T$ have the same cardinality. The question restricts $S$ and $T$ to finite sets.

Suppose $\lambda : F_1 \to F_2$ is an isomorphism. By the universal property, similarly to the above argument, it is straightforward to show that $F_2 = F(\lambda(S))$ and $F_1 = F(\lambda^{-1}(T))$. Therefore, if two free groups are isomorphic we can certainly express them both as free groups on sets of the same (possibly infinite) cardinality. It is more difficult to show that $|S|$ and $|T|$ above must be equal.

One method is to consider the commutator $F_1' = [F_1, F_1]$ of $F_1$. Then $F_1/F_1'$ is necessarily abelian and can be shown to be isomorphic to the free abelian group $\mathbb{Z}^{|S|}$, ie the direct sum of $|S|$ copies of $\mathbb{Z}$ (see (0.11), (0.12) in question **#10** below). Similarly $F_2/F_2' \cong \mathbb{Z}^{|T|}$. Then $F_1 \cong F_2 \implies \mathbb{Z}^{|S|} \cong \mathbb{Z}^{|T|}$. If $|S|$ and $|T|$ are finite then, by the uniqueness part of the Fundamental Theorem for Finitely Generated Abelian Groups, we must have $|S| = |T|$. We have proved what we set out to:

$$F(S) \cong F(T) \implies |S| = |T| \qquad (|S|, |T| < \infty). \tag{0.10}$$

To extend the result to free groups on infinite sets we would need to know that these free abelian groups are isomorphic exactly if their free generating sets have the same cardinality.

**#10** [Q11, §6.3.] This question is on the universal property of free abelian groups. See the text.

**Solution:** Let $F(S)$ be the free group on $S$ and let $F(S)'$ be the commutator subgroup $[F(S), F(S)]$. The free abelian group $A(S)$ is defined in this question as the group with presentation $(S, R)$ for $R = \{[s,t] | s, t \in S\}$. By definition this means that

$$A(S) = F(S)/\text{the normal closure of } \langle R \rangle \text{ in } F(S).$$

But $\langle R \rangle = F(S)'$ and $F(S)'$ is already normal in $F(S)$ (this can be seen for example by using (0.2) with $\phi$ given by conjugation by any element in $F(S)$). Therefore

$$A(S) = F(S)/F(S)'. \tag{0.11}$$

Check that $A(S)$ is abelian (see also Prop 7(3) in §5.4) and if $|S| = 1$ then $A(S) \cong \mathbb{Z}/1 \cong \mathbb{Z}$.

• We now prove that $A(S)$ satisfies the required universal property. Let $G$ be any abelian group. Given a map $S \to G$ there is a unique extension to a homomorphism $\phi : F(S) \to G$ by the universal property for $F(S)$. Since $G$ is abelian we obtain a homomorphism $\phi : F(S)/F(S)' \to G$, see Prop 7(5) in §5.4. This proves: *given any set map $\phi : S \to G$, for $G$ an abelian group, then there exists a unique homomorphism $\Phi : A(S) \to G$ so that $\Phi|_S = \phi$.* (Note that since this universal property defines $A(S)$ up to (a unique) isomorphism, it is often taken as the definition of $A(S)$.)

• This universal property can be used to describe $A(S)$ precisely. We now claim:

$$A(S \cup T) \cong A(S) \times A(T)$$

for all disjoint sets $S, T$. Consider first the "inclusion" map

$$S \cup T \to A(S) \times A(T)$$

where $s \mapsto (s, 0)$ and $t \mapsto (0, t)$. By the universal property for $A(S \cup T)$ we see this map extends to a homomorphism $\alpha : A(S \cup T) \to A(S) \times A(T)$. Similarly

$$S \hookrightarrow A(S \cup T), \quad T \hookrightarrow A(S \cup T)$$

extend to homomorphisms $\beta_1 : A(S) \to A(S \cup T)$ and $\beta_2 : A(T) \to A(S \cup T)$. Combine these to get a homomorphism $\beta : A(S) \times A(T) \to A(S \cup T)$ given by $\beta((u, v)) = \beta_1(u) + \beta_2(v)$. Check that composing $\alpha$ with $\beta$ fixes $S$ and $T$ so that, by uniqueness, their compositions are the identity. Hence they're isomorphisms, proving the claim.

Since $A(S) \cong \mathbb{Z}$ for $|S| = 1$ as we saw earlier, induction now shows that for $m \in \mathbb{Z}_{\geqslant 1}$ we have

$$A(S) \cong \mathbb{Z}^m \tag{0.12}$$

when $|S| = m$.