ALGEBRA 2B (MA20217)

ALGEBRA 2B MOCK EXAM

This is a mock exam which has not been checked as carefully as a real exam would be. In the real exam you will be asked to attempt all of Section A and two questions out of three from Question B (if you attempt them all, your best answers will count): here I have just indicated those sections with a letter after the question number. The numbers in square brackets are a general indication of how many marks that part would be worth if there were any marks: full marks would be 60.

1A. Define what is meant by a *normal subgroup* of a group G. [2]
Show that if $\phi\colon G \to H$ is a group homomorphism then the kernel $\operatorname{Ker}\phi$ is a normal subgroup of G. [2]
Suppose that $\psi\colon G \to H$ is a map such that $\{g \in G \mid \phi(g) = 1\}$ is a normal subgroup of G. Is it true that ϕ is necessarily a homomorphism? Give a proof or a counterexample. [2]
Show that there cannot exist a surjective homomorphism from S_5 to S_4 (the symmetric groups). [2]
Solution: *$H \subseteq G$ is a normal subgroup of G if H is a subgroup and $g^{-1}Hg = H$ for every $g \in G$.*
Put $K = \operatorname{Ker}\phi$ and notice first that K is a subgroup because it is not empty since $\phi(1) = 1$ so $1 \in K$, and if $a, b \in K$ then $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = 1$ so $ab^{-1} \in K$. Similarly it is normal because if $k \in K$ and $g \in G$ then $\phi(g^{-1}kg) = \phi(g)^{-1}\phi(k)\phi(g) = \phi(g)^{-1}\phi(g) = 1$ so $g^{-1}kg \in K$.
This is not usually true. For example, the map $x \mapsto x^2$ from $\mathbb{Z}$ to $\mathbb{Z}$ has "kernel" 0 which is a normal subgroup of $\mathbb{Z}$, but it is not a homomorphism because $(1+1)^2 \neq 1^2 + 1^2$.
The order of S_5 is 120 and the order of S_4 is 24, so such a homomorphism would have to have kernel of order 5. But a subgroup of order 5 must be cyclic (because 5 is prime) so it is generated by the powers of (12345) after relabelling the symbols if necessary. But $(12)(12345)(12) = (13452)$ which is not a power of (12345).

2A. Define what it means for an ideal P to be a *prime ideal* of a commutative ring R. [2]
Give an example of a ring in which every nonzero prime ideal is maximal. [1]
Consider the ring $Q = \{\frac{a}{b} \in \mathbb{Q} \mid \operatorname{hcf}(b, 3) = 1\}$. Show that $\langle 3\rangle$ is a prime ideal in Q. Are there any other nonzero prime ideals in Q? Justify your answer briefly. [5]
Solution: *P is a prime ideal of R if $xy \in P$ implies $x \in P$ or $y \in P$.*
$\mathbb{Z}$ is such a ring, for instance because $\mathbb{Z}/p$ is a field (there are several other ways to show this).

$\langle 3\rangle$ is an ideal by definition. Suppose that $x=\frac{a}{b}$, $y=\frac{c}{d}$ and $xy=\frac{ac}{bd}\in\langle 3\rangle$. Then there exists $\frac{e}{f}\in Q$ such that $\frac{3e}{f}=\frac{ac}{bd}$, so $3bde=acf$. But 3 does not divide f, and 3 is prime so it must divide a or c: wlog $3|a$, say $a=3a'$. Now $x=3\frac{a'}{b}\in\langle 3\rangle$.
There are no other nonzero prime ideals because every nonzero element of Q that is not in $\langle 3\rangle$ is a unit: if 3 does not divide a then $\frac{a}{b}\in Q$ has the inverse $\frac{b}{a}\in Q$. So $\langle 3\rangle$ is a maximal ideal (in fact we could have used this to prove that it is a prime ideal) so any other prime ideal P would have to be contained in $\langle 3\rangle$, i.e. consist of multiples of 3. But then we have $3x\in P$ for some x: choose this x to be divisible by 3 as few times as possible. Now $3\notin P$ and $x\notin P$ so P is not prime.

3A. State and prove the Chinese Remainder Theorem. [5]
If the characteristic of R is n (possibly $n=0$) and I is an ideal of R, show that $\operatorname{char} R/I$ divides $\operatorname{char} R$. [3]
Solution:
The first part is bookwork. For the second part, if $n=0$ there is nothing to prove since every integer (even 0) divides 0: otherwise, consider addition only and look at the subgroup G generated by 1 (this is the prime subring). It is a group of order n, and the prime subring of R/I is $G/(I\cap G)$ so we have $\operatorname{char} R=|G|=|G/(I\cap R)|\cdot|I\cap R|=|I\cap R|\cdot\operatorname{char} R/I$.

4B. Define the terms *Euclidean domain*, *principal ideal domain* (PID) and *unique factorisation domain* (UFD). [5]
Show that every Euclidean domain is a PID. [5]
State Eisenstein's criterion for irreducibility of an element of $\mathbb{Q}[x]$. [2]
For each of the following polynomials, say with brief reasons whether or not it is irreducible in $\mathbb{Q}[x]$.
(a) $x^4-2x^3-4x^2-17x-20$
(b) $2x^4+5x^3+25x^2-10x-10$
(c) $2x^4+13x^3+2x^2+3x+2$
Solution: *All but the polynomials are bookwork.*
(a) I don't see anything obvious so let's try some substitutions. Replacing x with $x+1$ gives a constant coefficient of -42, which is encouraging because that gives us a chance of Eisenstein with $p=2$, 3 or 7, but unfortunately the x^3 coefficient is 2 and the x coefficient is odd because of the 17. Before we give up, though, let's try replacing x with $x-1$. That gives an x^3 coefficient of 6 but the constant coefficient is $1+2-4+17-20=-4$ which is no good. Perhaps we should try factorising. No linear factors (calculus) so if anything it's $(x^2+ax+b)(x^2+cx+d)$, and then we have $bd=-20$ and $a+c=-2$. Let's do some guessing. How about $b=4$ and $d=-5$? Then the x term gives $-5a+4c=-17$ and $a=-c-2$ so that's $9c=-27$. Lucky! If we had picker $b=-4$ and $d=5$ we'd have had to try again. But now we are being told $c=-3$ and $a=1$: does that work? $(x^2+x+4)(x^2-3x-5)=x^4-2x^3-4x^2-17x-20$. Yes. (This was a

bit fortunate. 20 *is too factorisable. We might have wasted time with* 10 *and* -2 *or* -20 *and* 1. *This is most likely to work when the constant term is prime).*
(b) That's Eisenstein, with $p = 5$. *Irreducible.*
(c) Lets try some substitutions again. Replacing x *with* $x + 1$ *gives us a constant term* 22, *but* $x - 1$ *gives* 10. *Where did we just see that? Oh yes, it's just the polynomial from (b) again. Irreducible.*
5B. Define what it means for a group G to *act on a set* X. [2]
If G acts on X, say what is meant by the *orbit* of an element of $x \in X$, and what is meant by the *stabiliser* of an element $x \in X$. [4]
Show that the rule $g(h) = ghg^{-1}$ defines an action of G on G, for any group G, called the conjugation action. [2]
Take $G = S_n$ and consider the conjugation action of S_n on S_n.
Suppose that $\sigma = (12\ldots k)$, for some $k \leq n$. What is the orbit of σ under this action? What is its stabiliser? [4]
The alternating group A_5 is a subgroup of S_5 so it also acts on S_5 by conjugation. Consider the elements (12345) and (21345). Do they have the same orbit under the action of A_5? Justify your answer carefully. [6]
Solution: *The first two are bookwork. The conjugation action was mentioned: we just need to check that conjugation by* 1 *does nothing, which is obvious, and that conjugation by* gk *is the same as conjugation by* k *followed by conjugation by* g. *And indeed* $(gk)(h) = gkh(gk)^{-1} = g(khk^{-1})g^{-1}$. *The most difficult thing here is for the examiner, who has to remember to write* ghg^{-1} *and not* $g^{-1}hg$.
If we take any other k*-cycle, say* $\tau = (a_1 \ldots a_k)$, *then* σ *is conjugate to* τ *via any element of* S_n *that sends* 1 *to* a_1, 2 *to* a_2 *and so on (the element* a, *in fact). And all elements of* S_n *do that for some* $a_1 \ldots a_n$ *so that's the orbit: all the elements with the same cycle type, in this case all the* k*-cycles. The stabiliser is all the elements that permute* $(1 \ldots k)$ *cyclically, i.e. the ones that have* $(1 \ldots k)$ *in their cycle decomposition. They can do what they like to the other* $n - k$ *symbols.*
These two don't have the same orbit under A_5. *The recipe above tells us that we can get from one to the other by conjugating by* (12), *but that's odd. The only other thing we could do would be to conjugate by something in the stabiliser, but those are 5-cycles and 5-cycles are even permutations. So we can do it only with* (12)*(5-cycle) and that's odd, so we can't do it in* A_5.

6B. Suppose that G is a group and $S \subseteq G$ is a subset. Say what is meant by the *subgroup* $\langle S \rangle$ *generated by* S. [2]
Show that $\langle S \rangle$ is equal to the intersection of all subgroups of G that contain S. [2]
If H_1 and H_2 are both subgroups of a group G, the *product subgroup* H_1H_2 is defined to be $\langle R \rangle$, where $R = \{h_1h_2 \mid h_1 \in H_1,\, h_2 \in H_2\}$

(a) Explain why $H_1H_2 = H_2H_1$, even if G is not abelian. [2]
(b) If S_1 and S_2 are subsets of G, show that $\langle S_1 \cup S_2\rangle = \langle S_1\rangle\langle S_2\rangle$. [2]
(c) Is it true that $\langle S_1 \cap S_2\rangle = \langle S_1\rangle \cap \langle S_2\rangle$? Give a proof or a counterexample. [2]
(d) Suppose that $S \subseteq G$ and $gSg^{-1} \subseteq S$ for all $g \in G$. Does it follow that $\langle S\rangle$ is a normal subgroup of G? Give a proof or a counterexample. [2]
(e) If a, $b \in G$ then the *commutator* of a and b, denoted $[a, b]$, is the element $[a, b] = aba^{-1}b^{-1} \in G$. Let $C \subset G$ be the set of all commutators, i.e. $C = \{[a, b] \mid a, b \in G\}$, and let $G' = \langle C\rangle$. Show that G' is a normal subgroup of G, that G/G' is abelian, and that if H is a normal subgroup of G such that G/H is abelian then there is a surjective group homomorphism $G/H \to G/G'$. [6]
Solution: *The first part is bookwork. For the second part, If a subgroup H of G contains S then it contains $\langle S\rangle$ because H is closed under the group operations. Hence $\langle S\rangle$ is contained in this intersection. On the other hand an element that is in all subgroups of G that contain S is in $\langle S\rangle$ as that is one of those subgroups. So $\langle S\rangle$ contains the intersection.*
(a) is a trick really. R contains both H_1 and H_2 (take $h_2 = 1$ and then take $h_1 = 1$) so actually $H_1H_2 = \langle H_1 \cup H_2\rangle$, which obviously doesn't depend on the order.
(b) is the same thing. Both sides consist of words with letters from (or inverses of letters from) S_1 and S_2.
(c) is false. You could take the integers mod 3 and $S_1 = \{1\}$, $S_2 = \{2\}$. Those both generate $\mathbb{Z}/3$, but their intersection is empty.
(d) Yes. One way to see this is to say that $gs_1 \dots s_kg^{-1} = (gs_1g^{-1}) \dots (gs_kg^{-1})$ and if $s_i \in S$ then $gs_ig^{-1} \in S$, while if $s_i^{-1} \in S$ then $(gs_ig^{-1})^{-1} = gs_i^{-1}g^{-1} \in S$.
(e) We use (d), noting that $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$. Hence G' is a normal subgroup. Moreover, in any group, $[a, b] = 1$ if and only if $ab = ba$ and applying that to G/G' we get $[aG', bG'] = [a, b]G' = 1_{G/G'}$ so aG' and bG' commute, so G/G' is abelian. The last part comes from the first isomorphism theorem: since the quotient is abelian we must have killed all the commutators, i.e. $H \supseteq G'$, so we can do that first. and then go on as in Theorem II.24.

GKS, 6/4/23