PURDUE UNIVERSITY

Department of Mathematics

HONORS ALGEBRA

MA 45000 – SOLUTIONS

14th December 2022   120 minutes

This paper contains **EIGHT** *questions worth a total of* **200 points**.
All EIGHT answers will be used for assessment.
Calculators, textbooks, notes and cribsheets are **not** *permitted in this examination.*

Do not turn over until instructed.

1. [4+4+4+4+4+4+4+4+4+4=40 points] Decide which of the following statements are necessarily true, and which may be false. Mark those which are true with “T”, and those which may be false with “F”.

a. The group $\mathbb{Z}_3 \times \mathbb{Z}_5$ is cyclic.

Solution: TRUE (The orders 3 and 5 of $\mathbb{Z}_3$ and $\mathbb{Z}_5$ are coprime, and each group is cyclic, so $\mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$).

b. The alternating group A_5 has an element of order 6.

Solution: FALSE (The only elements of S_5 having order 6 have the shape $(a, b, c)(d, e)$, but this is an odd permutation so does not belong to A_5).

c. Suppose that G is a finite group with an abelian normal subgroup H satisfying the property that G/H is abelian. Then G is abelian.

Solution: FALSE (Consider $G := S_3$ and $H := \langle (1, 2, 3) \rangle \lhd G$ with $G/H \cong \mathbb{Z}_2$).

d. There are no simple groups of order 2022.

Solution: TRUE (If $|G| = 2022 = 2 \cdot 3 \cdot 337$, with 337 prime, then by Sylow’s third theorem there is precisely one Sylow 337-subgroup of G of order 337, which must therefore be normal. Thus G cannot be simple).

e. Suppose that $\varphi : G \to G'$ is an injective homomorphism of groups. Then $G' \cong G/\ker(\varphi)$.

Solution: FALSE (This would be true if φ were surjective instead of injective. For a counterexample consider $G = \{e\}$ and $G' = \mathbb{Z}$, with φ defined by $\varphi(e) = 0$. Then $\ker(\varphi) = \{e\}$ and $G/\ker(\varphi) \cong \{e\} \not\cong G'$).

f. Suppose that R is a commutative ring with a unit, and M is a maximal ideal of R. Then R/M is an integral domain.

Solution: TRUE (A theorem from class shows that R/M is a field, and hence also an integral domain).

g. The polynomial $2x^9 + 6x^2 - 18x + 3$ is irreducible in $\mathbb{Q}[x]$.

Solution: TRUE (Eisenstein’s criterion appiles with $p = 3$, since the lead coefficient is coprime to 3, all other coefficients are divisible by 3, and the constant coefficient is not divisible by 3^2).

h. If R and S are rings with respective units 1_R and 1_S, and $\varphi : R \to S$ is a homomorphism of rings, then $\varphi(1_R) = 1_S$.

Solution: FALSE (Consider $\varphi : R \to S$ defined by $\varphi(r) = 0_S$ for each $r \in S$. This defines a homomorphism of rings).

i. Every ring R with a unit has a commutative subring S with $S \neq \{0\}$.

Solution: TRUE (Consider $S = \langle 1_R \rangle$, which is plainly commutative).

j. There is no field F having 27 elements.

Solution: FALSE (A result from class shows that there is a field of order p^n, for any p prime and $n \in \mathbb{N}$).

Continued...

2. [5+5+5+5+5+5=30 points]

(a) Define what is meant by an *integral domain.*

Solution: An integral domain is a *commutative* ring R such that, whenever $a, b \in R$, then $a = 0$ or $b = 0$.

(b) Suppose that $\varphi : R \to R'$ is a homomorphism of rings. Define what is meant by the *kernel* of φ.

Solution: $\ker(\varphi) = \{x \in R : \varphi(x) = 0_R\}$.

(c) Let I be an ideal of a ring R. Define what it means for I to be a *maximal ideal* of R.

Solution: The ideal I is a maximal ideal of I if (i) one has $\{0_R\} \subsetneq I \subsetneq R$, and (ii) whenever $J \lhd R$ and $I \subseteq J \subseteq R$, then $J = I$ or $J = R$.

(d) Let I be an ideal of a ring R. Define what it means for I to be a *principal ideal* of R.

Solution: The ideal I is a principal ideal of R if $I = (a)$ for some $a \in R$, so that $I = \{ax : x \in R\} = \{xa : x \in R\}$.

(e) Let G be a group. Define what it means for two subgroups H_1 and H_2 of G to be *conjugate* to one another.

Solution: The subgroup H_1 is conjugate to H_2 if $H_1 = g^{-1}H_2g$ for some $g \in G$.

(f) Let G be a group. Define what is meant by a *normal* subgroup of G.

Solution: The subgroup H is a normal subgroup of G if $g^{-1}Hg \subseteq H$ for all $g \in G$.

3. [8+8+9=25 points] (a) Let G be a group. Show that when H is the only subgroup of G having a given order, then H is a normal subgroup of G.

Solution: By the subgroup criterion, the set $g^{-1}Hg = \{g^{-1}hg : h \in H\}$ is a subgroup of G, for when $h_1, h_2 \in H$, we have $(g^{-1}h_1g)(g^{-1}h_2g) = g^{-1}(h_1h_2)g \in g^{-1}Hg$. Moreover, one has $|g^{-1}Hg| = |H|$. Since H is the only subgroup of G having a given order, we must have $g^{-1}Hg = H$. But this relation holds for all $g \in G$, and thus H is a normal subgroup of G.

(b) Suppose that H_1 and H_2 are two distinct subgroups of a group G, with $|H_1| = |H_2| = p$, for some prime number p. Show that $H_1 \cap H_2 = \{e\}$.

Solution: The subgroup H_1 has prime order p, so by Lagrange's theorem any subgroup of H_1 must have order 1 or p. Since $H_1 \cap H_2$ is a subgroup of H_1, we have $|H_1 \cap H_2| = 1$ or p. In the latter case $|H_1 \cap H_2| = |H_1|$, so $H_1 \cap H_2 = H_1$ and so $H_1 = H_2$. But H_1 and H_2 are distinct subgroups of G, so instead we must have $|H_1 \cap H_2| = 1$, whence $H_1 \cap H_2 = \{e\}$.

(c) Let G be a group of order $992 = 32 \cdot 31$. Show that G contains a normal Sylow p-subgroup, for some prime p, and hence cannot be simple.

Solution: Sylow's first theorem shows that G has a Sylow 31-subgroup of order 31 and a Sylow 2-subgroup of order 32. If either subgroup is unique, then part (a) shows the subgroup to be normal and G is not simple. Otherwise, Sylow's third theorem shows that there are $31k + 1$ Sylow 31-subgroups, with k a non-negative integer with $(31k + 1)|992$, whence $k = 1$ and there are 32 Sylow 31-subgroups. Part (b) then shows these subgroups to have trivial pairwise intersection, whence $32 \cdot (31 - 1) = 960$ elements in G have order 31. The remaining $992 - 960 = 32$ elements must belong to the Sylow 2-subgroup of order 32, now seen to be unique. We are therefore in the situation previously discussed, and find that G has a normal Sylow p-subgroup, for $p = 2$ or $p = 31$, and hence is not simple.

Continued...

4. [6+6+6+7=25 points] Consider the polynomials $f(x) = (x+1)^4$, $g(x) = x^2+1$ and $h(x) = x^4+4x^3+6x^2+4x+2$ over $\mathbb{Q}[x]$.

(a) Prove that the polynomials $g(x)$ and $h(x)$ are irreducible in $\mathbb{Q}[x]$.

Solution: By Gauss' Lemma, it suffices to show that g and h are irreducible over $\mathbb{Z}[x]$. But $g(x+1) = (x+1)^2+1 = x^2+2x+2$ is irreducible over $\mathbb{Z}[x]$ as a consequence of Eisenstein's criterion using the prime 2, since this polynomial is monic, all coefficients aside from the leading coefficient are divisible by 2, and the constant coefficient is not divisible by 2^2. Thus, since $g(x+1)$ is irreducible, so too is $g(x)$. Eisenstein's criterion using the prime 2 also applies to show that f is irreducible over $\mathbb{Z}[x]$, for precisely the same reason.

(b) Explain why the ideals $(g(x))$ and $(h(x))$ are maximal in $\mathbb{Q}[x]$, and show that the ideal $(f(x))$ is not maximal in $\mathbb{Q}[x]$.

Solution: Since $\mathbb{Q}$ is a field, it follows that a polynomial $p(x)$ in $\mathbb{Q}[x]$ is irreducible if and only if the ideal $(p(x))$ is maximal. But g and h are irreducible over $\mathbb{Q}[x]$, and thus $(g(x))$ and $(h(x))$ are both maximal ideals. Also, since $f(x) = (x+1)^4 = (x+1)^2 \cdot (x+1)^2$ is not irreducible, it follows that the ideal $(f(x))$ is not a maximal ideal in $\mathbb{Q}[x]$

(c) Explain why the quotient rings $F = \mathbb{Q}[x]/(g(x))$ and $K = \mathbb{Q}[x]/(h(x))$ are fields, and show that the quotient ring $\mathbb{Q}[x]/(f(x))$ is not a field.

Solution: The ring $\mathbb{Q}[x]$ is a commutative ring with a unit, and thus the ideal M of $\mathbb{Q}[x]$ is maximal if and only if $\mathbb{Q}[x]/M$ is a field. Since $(g(x))$ and $(h(x))$ are maximal ideals of $\mathbb{Q}[x]$, it follows that $F = \mathbb{Q}[x]/(g(x))$ and $K = \mathbb{Q}[x]/(h(x))$ are fields. Also, since $(f(x))$ is not a maximal ideal of $\mathbb{Q}[x]$, we see that the quotient ring $\mathbb{Q}[x]/(f(x))$ is not a field.

(d) Let $F = \mathbb{Q}[x]/(x^2+1)$, which is a field (as explained in part (c)), and consider the polynomial $h(t) = t^4+4t^3+6t^2+4t+2$ in $F[t]$. Is the quotient ring $L = F[t]/(h(t))$ a field? Explain your answer.

Solution: Write J for the ideal (x^2+1) of $\mathbb{Q}[x]$, so $F = \mathbb{Q}[x]/J$. Then since $h(t) = (t+1)^4+1$, we see that $((t+1)^2+x+J)((t+1)^2-x+J) = ((t+1)^2+x)((t+1)^2-x)+J = ((t+1)^4-x^2)+J$. Since $(x^2+1)+J = J$, it follows that $((t+1)^4-x^2)+J = ((t+1)^4+1)+J = h(t)+J$, and hence $h(t)$ factors as a product of two quadratic polynomials in $F[t]$. We conclude that $h(t)$ is not irreducible over $F[t]$, and hence $(h(t))$ is not a maximal ideal in $F[t]$, whence $F[t]/(h(t))$ is not a field.

5. [10+10=20 points] Let D be a finite division ring, and suppose that $|D| = n$ with $n \geq 2$.

(a) Let p be any prime divisor of n. Show that $pb = 0$ for all $b \in D$.

Solution: Consider the additive group of D, an abelian group of order n. Since $p|n$, Cauchy's theorem shows that there is an element $a \in D \setminus \{0\}$ of order p, so $pa = 0$. Since $a \neq 0$ and D is a division ring, there exists an element $a^{-1} \in D$ with $aa^{-1} = 1$, and thus for all $b \in D$ one has $pb = p(aa^{-1})b = (pa)(a^{-1}b) = 0(a^{-1}b) = 0$. Hence $pb = 0$ for all $b \in D$.

(b) Prove that there is a prime number p and a natural number m such that $|D| = p^m$.

Solution: Suppose that $|D| = n$ has two distinct prime divisors, say p_1 and p_2. Then for all $b \in D$, it follows from part (a) that $p_1b = 0 = p_2b$. Thus the (additive) order of b divides both p_1 and p_2, and hence is 1, which is to say that $b = 0$ for every $b \in D$. This yields a contradiction, since then $|D| = 1$. We are therefore forced to conclude that n is divisible only by one prime, say p, and hence $|D| = p^m$ for some $m \in \mathbb{N}$.

Continued...

6. [10 points] If I and J are ideals of a ring R, define $I+J$ by $I+J = \{i+j : i \in I \text{ and } j \in J\}$. Prove that $I+J$ is an ideal of R.

   Solution: If $a, b \in I+J$, then $a = i_1 + j_1$ and $b = i_2 + j_2$ for some $i_1, i_2 \in I$ and $j_1, j_2 \in J$. Since I and J are both ideals of R, and hence are additive subgroups of R, we see that $i_1 - i_2 \in I$ and $j_1 - j_2 \in J$, so that $a - b = (i_1 - i_2) + (j_1 - j_2) \in I + J$. Also, we have $0 \in I + J$, so it follows that $I + J$ is an additive subgroup of R by the subgroup criterion. Moreover, given any $a \in I + J$, we have $a = i + j$ for some $i \in I$ and $j \in J$. Since I and J are ideals, it follows that for all $r \in R$ we have $ri \in I$ and $rj \in J$, and hence $ra = r(i + j) = ri + rj \in I + J$. Similarly, we have $ar = (i + j)r = ir + jr \in I + J$. Thus we conclude that $I + J$ is an ideal of R.

7. [8+8+9=25 points] Let R be a commutative ring with a unit. We say that the element $a \in R$ is *nilpotent* if there exists some natural number n, perhaps depending on a, with the property that $a^n = 0$.

   (a) Prove that when a and b are nilpotent, then $a + b$ is also nilpotent.

   Solution: When a and b are nilpotent, there exist $n, m \in \mathbb{N}$ with $a^n = 0$ and $b^m = 0$. Take $k = n + m$. Then (using the commutative property of R), it follows from the binomial theorem that $(a + b)^k = \sum_{r=0}^{k} \binom{k}{r} a^r b^{k-r}$. In each summand on the right hand side, either $r \geq n$ or $k - r \geq m$, and thus $a^r = a^n \cdot a^{r-n} = 0$ or $b^{k-r} = b^m \cdot b^{k-r-m} = 0$. Thus $(a + b)^k$ is a sum of terms, each of which is 0, whence $(a + b)^k = 0$ and $a + b$ is nilpotent.

   (b) Define N to be the set of all nilpotent elements in R. Prove that N is an ideal of R.

   Solution: Adopt the notation of part (a). Then, whenever $b \in N$, we have $b^m = 0$, and hence $(-b)^m = (-1 \cdot b)^m = (-1)^m b^m = 0$, so $-b \in N$. Then it follows from part (a) that $a - b \in N$ whenever $a, b \in N$. Moreover, whenever $r \in R$ and $a \in N$, we have $(ra)^n = r^n a^n = r^n 0 = 0$, so that $ra \in N$. Thus we deduce that N is an ideal of R.

   (c) Prove that the quotient ring R/N is a ring with no non-zero nilpotent elements.

   Solution: The quotient ring R/N is of course a ring, because N is an ideal of R. Suppose that there is a non-zero nilpotent element $u \in R/N$, say $u = v + N$ with $v \in R \setminus N$. Then there is a natural number r satisfying the property that u^r is equal to the zero element in R/N, which is to say that $N = (v + N)^r = v^r + N$, whence $v^r \in N$. Thus v^r is nilpotent, so there exists $s \in \mathbb{N}$ with the property that $0 = (v^r)^s = v^{rs}$. Consequently, the element v is itself nilpotent, whence $v \in N$ and $u = v + N = N$. We conclude that the only nilpotent element in R/N is the zero element N.

8. [8+8+9=25 points] Let G be a finite group, and when $g \in G$, define the map $\sigma_g : G \to G$ by putting $\sigma_g(x) = g^{-1}xg$ for each $x \in G$.

   (a) Show that σ_g is an automorphism of G.

   Solution: We check that σ_g is a homomorphism from G into G by observing that whenever $x, y \in G$, one has $\sigma_g(xy) = g^{-1}xyg = (g^{-1}xg)(g^{-1}yg) = \sigma_g(x)\sigma_g(y)$. Next, using a slightly devious shortcut, we note that $G \lhd G$, and hence $g^{-1}Gg = G$ for all $g \in G$. In particular, since G is finite, we find that $\sigma_g : G \to G$ is a bijective mapping. Then σ_g is a bijective homomorphism from G into G, and hence an automorphism.

Continued...

(b) Show that the set $\operatorname{Inn}(G) = \{\sigma_g : g \in G\}$ is a subgroup of the group $\operatorname{Aut}(G)$ of all automorphisms of G (you may assume here that $\operatorname{Aut}(G)$ is indeed a group without further comment).

Solution: In order to check that $\operatorname{Inn}(G)$ is a subgroup of $\operatorname{Aut}(G)$, we can apply the subgroup criterion. First observe that whenever $g \in G$, one has $\sigma_g(gxg^{-1}) = g^{-1}(gxg^{-1})g = x$ for each $x \in G$, and thus $\sigma_g^{-1} = \sigma_{g^{-1}}$. Next, if $\sigma_g, \sigma_h \in \operatorname{Inn}(G)$, then it follows that $\sigma_g\sigma_h^{-1} = \sigma_g \circ \sigma_h^{-1}$ is defined for each $x \in G$ by $(\sigma_g\sigma_h^{-1})(x) = \sigma_g(\sigma_{h^{-1}}(x)) = \sigma_g(hxh^{-1}) = g^{-1}hxh^{-1}g = (h^{-1}g)^{-1}x(h^{-1}g) = \sigma_{h^{-1}g}(x)$. Thus $\sigma_g\sigma_h^{-1} = \sigma_{h^{-1}g} \in \operatorname{Inn}(G)$, and it follows from the subgroup criterion that $\operatorname{Inn}(G)$ is indeed a subgroup of $\operatorname{Aut}(G)$.

(c) Denote the center of G by $Z(G)$. Use the first homomorphism theorem to show that $G/Z(G) \cong \operatorname{Inn}(G)$.

Solution: Consider the map $\varphi : G \to \operatorname{Inn}(G)$ defined by taking $\varphi(g) = \sigma_{g^{-1}}$. This map is well-defined, and plainly surjective. Moreover, when $g, h \in G$, we have $\varphi(gh) = \sigma_{(gh)^{-1}}$. For each $x \in G$, we have $\sigma_{(gh)^{-1}} = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = g\sigma_{h^{-1}}(x)g^{-1} = \sigma_{g^{-1}}(\sigma_{h^{-1}}(x))$. Thus we see that $\sigma_{(gh)^{-1}} = \sigma_{g^{-1}} \circ \sigma_{h^{-1}}$, and hence $\varphi(gh) = \varphi(g)\varphi(h)$. Then φ is a surjective homomorphism from G into $\operatorname{Inn}(G)$, and it follows from the First Homomorphism theorem that $G/\ker(\varphi) \cong \operatorname{Inn}(G)$. But we have $\ker(\varphi) = \{g \in G : \sigma_{g^{-1}}(x) = x \text{ for all } x \in G\} = \{g \in G : gxg^{-1} = x \text{ for all } x \in G\} = \{g \in G : gx = xg \text{ for all } x \in G\} = Z(G)$. Thus we conclude that $\operatorname{Inn}(G) \cong G/Z(G)$.

End of examination.