GROUPS AND RINGS (MA22017)

SOLUTIONS TO PROBLEM SHEET 7

Section A

1.

(a) Say what it means for a map $\alpha\colon G \times X \to X$ to be an *action* of a group G on a set X. [2]

(b) Show that an action of G on X determines a homomorphism $G \to \mathrm{Sym}(X)$, where $\mathrm{Sym}(X)$ is the group of permutations of X. [2]

(c) Define what it means for an action to be *free*, to be *faithful*, and to be *transitive*. [3]

(d) For each of the conditions in (c), either give an example of an action satisfying the other two but not that one, or show that this is impossible. [3]

Solution:

(a) $\alpha(g_1g_2, x) = \alpha(g_1, \alpha(g_2, x))$ *for all* g_1, $g_2 \in G$ *and* $x \in X$

(b) The map $a\colon G \to \mathrm{Sym}(X)$ *is given by* $a(g)(x) = \alpha(g, x)$. *This is a homorphism because* $a(g_1g_2)(x) = \alpha(g_1g_2, x) = \alpha(g_1, (\alpha(g_2, x)) = a(g_1)(a(g_2)(x))$.

(c) The action is free if only the identity has fixed points, i.e. $a(g)(x) = x$ *for some* $x \in X$ *implies* $g = 1_G$. *It is faithful if* a *is injective. It is transitive if for any* x, $y \in X$ *there exists* $g \in G$ *such that* $\alpha(g, x) = y$.

(d) Faithful and transitive but not free: S_3 *acts on three points by permutation, because* $\alpha = \mathrm{id}$ *and the action is transitive by definition, but* (12) *fixes* 3. *Transitive and free but not faithful: impossible because if* $g \in \operatorname{Ker} a$ *then* $a(g)$ *has fixed points because it is the identity. Free and faithful but not transitive:* S_2 *acts on* $\{1, 2, 3, 4\}$ *by* (12)(34).

2 In this question, R is a commutative ring.

(a) Define what it means for an ideal I in R to be a *prime ideal*. [1]

(b) Define what it means for an ideal I in R to be a *maximal ideal*. [1]

(c) Prove that any maximal ideal is prime. [3]

(d) Define what it means for an ideal to be *finitely generated*. [1]

(e) Suppose that R is Noetherian; that is, every ideal in R is finitely generated. Show that if I_j is an ideals in R, for every $j \in \mathbb{N}$, and $I_j \subseteq I_{j+1}$, then there exists $N \in \mathbb{N}$ such that $I_j = I_N$ for every $j \geq N$. [4]

Solution:

(a) I is prime if $ab \in I$ implies $a \in I$ or $b \in I$.

(b) I is maximal if whenever J is an ideal such that $I \subseteq J \subseteq R$ then $J = I$ or $J = R$.

(c) Suppose I is maximal and $ab \in I$. Suppose $a \notin I$: we aim to show that $b \in I$. We have $\langle a, I\rangle = R$ by maximality, so $1 \in \langle a, I\rangle$, say $1 = ra + c$ with $c \in I$. But then $b = b(ra + c) = rab + bc$ which is in I because $ab \in I$ so $rab \in I$ and $c \in I$ so $bc \in I$.

(d) Consider $I = \bigcup_{j=0}^{\infty}$, which is an ideal. Then $I = \langle a_1, \ldots, a_r\rangle$ for some $a_i \in I$ and $r \in \mathbb{N}$. Because $a_i \in I$ there exists j_i such that $a_i \in I_{j_i}$: take $N = \max j_1, \ldots, j_r$, Then for every i we have $a_i \in I_{j_i} \subseteq I_N$, so if $j \geq N$ then $I \subseteq I_N \subseteq I_j \subseteq I$, so $I_j = I_N = I$.

3 In this question R is a commutative ring.

(a) Define what it means for an R-module M to be *free*. [2]

(b) If M is an R-module and N is a submodule of M, define what it means for N to be *direct summand* of M. [2]

(c) Give, with justification, an example of a module M and a submodule N that is not a direct summand. [2]

(d) State and prove a sufficient condition for N to be a direct summand of a finitely generated R-module M. [2]

(e) Show by giving an example that the condition in (d) is not a necessary condition. [2]

Solution:

(a) M is free if there is a set X and a map $i\colon X \to M$ such that if W is any module and $f\colon X \to W$ is a map then there exists a unique R-linear map $\varphi\colon M \to W$ such that $\varphi i = f$.

(b) N is a direct summand if there exists a submodule $Q \subset M$ such that $M = N \oplus Q$ (that is, $M = N + Q$ and $N \cap Q = 0$).

(c) *$2\mathbb{Z}$ is not a direct summand of $\mathbb{Z}$ because it is of index 2 so Q would have to be of order 2 but $\mathbb{Z}$ has no subgroup of order 2.*

(d) *If M/N is free then N is a direct summand. Choose a basis $X = x_1 + N, \ldots, x_r + N$ for M/N, with $x_i \in M$, and define $f\colon X \to M$ by $f(x_i + N) = x_i$. By (a) this extends to a linear map $\varphi\colon M/N \to M$ with image Q. Then $M = N + Q$ because any element of M is in $(\sum r_i x_i) + N$ for some $r_i \in R$, and $Q \cap N = Im\varphi \cap \mathrm{Ker}(M \to M/N)$ but the composition of those two maps is the identity.*

(e) *$\mathbb{Z}/6 = \mathbb{Z}/2 \oplus \mathbb{Z}/3$ but $\mathbb{Z}/3$ is not free.*

4 Let G be a group, which may be infinite, and let H be a subgroup of G.

(a) Define what is meant by a *left coset* of H in G. [1]

(b) Show that if $g \in G$ then there is a unique left coset of H containing g. [2]

(c) Define what it means for H to be a *normal subgroup* of G. [1]

(d) Show that if $|G : H| = 2$ then H is a normal subgroup of G. Remember that G may be infinite. [2]

(e) By considering the group $G = D_8$ (the symmetries of a square), or otherwise, give an example of a group G with subgroups H_1 and H_2 such that $|G : H_1| = |G : H_2|$ but H_1 is a normal subgroup of G and H_2 is not. [4]

Solution:

(a) *The left coset $gH = \{gh \mid h \in H\}$.*

(b) *$g = g1_G \in gH$, so every g is in a left coset. If $g' \in gH$, say $g' = gh'$, then $g'H = \{gh'h \mid h \in H\} = gH$ since $\{h'h \mid h \in H\} = H$.*

(c) *H is normal if $gH = Hg$ for any $g \in G$.*

(d) *Show that if $|G : H| = 2$ then H is a normal subgroup of G. Remember that G may be infinite.*

(e) *D_8 is generated by $a = (1234)$ and $b = (14)(23)$. Since $aba^{-1} = (1234)(14)(23)(4321) = (14)(23)$ the group $\langle b \rangle$ of order 2 is normal but $ab = (13)$ is also of order 2 and $b(ab)b^{-1} = ba = (24) \neq ab$ so $\langle ab \rangle$ is not normal.*

Section B

5 In this question R is an integral domain.

(a) Define what it means for an element of R to be *prime*, and what it means for an element of R to be *irreducible*. [2]

(b) Show that if $p \in R$ is prime then p is irreducible. [2]

(c) Show that if R is a UFD and $p \in R$ is irreducible then p is prime. [3]

(d) Suppose that R is a UFD, that $f \in R[t]$ is primitive, that $\deg f > 0$, and that $p \in R$ is prime. Put $S = R/pR$. Denote by red_p the quotient map $R[t] \to R[t]/\langle p \rangle = S[t]$. Suppose that $\deg \mathrm{red}_p(f) = \deg f$, and that $\mathrm{red}_p(f) \in S[t]$ is irreducible. Show that f is irreducible. [3]

(e) Suppose that $f \in R[t]$, and that there exists $g \in R[t]$ with $\deg g < \deg f$ such that $f + g^2 = h^2$ for some $h \in R[t]$. Show that f is reducible. [2]

(f) Are the following polynomials in $\mathbb{Z}[t]$ irreducible or not? [8]

(i) $t^3 - 14t^2 + 21t + 24$ *[Use (d)]*

(ii) $t^4 + 3t^2 + 10t - 21$ *[Use (e) with* $g = t - 5$*]*

(iii) $t^4 + 3t^2 + 9t - 21$

(iv) $t^4 + 4t^3 + 11t^2 + 4t + 26$ *[Put* $t = s - 1$*].*

Solution:

(a) *$p \in R$ is prime if it is a nonzero nonunit and $p|ab$ implies $p|a$ or $p|b$, for a, $b \in R$. It is irreducible if $p = rs$ implies r is a unit or s is a unit, for r, $s \in R$.*

(b) *Suppose p is prime and $p = rs$. Then $p|rs$, so $p|r$ or $p|s$: without loss of generality assume that $p|r$, so $r = pr'$. Then $p = pr's$ so as R is a domain $1 = r's$, so s is a unit.*

(c) *Suppose that $p|ab$, say $ab = pc$ and factorise: $a = up_1 \dots p_l$, and $b = vq_1 \dots q_m$, and $c = wr_1 \dots r_n$ with u, v, w units and p_i, q_j, r_k irreducible. Now we have*

$$wpr_1 \dots r_n = uvp_1 \dots p_l q_1 \dots q_m$$

so by uniqueness $p \in \{p_1, \dots, p_l, q_1, \dots, q_m\}$ (up to a unit). So either $p = p_i$ (up to a unit), and then $p|a$, or $p = q_j$ and $p|b$.

(d) *Note that red_p is a ring homomorphism. If f is reducible then $f = gh$ for some nonunits g, $h \in R[t]$; then $\mathrm{red}_p(f) = \mathrm{red}_p(g)\,\mathrm{red}_p(h)$, but $\mathrm{red}_p(f)$ is irreducible so one of the factors, wlog $\mathrm{red}_p(g)$, is a unit in*

$S[t]$. Therefore $\operatorname{red}_p(g) \in S^*$, because S is a domain and so the units of $S[t]$ are the units of S. So $\deg \operatorname{red}_p(g) = 0$. But

$$\deg f = \deg g + \deg h \geq \deg \operatorname{red}_p g + \deg \operatorname{red}_p h = \deg \operatorname{red}_p f = \deg f$$

so $\deg \operatorname{red}_p g = \deg g$ (and $\deg \operatorname{red}_p h = \deg h$). But $\operatorname{red}_p g \in S$ So $\deg \operatorname{red}_p g = 0$ so $\deg g = 0$, i.e. $g = r \in R$. Then r divides the content of f so r is a unit so g is a unit, a contradiction.

(e) We have $f = h^2 - g^2$ so $f = (h+g)(h-g)$ so if f is irreducible we must have $h \pm g$ a unit. Therefore $\deg h = \deg g$, but then $\deg f = \deg(h \mp g) \leq \max(\deg h, \deg g) = \deg g < \deg f$.

(f) (i) If $f = t^3 - 14t^2 + 21t + 24$ then $\operatorname{red}_p f = t^3 + 3$ and $S = \mathbb{F}_7$. But $t^3 + 3 = t^3 - 4$ is irreducible mod 7, because otherwise it would have to have a linear factor, i.e. $\mathbb{F}_7$ would have to have a cube root of 4, and the cubes are $1^3 = 2^2 = 4^3 = 1$ and $3^3 = 5^3 = 6^3 = -1$ which do not include 4.

(ii) If $f = t^4 + 3t^2 + 10t - 21$ and $g = t - 5$ then $f + g^2 = t^4 + 3t^2 + 10t - 21 + t^2 - 10t + 25 = t^4 + 4t^2 + 4 = (t^2+2)^2$ so this is reducible (equal to $(t^2 + 2 + t - 5)(t^2 + 2 - t + 5) = (t^2 + t - 3)(t^2 - t + 7)$).

(iii) $t^4 + 3t^2 + 9t - 21$ is Eisenstein with $p = 3$, hence irreducible.

(iv) If $f(t) = t^4 + 4t^3 + 11t^2 + 4t + 26$ then

$$f(s-1) = (s-1)^4 + 4(s-1)^3 + 11(s-1)^2 + 4s - 4 + 26$$

which is

$$s^4 - 4s^3 + 6s^2 - 4s + 1 + 4(s^3 - 3s^2 + 3s - 1) + 11(s^2 - 2s + 1) + 4s + 22$$

which simplifies to

$$s^4 + (6 - 12 + 11)s^2 + (-4 + 12 - 22 + 4)s + (1 - 4 + 11 + 22)$$

which is $s^4 + 5s^2 - 10s + 30$ which is Eisenstein with $p = 5$ so irreducible.

6 In this question R is a commutative ring and K is a field.

(a) Define what is meant by the dual $M^\vee$ of M. [2]

(b) Show that if V is a finite-dimensional K-vector space then $V^\vee$ is isomorphic to V. [3]

(c) Give, with justification, an example of a ring R and a finitely generated R-module M such that $M^\vee$ is not isomorphic to M. [3]

(d) Let M be any R-module. Exhibit, with justification, a linear map $M \to M^{\vee\vee}$ from M to its double dual, which is injective in the case where $R = K$ and M is a finite-dimensional K-vector space. [3]

(e) Give an example to show that the map in (d) need not be injective in general. [3]

(f) Let X be the $\mathbb{Z}$-module consisting of all finite sequences of integers: that is, $X = \{f\colon \mathbb{Z} \to \mathbb{Z} \mid f(n) = 0 \text{for all but finitely many} n\}$.

(i) By considering the map $f \mapsto \sum_i f(i)$, show that the map $\mathrm{ev}\colon \mathbb{Z} \to X^\vee$ given by $\mathrm{ev}(r)(f) = f(r)$ is not surjective. [4]

(ii) Show that if $a\colon \mathbb{Z} \to \mathbb{Z}$ is a map of sets, there is a map $\hat{a} \in X^\vee$ given by $\hat{a}(\delta_i) = a(i)$, where $\delta_i \in X$ is the sequence with $\delta_i(j) = \delta_{ij}$. Deduce that in fact $X^\vee$ is uncountable, so cannot be isomorphic to X. [5]

Solution:

(a) $M^\vee = \mathrm{Hom}(M, R)$, *the module of* R*-linear maps* $f\colon M \to R$.

(b) Choose a basis $e_1, \ldots, e_n$ *of* V *and consider the map* $d\colon V \to V^\vee$ *given by* $d(e_i)(e_j) = \delta_{ij}$. *This is well-defined (we extend it to the whole of* V *by linearity) and injective since* $d(\sum a_i e_i)(e_j) = a_j$ *so if* $d(\sum a_i e_i) = 0$ *then* $a_i = 0$ *for all* i, *so* $\mathrm{Ker}\, d = 0$. *It is also surjective because if* $f \in V^\vee$ *then* $f = d(\sum f(e_i)e_i)$. *So it is a bijective linear map, hence an isomorphism.*

(c) Take $R = \mathbb{Z}$ *and* $M = \mathbb{Z}/2\mathbb{Z}$. *A linear map* $f\colon M \to \mathbb{Z}$ *must have* $f(1) + f(1) = f(1+1) = f(0) = 0$*: therefore* $f(1) = 0$ *so* f *is the zero map. So* $M^\vee = 0$ *but* $M \neq 0$.

(d) We define $\mathrm{ev}\colon M \to M^{\vee\vee}$ *by* $\mathrm{ev}(m) = \mathrm{ev}_m\colon M \to R$. *That is* $\mathrm{ev}(m)(f) = f(m)$ *for any* $f \in M^\vee$. *This is linear because* $\mathrm{ev}(\lambda m_1 + \mu m_2)(f) = f(\lambda m_1 + \mu m_2) = \lambda f(m_1) + \mu f(m_2) = \lambda\,\mathrm{ev}(m_1)(f) + \mu\,\mathrm{ev}(m_2)(f)$. *In the vector space case, if* $\mathrm{ev}(m) = 0$ *then* $f(m) = \mathrm{ev}(m)(f) = 0$ *for all linear maps* $f\colon V \to K$*: in particular (using (b))* $d(e_i)(m) = 0$ *so if* $m = \sum a_i e_i$ *then* $a_i = 0$ *for all* i *so* $m = 0$.

(e) The example in (c) has $M^\vee = 0$ *so* $M^{\vee\vee} = 0$ *so in fact any map* $M \to M^{\vee\vee}$ *is zero and thus not injective.*

(f) (i) Note that $\sigma\colon f \mapsto \sum_i f(i)$ *is linear:* $\sigma(rf+sg) = \sum_i (rf+sg)(i) = r\sum_i f(i) + s\sum_i g(i) = r\sigma(f) + s\sigma(g)$. *But if* f *is given by* $f(0) = f(1) = 1$ *and* $f(i) = 0$ *otherwise, then for any* $r \in \mathbb{Z}$ *we have* $\mathrm{ev}(r)(f) = 0$ *or* 1, *but* $\sigma(f) = 2$

(ii) All we have to do is check that $\hat{a}$ is linear: in fact it is because $\hat{a} = \sum a_i \operatorname{ev}(i)$ so it is a linear combination of linear maps. Moreover, that also shows that $a \mapsto \hat{a}$ is injective because if $\hat{a} = 0$ then all the a_i are zero. But there are uncountably many maps from $\mathbb{Z}$ to $\mathbb{Z}$ by Cantor's diagonal argument (or just look at the ones that give only 1s and 0s and interpret them as binary expansions).

7 In this question G is a group. Let G' be the group generated by the elements $[a, b] = aba^{-1}b^{-1}$ for a, $b \in G$.

(a) Show that $G' = 1$ if and only if G is abelian. [3]

(b) Show that G' is a normal subgroup of G. Deduce that if G is a non-abelian simple group then $G' = G$. [5]

(c) A group is called *solvable* if the sequence

$$G^{(1)} = G',\ G^{(2)} = (G')' \dots$$

reaches $G^{(r)} = 1$ for some $r \in \mathbb{N}$. Show that the dihedral group D_{2n} is solvable. [6]

(d) Show that if $n > 4$ then the symmetric group S_n is not solvable. You may use the fact that A_n is simple for $n > 4$. [6]

Solution:

(a) If G is abelian then $aba^{-1}b^{-1} = aa^{-1}bb^{-1} = 1$ so $G' = 1$. If $G' = 1$ and a, $b \in G$ then $1 = aba^{-1}b^{-1} = (ab)(ba)^{-1}$ so $ab = ba$.

(b) If $g \in G$ then $g(aba^{-1}b^{-1})g^{-1} \in G'$ because

$$[g, [a, b]] = g(aba^{-1}b^{-1})g^{-1}(aba^{-1}b^{-1})^{-1} = g(aba^{-1}b^{-1})g^{-1}[a, b]^{-1}$$

so $g(aba^{-1}b^{-1})g^{-1} = [g, [a, b]][a, b] \in G'$. If G is a non-abelian group then $G' \neq 1$ by (a) and so $G' = G$ because the only normal subgroups of G are 1 and G.

(c) D_{2n} contains a normal subgroup C_n of index 2: in fact, $D_{2n} = C_n \cup \tau C_n$ where $\tau \in D_{2n}$ is a reflection. So if a, $b \in D_{2n}$ then $a \in \tau^i C_n$ and $b \in \tau^j C_n$ (with i and j being 0 or 1) so $[a, b] \in \tau^{2i+2j} C_n = C_n$. So $D'_{2n} \subseteq C_n$, and C_n is abelian so D'_{2n} is abelian so $D''_{2n} = 1$, so D_{2n} is solvable.

(d) Clearly $[a, b]$ is an even permutation (if a is the product of i transpositions and b is the product of j transpositions then $[a, b]$ is the product of $2i + 2j$ transpositions. So $S'_n < A_n$ but S_n is not abelian so $S'_n \neq 1$. Also $S'_n \lhd S_n$ so $S'_n \lhd A_n$ so $S'_n = A_n$. Now $S''_n = A'_n = A_n$ by (b), so $S_n(r) = A_n$ for all r so S_n is not solvable.

GKS, 3/4/25