GROUPS AND RINGS (MA22017)

SOLUTIONS TO REVISION SHEET

1 Recall (Example III.7(viii)) that any group G acts on itself by conjugation: $a(g,h) = ghg^{-1}$. The orbits are called *conjugacy classes*.

(a) Show that for this action, the map $a_g\colon G \to G$ is in fact a group homomorphism.

(b) Show that any normal subgroup of G is a union of conjugacy classes.

(c) Let $\mathcal{W}$ denote the set of all subgroups of G. Show that G acts on $\mathcal{W}$ by conjugation.

(d) Suppose $H \leq G$, so $H \in \mathcal{W}$. Show that $H \lhd G$ if and only if $\mathrm{Stab}_G(H) = G$ (under the conjugation action of G on W), and more generally that $H \lhd \mathrm{Stab}_G(H)$.

(e) Deduce that $\mathrm{Stab}_G(H) = N_G(H)$, the *normaliser* of H in G, which is by definition the largest subgroup $N < G$ such that $H \lhd N$.

Solution:

(a) $a_g(h_1h_2) = gh_1h_2g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = a_g(h_1h_2)$.

(b) *If $h \in H$ and $h' \in [h]$, the conjugacy class of h, then $h' = ghg^{-1} \in gHg^{-1} = H$ so $[h] \subset H$. So $H = \bigcup_{h\in H}[h]$.*

(c) *We need to show that $gHg^{-1} < G$ if $H < G$. But $gHg^{-1} \neq \varnothing$ because it contains $1 = g1g^{-1}$, and if $a = ghg^{-1}$, $b = gh'g^{-1} \in gHg^{-1}$, then $ab^{-1} = (ghg^{-1})(gh'g^{-1})^{-1} = (ghg^{-1})(gh'^{-1}g^{-1}) = ghh'^{-1}g^{-1} \in gHg^{-1}$. And we also need to show that that this is a group action, i.e. that $a(g_1g_2, H) = a(g_1, a(g_2, H))$, but*

$$a(g_1, a(g_2, H)) = g_1(g_2Hg_2^{-1})g_1^{-1} = (g_1g_2)H(g_1g_2)^{-1} = a(g_1g_2, H).$$

(d) *If $H \lhd G$ then for any $g \in G$ we have $gH = Hg$ so $gHg^{-1} = H$; that is, g stabilises $H \in \mathcal{W}$ under conjugation. So $\mathrm{Stab}_G(H) = G$. Conversely, if $\mathrm{Stab}_G(H) = G$ then $gHg^{-1} = H$ for all g so $gH = Hg$ for all g. More generally, even if $\mathrm{Stab}_G(H) \neq G$, if $g \in \mathrm{Stab}_G(H)$ then $gHg^{-1} = H$ so $gH = Hg$, so $H \lhd \mathrm{Stab}_G(H)$.*

(e) *We need to show that if $K < G$ and $H \lhd K$ then $K \subseteq \mathrm{Stab}_G(H)$, as then any subgroup of G in which H is normal is contained in $\mathrm{Stab}_G(H)$, which is what it means for that to be the biggest such subgroup. But if not, then there exists $k \in K$ such that $kH \neq Hk$; say $kh \notin Hk$ (or $hk \notin kH$, which is similar). But then $khk^{-1} \notin H$ so $kHk^{-1} \neq H$ so H is not a normal subgroup of K.*

2 Compute the following products of permutations:

(a) $(134)(125)(453)$

(b) $(12)(13)(12)$

(c) $(134)^{-1}(12)(34)(134)$

(d) $(134)^{-1}(12)(24)(134)$

Solution:

(a) (12543)

(b) (23)

(c) $(13)(42)$

(d) $(42)(23)$, *or* (234) *which is the same thing.*

3 Show that the dihedral group D_{2n} (the symmetries of an n-gon) is generated by two elements of order 2 by showing the following things:

(a) If $n = 2m - 1$ is odd, then D_{2n} is generated by the rotation $a = (123\ldots n)$ and the reflection $b = (2\ n)(3\ n-1)\ldots(m\ m+1)$; if $n = 2m$ is even then instead $b = (1\ n)(2\ n-1)\ldots(m\ m+1)$.

(b) a has order n and b has order 2.

(c) bab^{-1} also has order n.

(d) $c = ba$ has order 2. Thus D_{2n} is generated by b and c, with relation $b^2 = c^2 = (bc)^n = 1$.

Note about notation: We may write the statement in (d) as

$$D_{2n} = \langle b, c \mid b^2 = c^2 = (bc)^n = 1 \rangle,$$

meaning that D_{2n} is generated by b and c and they satisfy the relations $b^2 =$, $c^2 = 1$ and $(bc)^n = 1$, and no others apart from the ones that follow from those. It is also true that

$$D_{2n} = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1} \rangle.$$

Either of these may be taken as the definition of D_{2n}, if you want a definition purely in terms of elements, not referring to the polygon that D_{2n} acts on.
Solution:

(a) a is the rotation by $2\pi/n$ and b is the reflection in the vertical axis, if we put vertex 1 at the bottom (odd case) or bottom right (even case) and number the vertices anticlockwise.

(b) *Obvious from the description above or from the permutations.*

(c) *In fact* $o(ghg^{-1}) = o(h)$ *in all cases, because* $(ghg^{-1})^r = gh^r g^{-1}$ *which is 1 if and only if* $h^r = 1$.

(d) $bab = bab^{-1}$ *is the opposite rotation: the multiplication gives* $bab = (1\ n\ n-1\ \ldots\ 2)$ *(odd case) or* $bab = (n\ n-1\ \ldots\ 1)$ *(even case) which is* a^{-1} *in both cases, so* $c^2 = baba = (bab)a = a^{-1}a = 1$. *These two generate* D_{2n} *becuse* $bc = bba = a$ *so we recover* a *and* b, *and* $(bc)^n = a^n = 1$.

4 For each of the following polynomials in $\mathbb{Q}[t]$, say whether it is irreducible or not.

(a) $t^5 + 132t^4 - 99t^3 - 143t^2 + 121t + 11$. *[Eisenstein.]*

(b) $t^5 + 132t^4 - 99t^3 - 143t^2 + 121t + 34$. *[Look for a linear factor.]*

(c) $t^4 + 4t^3 - 3t^2 - 14t + 8$. *[Subtract* $(t^2 + 2t - 3)^2$*.]*

Solution:

(a) $t^5 + 132t^4 - 99t^3 - 143t^2 + 121t + 11$ *is Eisenstein with* $p = 11$, *hence irreducible.*

(b) $t^5 + 132t^4 - 99t^3 - 143t^2 + 121t + 34$ *has a factor of* $t + 1$ *since putting* $t = -1$ *gives* $-1 + 132 + 99 - 143 - 121 + 34 = -1 + 11 \times (12 + 9 - 13 - 11 + 3) + 1 = 0$.

(c) $t^4+4t^3-3t^2-14t+8-(t^2+2t-3)^2 = -(t+1)^2$ *so* $t^4+4t^3-3t^2-14t+8 = (t^2 + 2t - 3)^2 - (t + 1)^2$ *which factorises because it is the difference of two squares,* $t^4 + 4t^3 - 3t^2 - 14t + 8 = ((t^2 + 2t - 3) + (t + 1))((t^2 + 2t - 3) - (t + 1))$, *so it is reducible.*

5 What is the characteristic of each of these rings?

(a) $\mathbb{F}_{25}$

(b) $\mathbb{F}_{25}[t]$

(c) $\mathbb{F}_{25}[t]/\langle t^2 \rangle$

(d) $\mathbb{Z}/25\mathbb{Z}$

(e) $R/3R$, where $R = \mathbb{Z}/15\mathbb{Z}$

(f) $\mathbb{Z}[t]/\langle t^5 \rangle$

(g) $\mathrm{Hom}(R, S)$, the set of ring homomorphisms $\varphi\colon R \to S$ where R and S are rings, with addition and multiplication defined by $(\varphi + \psi)(r) = \varphi(r) + \psi(r)$ and $(\varphi\psi)(r) = \varphi(r)\psi(r)$.

Solution: *5, 5, 5, 25, 3, 0, the characteristic of S.*

6 Suppose G is a group and V is a finite-dimensional vector space (over some field K). We say that G acts linearly on V if G acts on V and $g(\lambda v+\mu w) = \lambda g(v) + \mu g(w)$, for all $g \in G$, v, $w \in V$, λ, $\mu \in K$. Recall that if G acts on X then $\alpha(g)$ is the element of $\mathrm{Sym}(X)$ given by $\alpha(g)(x) = g(x)$.

(a) Show that G acts linearly on V if and only if the image of $\alpha\colon G \to \mathrm{Sym}\, V$ is a subgroup of $\mathrm{GL}(V)$. (Remember that $\mathrm{Sym}\, V$ is the group consisting of all bijections from V to V, which may totally disregard the vector space structure: $\mathrm{GL}(V)$ is the group of bijective linear maps from V to V, sometimes called $L(V)$ or $\mathrm{Aut}(V)$.)

(b) Show that if G acts linearly on V then G also acts on the set (called $\mathbb{P}V$) of all lines through the origin in V, To do this, note that to specify $\ell \in \mathbb{P}V$ we only need to specify a non-zero point $v \in \ell$, because then $\ell = \{\lambda v \mid \lambda \in K\}$ and that μv and v determine the same ℓ if $\mu \neq 0$.

(c) If G acts on a set X, then X^G denotes the set of invariants of G: that is, $X^G = \{x \in X \mid \mathrm{Stab}_G(x) = G\}$. Show that if G acts linearly on V then V^G is the set of vectors that are eigenvectors of g with eigenvalue 1 for every $g \in G$.

(d) Show that $\ell = \{\lambda v \mid \lambda \in K\}$ is in $(\mathbb{P}V)^G$ if and only if v is an eigenvector of g for every $g \in G$.

Solution:

(a) If $\alpha(G) \leq \mathrm{GL}(V)$ then $g(\lambda v + \mu w) = \alpha(g)(\lambda v + \mu w)$ by the definition of α, but $\alpha(g)$ is linear so $\alpha(g)(\lambda v + \mu w) = \lambda\alpha(g)v + \mu\alpha(g)(w) = \lambda g(v) + \mu g(w)$ hence irreducible.

(b) If $\ell = \{\lambda v\}$ and $g \in G$ we define the action of G on $\mathbb{P}V$ by putting $g(\ell) = \{\lambda g(v)\}$. We need to check that this gives a well-defined map $G\times\mathbb{P}V \to \mathbb{P}V$, and that $(g_1g_2)\ell = g_1(g_2(\ell))$. The second of these is immediate, because $(g_1g_2)\ell = \{\lambda(g_1g_2)(v)\} = \{\lambda g_1(g_2(v))\} = g_1(g_2(\ell))$. As usual, it well-definedness that needs checking. If $\ell = \{\lambda v\} = \ell\{\lambda w\}$ then $w \in \ell$ so $w = \nu v$ for some $\nu \in K$, so $g(w) = \nu g(v)$, so $g(v)$ and $g(w)$ determine the same line, as required.

(c) $v \in V^G$ if and only if $g(v) = v$ for every $g \in G$, but g is a linear map so that says exactly that $g(v) = 1v$, i.e. v is an eigenvector with eigenvalue 1.

(d) If $\ell \in (\mathbb{P}V)^G$ then $g(\ell) = \ell$. Suppose $\ell = \{\lambda v\}$: then $g(v) \in g(\ell) = \ell$ so $g(v) = \lambda v$ for some λ, so v is an eigenvector for g with eigenvalue λ. Conversely, if for every g there is a λ such that $g(v) = \lambda v$ then $g(\ell) = \ell$ for every $g \in G$, so $\ell \in \mathbb{P}V^G$. (Note that this λ may well

depend on g. each element of g multiplies v by a constant, but it does not have to be the same constant.)

7 Find all abelian groups of order 1400.
Solution: $700 = 2^3 \times 5^2 \times 7$ *so if we write the group as* $\mathbb{Z}/a_1 \times \cdots \times \mathbb{Z}/a_k$ *we must have* $k < 4$, *because* $1400 = a_1 \cdots a_k$ *and* $a_i | a_{i+1}$, *so* $a_i^k | 1400$.
If $k = 1$ *then* $G = \mathbb{Z}/1400$.
If $k = 2$ *then* $a_1^2 | 1400$. *The squares that divide 1400 are 4, 25 and 100, so* $a_1 = 2$, *5 or 10. So the possibilities are* $G = \mathbb{Z}/2 \times \mathbb{Z}/700$, $\mathbb{Z}/5 \times \mathbb{Z}/280$ *and* $\mathbb{Z}/10 \times \mathbb{Z}/140$.
If $k = 3$ *then* $a_1^3 | 1400$ *so* $a_1 = 2$. *Then* $G = \mathbb{Z}/2 \times \mathbb{Z}/a_2 \times \mathbb{Z}/a_3$, *with* a_2 *even,* $a_2 a_3 = 700$ *and* $a_2 | a_3$. *So* $a_2^2 | 700$. *The even squares that divide 700 are 4 and 100, so* $a_2 = 2$ *or 10. So the possibilities are* $G = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/350$ *and* $\mathbb{Z}/2 \times \mathbb{Z}/10 \times \mathbb{Z}/70$.
In this case it was easy to compute the numbers completely, but it would have been all right to write $\mathbb{Z}/2^2 \times 5^2 \times 7$ *instead of* $\mathbb{Z}/700$ *if we had wanted to.*

8

(a) $\mathbb{Z}/2$ and $\mathbb{Z}/4$ are both $\mathbb{Z}$-modules. Compute $\mathbb{Z}/2 \otimes \mathbb{Z}/4$.

(b) There are six $\mathbb{Z}$-modules (abelian groups) G of order 1400: you computed them in Question 7. For each of them, say what $\mathbb{Z}/2 \otimes G$ is. What about $\mathbb{Z}/5 \otimes G$ and $\mathbb{Z}/7 \otimes G$?

(c) Define a map $\mathbb{Z}/2 \times \mathbb{Z}/4 \to \mathbb{Z}/4$ by calling the elements of $\mathbb{Z}/2$ by the names 0_2 and 1_2, and those of $\mathbb{Z}/4$ by $0_4, 1_4, 2_4, 3_4$, and setting $a_2 b_4 = a b_4$, where ab denotes usual integer arithmetic. Does this make $\mathbb{Z}/4$ into a $\mathbb{Z}/2$-module?

Solution:

(a) A bilinear map $\mathbf{f} \colon \mathbb{Z}/2 \times \mathbb{Z}/4 \to M$ *is determined if we know* $\mathbf{f}(1,1)$. *But* $2\mathbf{f}(1,1) = \mathbf{f}(2,1) = \mathbf{f}(0,1) = 0$ *so there is one bilinear map for every element of* $\mathbb{Z}/2$, *that is,* $\mathbb{Z}/2 \otimes \mathbb{Z}/4 = \mathbb{Z}/2$.

(b) Generalising (a), we see that each $\mathbb{Z}/a_i$ *with* a_i *even contributes a* $\mathbb{Z}/2$ *to* $G \otimes \mathbb{Z}/2$, *and similarly for other primes. So in the above, for* $k = 3$ *we get* $(\mathbb{Z}/2)^3$, *for* $k = 2$ *we get* $(\mathbb{Z}/2)^2$ *except in the case of* $\mathbb{Z}/5 \times \mathbb{Z}/280$, *which gives* $\mathbb{Z}/2$, *and for* $k = 1$ *we get* $\mathbb{Z}/2$. *Similarly tensoring with* $\mathbb{Z}/5$ *counts the number of factors for which* $5 | a_i$ *(so* $\mathbb{Z}/5$ *except for* $\mathbb{Z}/2 \times \mathbb{Z}/10 \times \mathbb{Z}/70$, $\mathbb{Z}/5 \times \mathbb{Z}/280$, *and* $\mathbb{Z}/10 \times \mathbb{Z}/140$, *which give* $(\mathbb{Z}/5)^2$. *Tensoring with* $\mathbb{Z}/7$ *always gives* $\mathbb{Z}/7$. *Notice that if you what* $G \otimes \mathbb{Z}/2$ *and* $G \otimes \mathbb{Z}/5$ *are, then you know* G.

GKS, 1/5/26