GROUPS AND RINGS (MA22017)

PROBLEM SHEET 0 WITH SOLUTIONS

The notation $\mathbb{Z}$ means the group of integers where the operation is addition. (Why not multiplication?) $\mathbb{Z}/r$ means the integers mod r: you may have called this $\mathbb{Z}_r$ or $\mathbb{Z}/r\mathbb{Z}$ or C_r, which are common alternatives.

0. Find your notes from the algebra course you did in Semester 1 of your *first* year (this may be the hard part) and read them again, paying special attention to Subsections 1.3 (Prime factorisation), 1.4 (Modular arithmetic) and 2.6 (Permutations), and to Section 3 (Polynomials and unique factorisation).
Solution: *Ring your mum and ask her to have a look at the pile in your bedroom behind those old shoes.*

1. Compute, by hand (or even in your head):

(a) The product of permutations $(125)(26)(4563)(23)$

(b) The highest common factor d of the integers 1547 and 7531.

(c) Integers λ and μ such that $1547\lambda + 7531\mu = d$

(d) Polynomials $q(t)$ and $r(t)$, with rational coefficients, such that

$$39t^4 - 21t^3 + 6t^2 + t - 11 = q(t)(3t^3 + t^2 + 2t - 8) + r(t)$$

and $\deg r < 3$.

Solution:

(a) Start by feeding 1 *in from the right: the first three brackets from the right do nothing to it and the last one takes it to* 2*, so so far we have* $(12\ldots$ *now feed in* 2*, which goes to* 3 *(first bracket) which goes to* 4 *second bracket and stays there, so we have* $(124\ldots$ *and* 4 *goes to* 5 *which goes back to* 1 *so we have* (124)*. Now start again feeding in* 3*, which goes to* 2 *and then* 6*, so that's* $(124)(36\ldots$ *feeding in* 6 *it gets taken back to* 3*, so that's* $(124)(36)$*, and we've finished because* 5 *must stay at* 5 *because it's got nowhere else to go. Indeed, it gets taken to* 6 *and then to* 2 *and then back to* 5 *again if you actually try it.*

(b) 75 *is five 15s so let's try* $5 \times 1547 = 7500 + 5 \times 50 - 5 \times 3 = 7500 + 250 - 15 = 7735$*. That's too big, but never mind: we have* $7531 = 5 \times 1547 - 204$*. Go on to* 204 *and* 1547*: eight copies of* 204 *is going to be close (it's* 1632*, obviously) so we can write* $1547 = 8 \times 204 - 85$*; then* $204 = 2 \times 85 + 34$ *and* $85 = 2 \times 34 + 17$*, and* 17 *divides* 34 *so the next step will give us* 0*, so we've finished:* $d = 17$*.*

(c) *We have* $17 = 85 - 2 \times 34 = 85 - 2 \times (204 - 2 \times 85) = 5 \times 85 - 2 \times 204$*; and then that's* $-2 \times 204 + 5 \times (8 \times 204 - 1547) = 38 \times 204 - 5 \times 1547$*, which is* $38 \times (5 \times 1547 - 7531) - 5 \times 1547$ *which is* $185 \times 1547 - 38 \times 7531$*. So* $\lambda = 185$ *and* $\mu = -38$*.*

(d) *q had better begin $13t \ldots$ to get the $39t^4$ that we need, and then we have a $13t^3$ and we want to have $-21t^t$ so the constant term in q has to be $-34/3$ to make that come out, so $q(t) = 13t - \frac{34}{3}$. Then we just multiply everything out and we get $r(t) = -\frac{62}{3}t^2 - \frac{247}{3}t + \frac{239}{3}$.*

2. Which of the following are groups and which are not? If not, what is wrong?

(a) $\mathbb{N}$ with addition.

(b) $\mathbb{N}$ with multiplication.

(c) $\mathbb{R}^3$ with vector cross product.

(d) $\mathbb{R}^3$ with vector dot product.

(e) For a fixed non-empty set S, the set of functions $f\colon S \to \mathbb{Z}/2$, with addition: that is, we define $(f_1 + f_2)(x) := f_1(x) + f_2(x)$, where the $+$ on the right-hand side is addition in $\mathbb{Z}/2$.

(f) $H \subset S_5$, where $\sigma \in H$ if $\sigma = \rho$ or $\sigma = (45)\rho$ for some $\rho \in S_3$.

(g) For a fixed non-empty set S, the power set of S (the set of all subsets of S) with the operation of symmetric difference: $A \cdot B = (A \cup B) \setminus (A \cap B)$.

Solution:

(a) *Not a group: for example, 1 has no inverse.*

(b) *Not a group (regardless of whether you think $0 \in \mathbb{N}$): for example, 2 has no inverse.*

(c) *Not a group for many reasons, but the simplest is that vector cross product is not associative.*

(d) *This isn't even a binary operation. The output of dot product isn't in $\mathbb{R}^3$ at all.*

(e) *Yes: the identity is the constant function 0 and all the axioms hold because they hold in $\mathbb{Z}/2$.*

(f) *Yes. You can check this by hand: writing* $\tau = (45)$ *we have*

$$(\tau\rho_1)(\tau\rho_2)^{-1} = \tau\rho_1\rho_2\tau = \rho_1\rho_2$$

and similarly for the other cases. But you can also say that it is the symmetries of three red balls and two blue ones. Or, actually, it is the stabiliser of τ *under conjugation, but you aren't supposed to be ready for that yet.*

(g) *Yes. You can check it by hand but a much better way is to look at the indicator functions and notice that it's the same group as in part (e). Boolean* $+$ *is* `XOR`*!*

3. Here is a list of maps between groups. Say which ones are group homomorphisms. Don't guess: try to find a proof.

(a) $\phi\colon \mathbb{Z} \to \mathbb{Z}$ given by $\phi(x) = 0$.

(b) $\phi\colon \mathbb{Z} \to \mathbb{Z}$ given by $\phi(x) = 1$.

(c) $\phi\colon \mathbb{Z} \to \mathbb{Z}$ given by $\phi(x) = -x$.

(d) $\phi\colon \mathbb{Z} \to \mathbb{Z}$ given by $\phi(x) = x^2$.

(e) $\varepsilon\colon S_n \to \mathbb{Z}/2$, where ε is the sign of σ, i.e. 0 if σ is an even permutation and 1 if it is odd.

(f) $\eta\colon S_n \to \mathbb{Z}/2$ where $\eta(\sigma) = 0$ if σ is the product of an even number of disjoint cycles (possibly of length 1, i.e. fixed points) and 1 if that number is odd.

Solution:

(a) *Yes.* $\phi(0) = 0$ *and* $\phi(-a) = 0 = -0 = -\phi(a)$ *and* $\phi(a+b) = 0 = 0 + 0 = \phi(a) + \phi(b)$.

(b) *No.* $\phi(0) = 1 \neq 0$.

(c) *Yes.* $\phi(0) = -0 = 0$ *and* $\phi(-a) = a = -(-a) = -\phi(a)$ *and* $\phi(a+b) = -(a+b) = (-a) + (-b) = \phi(a) + \phi(b)$

(d) *No.* $\phi(-1) = 1$ *but* $-\phi(1) = -1$.

(e) *Yes. If* σ_1 *is even and* σ_2 *is even then so is* $\sigma_1\sigma_2^{-1}$*, and the same for the other cases.*

(f) *Yes if and only if* n *is even. If* n *is odd it fails immediately because* $\eta(1) = 1$ *whereas it should be* 0*. If* n *is even, suppose* σ *has* a *odd cycles and* b *even cycles. Then* a *must be even because* $a \equiv n \bmod 2$*. So* $\eta(\sigma) = b \bmod 2$*, but the signature of* σ *is also* $b \bmod 2$ *because odd cycles are even permutations, so in this case* $\eta = \varepsilon$*.*

GKS, 4/2/25