GROUPS AND RINGS (MA22017)

SOLUTIONS TO PROBLEM SHEET 3

1 W Consider the map $\varphi\colon \mathbb{R} \to \mathbb{C}^*$ given by $\varphi(x) = e^{2\pi i x}$. (Remember what the group operations on $\mathbb{R}$ and $\mathbb{C}^*$ are.) Verify that φ is a group homomorphism. What is its kernel? Describe the three maps π, $\bar\varphi$ and ι from the factorisation in Corollary II.26.

Solution: *$\varphi(x+y) = e^{2\pi i(x+y)} = e^{2\pi i x}e^{2\pi i y}$ so φ is a homomorphism. The kernel is $\mathbb{Z}$ so π sends x to $x+\mathbb{Z}$, which is effectively its fractional part, $\bar\varphi$ sends $t \in [0,1)$ to $e^{2\pi i t}$ or just sends x to $e^{2\pi i x}$, and ι sends $z \in S^1 = \{z \mid |z| = 1\}$ to $z \in \mathbb{C}^*$.*

2 H,E In each of the following cases say what the kernel and image of the group homomorphism φ are and describe π, $\bar\varphi$ and ι briefly.

(a) **H** $\varphi\colon S_n \to \mathbb{Z}/2$ where $\varphi(\sigma)$ is the signature of σ.

(b) **E** Suppose p is a prime number, and remember the notation $\mathbb{F}_p$, which is $\mathbb{Z}/p$ but as a filed, i.e. with multiplication mod p as well as addition mod p. Take $\varphi\colon \mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{Z}/p)$ to be the reduction mod p map: that is, $\varphi(M)$ is M mod p. *[The hard part is to determine the image of φ: you may want to use the Chinese Remainder Theorem.]*

Solution:

(a) The kernel is A_n and the image is $\mathbb{Z}/2$ since both odd and even permutations exist. In this case the factorisation is almost trivial: π sends σ to σA_n, then $\bar\varphi$ writes down the signature of σ and ι either does nothing (if your possible signatures are 0 and 1) or sends -1 to 1 and 1 to 0, depending on whether you prefer to write signatures additively or multiplicatively.

(b) This is harder than it looks. The kernel is what is called $\Gamma(p)$ ("the principal congruence subgroup of level p"), given by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(p)$ if and only if p divides all of $a-1$, $d-1$, b and c. The hard part is that the image is $\mathrm{SL}(2,\mathbb{F}_p)$: in other words, if $N = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2,\mathbb{F}_p)$ then there exists $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ such that $\varphi(M) = N$. It is not enough to take a, b, c, d to be arbitrary integers that are α, β, γ, δ mod p because all we then know is that $ad - bc \equiv 1$ mod p: we want it to be actually 1. Suppose that $ad - bc = kp + 1$. Then $(a+\lambda p)d - (b-\mu p)c = (k + (\lambda d + \mu c))p + 1$, and $M' = \begin{pmatrix} a+\lambda p & b-\mu p \\ c & d \end{pmatrix}$

also satisfies $\varphi(M') = N$, for any λ, $\mu \in \mathbb{Z}$. So if we can choose λ and μ so that $\lambda c + \mu d = -k$, we are done. We can do that if $\operatorname{hcf}(c, d) = 1$, but that is not necessarily the case. However, we still have the freedom to add multiples of p to c and d. Moreover, c and d are not both divisible by p (because otherwise $\det N = 0$). Suppose that c is not divisible by p. Then the Chinese Remainder Theorem allows us to solve $\nu p + c \equiv 1 \bmod d$ (we are finding amn integer that is c mod p and 1 mod d), and then $\operatorname{hcf}(\nu p + c, d) = 1$. So we replace c with $\nu p + c$, which does not change N, and then replace a and b with $a + \lambda p$ and $b - \mu p$. If $p|c$ then we just interchange the roles of c and d.

After that, π is reduction modulo $\Gamma(p)$, $\bar{\varphi}$ takes $M\Gamma(p)$ to N, and ι is the identity.

3 W In I.40 we mentioned "the smallest subgroup that contains S" (a subset of G) as another way to describing $\langle S \rangle$. Let G be a group, suppose $S \subset G$ and let H be the intersection of all (not necessarily proper) subgroups of G that contain S. Show that H is a subgroup, and that any subgroup that contains S also contains H. Deduce that $H = \langle S \rangle$.

Solution: *In general, intersections of subgroups are subgroups, because if $H = \bigcap_{\alpha \in A} H_\alpha$ and h_1, $h_2 \in H$ then $h_i \in H_\alpha$ for all α, so $h_1 h_2^{-1} \in H_\alpha$ for all α, so $h_1 h_2^{-1} \in H$. Since clearly $1 \in H$ we also have $H \neq \varnothing$, so H is a subgroup.*
According to I.41, $\langle S \rangle = \{s_1 \ldots s_k \mid s_i \text{ or } s_i^{-1} \in S \text{ for all } i\}$. It is a subgroup (again see I.41) and it contains S, so $\langle S \rangle \supseteq H$. On the other hand, any subgroup containing S has to contain $s_1 \ldots s_k$, so $\langle S \rangle$ is contained in any subgroup containing S, in particular $\langle S \rangle \subseteq H$.

4 W,E

(a) **W** Let G be a group and suppose $S \subseteq G$ is a subset. Is there a smallest normal subgroup of G that contains S? If so, can you describe what the elements look like?

(b) **E** If $H < G$, define the normaliser $N_G(H)$ to be the largest subgroup of G such that H is normal in $N_G(H)$. Make this definition precise, and show that $N_G(H)$ is a subgroup of G. Is $N_G(H)$ a normal subgroup of G?

Solution:

(a) Yes, this exists: we can construct it as we constructed H in Q3, replacing "subgroup" by "normal subgroup". The elements are all conjugates of elements of S or their inverses, and products of those: that is, things of the form $s_1 \ldots s_k$ where for each s_i there is a $g_i \in G$ such that $g_i s_i g_i^{-1} \in S$ or else $g_i s_i^{-1} g_i^{-1} \in S$.

(b) *This also exists: it is the group generated by the union of all subgroups G' of G such that $H \lhd G$. This is a non-empty union because H is such a subgroup. It is a group by definition: in this case, in fact, the union is already a group, because one of the groups G' is in fact $N_G(H)$. But it is not normal itself in general: if we take H to be the subgroup of S_3 generated by (12), which is not normal, then the only subgroup that strictly contains H is the group $G = S_3$. So the only subgroup G' in which H is normal is H itself, so $N_G(H) = H$ which is not a normal subgroup.*

5 E Prove the assertions in III.17(v) in the notes: that in the action of $\mathrm{SL}(2,\mathbb{Z})$ on the upper half-plane $\mathbb{H} = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}$, the stabiliser of most $z \in \mathbb{H}$ is $\pm I$, but the stabiliser of $i \in \mathbb{H}$ is a group of order 4 generated by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and the stabiliser of $\omega = e^{2\pi i/3}$ is of order 6, generated by $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.

Solution: *It is important to show both inclusions. Clearly* $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}(i) = \frac{1}{-i} = i$ *and since* $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ *we have* $1 + \omega = \frac{1}{2} + i\frac{\sqrt{3}}{2} = e^{\pi i/3}$*. Thus* $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}(\omega) = \frac{-1}{1+\omega} = -e^{-\pi i/3} = e^{\pi i - \pi i/3} = e^{2\pi i/3} = \omega$*. But we also need to show that there is nothing else.*
If $\frac{ai+b}{ci+d} = i$ *then* $ai + b = -c + di$ *so* $d = a$ *and* $b = -c$ *so the only elements that stabilise* i *are* $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ *with* $a^2 + b^2 = 1$*, and the only way to satisfy* $a^2 + b^2 = 1$ *in integers is* $a = 0$ *and* $b = \pm 1$ *or* $b = 0$ *and* $a = \pm 1$*, as required.*
Similarly, if $\frac{a\omega+b}{c\omega+d} = \omega$ *then* $a\omega + b = c\omega^2 + d\omega$*. They will now probably use* $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ *again, which is fine, but I prefer* $\omega^2 = -1 - \omega$ *so* $a\omega + b = -c - c\omega + d\omega$ *which (since 1 and* ω *are linearly independent over* $\mathbb{Q}$*) gives* $b = -c$ *and* $a + c = d$*. The determinant is 1 so* $ad + c^2 = 1$ *so* $a^2 + ac + c^2 = 1$*. Let's try to find solutions, treating it as a quadratic in* a*. There are real solutions only if the discriminant* $c^2 - 4(c^2 - 1)$ *is non-negative, so we must have* $4 \geq 3c^2$ *so* $c = \pm 1$ *or* $c = 0$*, and similarly for* a*. Of these, only* $(a, c) = (\pm 1, 0)$*,* $(a, c) = (0, \pm 1)$ *and* $(a, c) = (\pm 1, \mp 1)$ *actually give solutions, and those give the six matrices required.*

6 H Prove the assertion in the proof of Proposition III.18, that left multiplication by G on $X = \{gH \mid g \in G\}$ defines a group action and that the stabiliser of $1_G H$ is H.

Solution: *We need to check that if* $g_1,\ g_2 \in G$ *and* $gH \in X$ *then* $g_1(g_2 gH) = (g_1 g_2)gH$*, and that* $1(gH) = gH$*, according to Definition III.2. But the first two are both equal to* $g_1 g_2 gH$ *and the second is trivial. For the stabiliser,* *this is the statement that $gH = H$ if and only if $g \in H$, which is a case of Corollary II.6.*

GKS, 19/2/25