ALGEBRA 2B (MA20217)

PROBLEM SHEET 3 WITH SOLUTIONS

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

(b) $G = \mathrm{SL}(2,\mathbb{Z})$ and $\varphi(M)$ is M mod p for some prime 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 more 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 $\mathrm{hcf}(c,d)=1$, 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 $\nu p+c\equiv 1 \mod d$ (we are finding amn integer that is $c \mod p$ and $1 \mod d$), and then $\mathrm{hcf}(\nu p+c,d)=1$. 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 $h_1h_2^{-1}\in H_\alpha$ for all α, so $h_1h_2^{-1}\in H$. Since clearly $1\in H$ we also have $H\neq\varnothing$, so H is a subgroup.*
According to I.41, $\langle S\rangle=\{s_1\dots s_k\mid s_i \text{ or } s_i^{-1}\in S \text{ for all } i\}$. 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 $s_1\dots s_k$, so $\langle S\rangle$ is contained in any subgroup containing S, in particular $\langle S\rangle\subseteq H$.

4 H

(a) 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) 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 $s_1\dots s_k$ where for each s_i there is a $g_i\in G$ such that $g_is_ig_i^{-1}\in S$ or else $g_is_i^{-1}g_i^{-1}\in S$.

(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.*

GKS, 1/3/24