6111 Homework 1

September 5, 2017

Problem 1. (5) Let G be a group and H_1, H_2 two subgroups of G of finite index. Prove that $[G : H_1 \cap H_2] < \infty$ i.e. $H_1 \cap H_2$ is of finite index as well.

Proof. Let $X = \{a(H_1 \cap H_2) : a \in G\}$ be the set of left cosets of $H_1 \cap H_2$ and let $Y = \{(g_1H_1) \cap (g_2H_2) : g_1, g_2 \in G\}$ be the set of intersections of a left coset of H_1 with a left coset of H_2. We want to show that X is finite, since $H_1 \cap H_2$ finite index means there are only finitely many left cosets. We know that Y is a finite set, since H_1, H_2 finite index means that H_1 and H_2 both have finitely many left cosets, so the set of intersections is also finite. If we can find an injection $\phi : X \to Y$, then we know the cardinality of X is less than the cardinality of Y which implies X is finite. To construct such an injection, first note that for any coset $a(H_1 \cap H_2)$, we see that $a(H_1 \cap H_2) \subset aH_1$ and $a(H_1 \cap H_2) \subset aH_2$, and so $a(H_1 \cap H_2) \subset (aH_1) \cap (aH_2)$. Thus we have a map $\phi : X \to Y$ defined by $\phi(a(H_1 \cap H_2)) = (aH_1) \cap (aH_2)$. We see this map is well defined as if $a(H_1 \cap H_2) = b(H_1 \cap H_2)$, then $b^{-1}a \in H_1 \cap H_2$ and so $aH_1 = bH_1$ and $aH_2 = bH_2$. Next to show injectivity, if $\phi(a(H_1 \cap H_2)) = \phi(b(H_1 \cap H_2))$, then $(aH_1) \cap (aH_2) = (bH_1) \cap (bH_2)$. Thus, $\big((aH_1) \cap (aH_2)\big) \cap \big((bH_1) \cap (bH_2)\big) = \big(aH_1 \cap bH_1\big) \cap \big(aH_2 \cap bH_2\big)$ is nonempty, and so since the cosets of H_1 and H_2 are disjoint this implies $aH_1 = bH_1$, $aH_2 = bH_2$. Therefore, $a^{-1}b \in H_1$ and $a^{-1}b \in H_2$. Thus $a^{-1}b \in H_1 \cap H_2$ and so $a(H_1 \cap H_2) = b(H_1 \cap H_2)$. Thus $\phi(a(H_1 \cap H_2)) = \phi(b(H_1 \cap H_2))$ implies $a(H_1 \cap H_2) = b(H_1 \cap H_2)$ and so ϕ is injective. Therefore since Y is finite and there is an injection from X to Y this implies that X is finite. So we conclude $H_1 \cap H_2$ is of finite index. □

Problem 2. (9) Let m, n be two positive integers. What is the cardinality of $Hom(\mathbb{Z}_m, \mathbb{Z}_n)$:= the set of all group homomorphisms from $\mathbb{Z}_m$ to $\mathbb{Z}_n$.

Proof. We will show $|Hom(\mathbb{Z}_m, \mathbb{Z}_n)| = gcd(m, n)$.

First note that any homomorphism ϕ on a cyclic group $\langle g \rangle$ is determined by $\phi(g)$. This is because $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ and $\phi(g^k) = \phi(g)^k$ for all $k \in \mathbb{Z}$, and so if two homomorphism ϕ_1, ϕ_2 agree on g, then for all $k \in \mathbb{Z}$, $\phi_1(g^k) = \phi_1(g)^k = \phi_2(g)^k = \phi_2(g^k)$ and so $\phi_1 = \phi_2$ on all of $\langle g \rangle$. Now we know $\mathbb{Z}_m$ is a cyclic group, so let $g \in \mathbb{Z}_m$ be a fixed generator of $\mathbb{Z}_m$ and thus any homomorphism $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$ is determined by $\phi(g)$. Therefore if we let $\psi : Hom(\mathbb{Z}_m, \mathbb{Z}_n) \to \mathbb{Z}_n$ be the map $\psi(\phi) = \phi(g)$, then we see by above that ψ is injective. So to count the homomorphisms it is equivalent to count the number of elements of $\mathbb{Z}_n$ which a generator can be mapped to.

Claim: The set $\{\phi(g) : \phi \in Hom(\mathbb{Z}_m, \mathbb{Z}_n)\}$ is precisely the set of elements of $\mathbb{Z}_n$ with order dividing m.

Proof of claim: First if $h \in \mathbb{Z}_n$ and $h = \phi(g)$ for some $\phi \in Hom(\mathbb{Z}_m, \mathbb{Z}_n)$, then $h^m = \phi(g)^m = \phi(g^m) = \phi(e) = e$, and so $h^m = e$. Therefore the order of h divides m. (Let k be the order of h. If k does not divide m, then let l be the largest integer such that $kl < m$, and so $m \in \{kl+1, ..., kl+(k-1)\}$, but $h^{kl+j} = h^j \neq e$ for all $1 \leq j \leq k-1$, and so $h^m \neq e$. So by contrapositive if $h^m = e$ then the order of h divides m.) Conversely assume the order of h divides m and define the map $\phi_h(g^k) = h^k$ for all $k \in \mathbb{Z}$. First note that ϕ_h is well defined, since if $g^k = g^l$, then $g^{k-l} = e$ and so m divides $(k-l)$. Thus, $\phi_h(g^{k-l}) = h^{k-l} = e$, since $h^m = e$.

Thus $\phi_h(g^k) = \phi_h(g^l)$. Next note that ϕ_h is a homomorphism since $\phi_h(g^k g^l) = h^{k+l} = h^k h^l = \phi_h(g^k)\phi_h(g^l)$. Thus we have proven the claim and all that remains is to count the number of elements of $\mathbb{Z}_n$ which have order dividing m.

An element l having order dividing m means that $l^m = 0$ in $\mathbb{Z}_n$, equivalently $ml \equiv 0 \pmod{n}$. This is equivalent to $l\frac{m}{n} \in \mathbb{Z}$. Now we want to count all $l \in \{1, ..., n\}$ such that $l\frac{m}{n} \in \mathbb{Z}$. Let $gcd(m, n)$ be the greatest common divisor of m and n, and so we know that there exists $c_m, c_n \in \mathbb{N}$ with c_m, c_n relatively prime such that $m = gcd(m, n)c_m$ and $n = gcd(m, n)c_n$. Thus, $\frac{m}{n} = \frac{c_m}{c_n}$. Now since c_m, c_n are relatively prime, we see that for any integer l, $l\frac{c_m}{c_n} \in \mathbb{Z}$ if and only if $l = sc_n$ for some $s \in \mathbb{Z}$ (this is easy to see by looking at the prime factorizations). So The set of l which we want to count is precisely the set $\{sc_n : 1 \leq sc_n \leq n, s \in \mathbb{N}\}$. It is immediate that this set is indexed by the set $\{s : 1 \leq s \leq n/c_n, s \in \mathbb{N}\}$ which is of size $n/c_n = gcd(m, n)$. Thus we see that there are $gcd(m, n)$ many elements of $\mathbb{Z}_n$ which are the image of the generator g under some homomorphism, and those elements are precisely $\{1c_n, 2c_n, ..., gcd(m, n)c_n\}$. Therefore by the previous argument, this set is the same size as the set of homomorphisms, and so we see that $|Hom(\mathbb{Z}_m, \mathbb{Z}_n)| = gcd(m, n)$. ☐

Problem 3. (11) Let G be a group and consider the following subset of G:

$$X = \{aba^{-1}b^{-1} : a, b \in G\}$$

Let $H = \langle X \rangle$ the subgroup generated by X. Show that:
(i) H is normal
(ii) G/H is abelian

Proof. We will show a stronger result. Let H be any subgroup containing X (and so clearly the subgroup generated by X is one such subgroup). For any $g \in G$ and $h \in H$, we see that $ghg^{-1}h^{-1} \in X \subset H$, and so $ghg^{-1} = (ghg^{-1}h^{-1})h \in H$. Thus, $gHg^{-1} \subset H$ and so H is normal. Let $aH, bH \in G/H$. We want to show $(ab)H = (ba)H$, so equivalently we want to show $(ba)^{-1}ab \in H$. However, $(ba)^{-1}ab = a^{-1}b^{-1}ab \in X \subset H$. Thus, $(aH)(bH) = (bH)(aH)$ and since these are arbitrary cosets, we conclude that G/H is abelian. ☐

Problem 4. Let $M(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$. Let $G = \{M(\theta) : 0 \leq \theta \leq 2\pi\} \subset GL_2(\mathbb{C})$ and let $X = \mathbb{R}^2 \setminus 0$. Consider the group action of G on X. Determine whether the action is free, faithful, or transitive and describe the orbit space $G \setminus X$.

Proof. We will show that the action of G on X is faithful, free, and not transitive.

Let $\| \cdot \|$ be the standard euclidean norm on $\mathbb{R}_2$, and let $x = (x_1, x_2) \in \mathbb{R}^2$. We see that

$$\begin{aligned} \|M(\theta)x\|^2 &= (\cos(\theta)x_1 - \sin(\theta)x_2)^2 + (\sin(\theta)x_1 + \cos(\theta)x_2)^2 \\ &= \cos^2(\theta)x_1^2 + \sin^2(\theta)x_2^2 - 2\cos(\theta)\sin(\theta)x_1x_2 + \sin^2(\theta)x_1^2 + \cos^2(\theta)x_2^2 + 2\sin(\theta)\cos(\theta)x_1x_2 \\ &= \cos^2(\theta)(x_1^2 + x_2^2) + \sin^2(\theta)(x_2^2 + x_1^2) = x_1^2 + x_2^2 = \|x\|^2 \end{aligned}$$

Thus we see that $\|M(\theta)\| = 1$ for all θ (where this is the operator norm). Moreover we see from above that for any $x \in \mathbb{R}^2 \setminus 0$, $\|M(\theta)x\| = \|x\|$, which implies that the G orbit of x is a collection of vectors with the same norm as x. That is, $Gx \subset \{y \in \mathbb{R}^2 : \|y\| = \|x\|\}$. This implies there is more than one G orbit in X (since each orbit is a proper subset of X and the union of the orbits equals X), and thus G does not act transitively on X.

Now we will show that the action is free. Note that for any θ, the characteristic polynomial for $M(\theta)$ is $det(M(\theta) - Ix) = (\cos(\theta) - x)^2 + \sin^2(\theta) = x^2 - 2x\cos(\theta) + 1$ (where I is the identity matrix). We know by the fundamental theorem of algebra that $x^2 - 2x\cos(\theta) + 1 = (x - \lambda_1)(x - \lambda_2)$ for some $\lambda_1, \lambda_2 \in \mathbb{C}$, and since $\lambda_1\lambda_2 = 1$, we see that the two eigenvalues of $M(\theta)$ are multiplicative inverses. Therefore, if $M(\theta)x = x$ for some $x \in X$, then 1 is an eigenvalue of $M(\theta)$ and so by above we see that 1 is an eigenvalue of multiplicity two. Thus, $x^2 - 2x\cos(\theta) + 1 = (x-1)^2 = x - 2x + 1$, which implies $\cos(\theta) = 1$. Therefore, $\sin(\theta) = 0$, and so we see that $M(\theta) = I$. Thus if $M(\theta)$ fixes any element of X, then $M(\theta)$ is the identity. So we see that the action of G on X is free.

Free implies faithful, and so we have shown that the action is free, faithful, and not transitive.

We showed before that every orbit of G lie within a concentric circle. Next we will show that the orbits of G are exactly the concentric circles in $\mathbb{R}^2$. Let $C_r = \{x \in \mathbb{R}^2 : \|x\| = r\}$. By before we see that for all $\|x\| = r$, $Gx \subset C_r$. Now, let $x_r = (r, 0)$. For any $y = (y_1, y_2) \in C_r$, we see that there exists θ such that $y_1 = r\cos(\theta)$, $y_2 = r\sin(\theta)$. To justify this we see first that $y_1^2 + y_2^2 = r^2$, and so $0 \leq y_1/r, y_2/r \leq 1$. Thus since the image of cos is $[0, 1]$ we see that $y_1/r = \cos(\theta)$ for some θ. Since $\cos(\theta)^2 + \sin(\theta)^2 = 1$, this implies that $(y_2/r)^2 = \sin(\theta)^2$, and so $y_2/r = \pm\sin(\theta) = \sin(\pm\theta)$. Finally since $\cos(\theta) = \cos(-\theta)$, we conclude that $y = (r\cos(\theta), r\sin(\theta))$ for some θ. However, we see that $M(\theta)x_r = (r\cos(\theta), r\sin(\theta))$. Thus, $y = M(\theta)x_r$ and so $y \in Gx_r$. Therefore since $y \in C_r$ is arbitrary, we conclude that $C_r \subset Gx_r \subset C_r$ and therefore $Gx = C_r$ for all x with $\|x\| = r$. Thus, $G \setminus X = \{C_r : r \in \mathbb{R}^+\}$. □

Problem 5. Assume G is a group and H is a subgroup such that $[G : H] < \infty$. Prove that there exists a normal subgroup N of G such that $[G : N] < \infty$ and $N \subset H$.

Proof. We see that G acts on G/H by left multiplication, that is $g_1 \cdot (gH) = (g_1 g)H$. This group action is a homomorphism $\varphi : G \to Sym(G/H)$, and so the kernel $ker(\varphi)$ is a normal subgroup of G. Additionally, by the first isomorphism theorem, $G/ker(\varphi) \cong im(\varphi)$ and $im(\varphi) \leq Sym(G/H)$ a finite group, and so $|G/ker(\varphi)| < \infty$. Thus we see that $[G : ker(\varphi)] < \infty$. So $ker(\varphi)$ is a normal subgroup of finite index, so all that remains is to see that $ker(\varphi) \subset H$. Let $g \in ker(\varphi)$. Therefore for any coset $g_1 H$, $g g_1 H = g_1 H$. Looking at the coset H, we see $gH = H$ which implies that $g \in H$. Since $g \in ker(\varphi)$ is arbitrary we conclude $ker(\varphi) \subset H$. Thus we found a normal subgroup of finite index inside of H and so we are done. □