# Homework 5

1. Let $m \geq 2$ and set $\mathbb{Z}_m^* := \{k \in \mathbb{Z}_m : \gcd(k, m) = 1\}$.

   a. First we show that every element of $\mathbb{Z}_m^*$ generates $\mathbb{Z}_m$. We want to show there are $m$ distinct cosets in the cyclic subgroup generated by $k$. Let $n$ be the smallest positive integer such that $nk + m\mathbb{Z} = m\mathbb{Z}$. Then $nk$ is the least common multiple of $k$ and $m$. But since $\gcd(k, m) = 1$, we must have $nk = mk$ and $n = m$. Then $k$ generates $\mathbb{Z}_m$.

      Now take some element $l$ such that $\gcd(l, m) > 1$. Then there is some $r$ such that $m = nr$ and $l = pr$. Then $nl$ is a multiple of both $l$ and $m$, and $n < m$. Then $n$ is the order of $l$, and $l$ does not generate $\mathbb{Z}_m$.

   b. We will show $\mathbb{Z}_m^*$ is a group under multiplication. Clearly it contains the identity 1 since $\gcd(1, m) = 1$. To show inverses, let $n \in \mathbb{Z}_m^*$. Then by applying the euclidean algorithm, there are integers $a$ and $b$ such that $an + bm = 1$ and thus $an = 1 - bm$. Then we have $an + m\mathbb{Z} = 1 + m\mathbb{Z}$, and inverse of $a$ is $n$ in $\mathbb{Z}_m^*$.

      Finally suppose $a, b \in \mathbb{Z}_m^*$. If $p$ is a prime which divides $m$ and $ab$, then $p$ must divide either $a$ or $b$. But this is impossible. Then $ab \in \mathbb{Z}_m^*$.

   c. Suppose $\gcd(a, m) = 1$. Then any element of $a + m\mathbb{Z}$ is also relatively prime with $m$, and thus $a + m\mathbb{Z}$ generates $\mathbb{Z}_m^*$. Then the cyclic group generated by $a + m\mathbb{Z}$ under multiplication must be at most order $m$, and thus $(a+m\mathbb{Z})^{\varphi(m)} = 1+m\mathbb{Z}$, where $\varphi(m)$ is the order of $\mathbb{Z}_m^*$. But $(a+m\mathbb{Z})^{\varphi(m)} = a^{\varphi(m)}+m\mathbb{Z} = 1 + m\mathbb{Z}$, and we have $a^{\varphi(m)} \equiv m \mod m$.

   d. Suppose $\gcd(a, b) = 1$. Then $\mathbb{Z}_a \times \mathbb{Z}_b$ is a group of order $ab$. Moreover, the order of the element $(1_a, 1_b)$ is the least common multiple of the orders $a$ and $b$ of $1_a$ and $1_b$, which must be $ab$. We have shown $(1, 1)$ generates $\mathbb{Z}_a \times \mathbb{Z}_b$, and thus $\mathbb{Z}_a \times \mathbb{Z}_b$ is a cyclic group isomorphic to $\mathbb{Z}_{ab}$.

      Then $\mathbb{Z}_a \times \mathbb{Z}_b$ has the same number of generators as $\mathbb{Z}_{ab}$. Let $p \in \mathbb{Z}_a$ and $q \in \mathbb{Z}_b$ both be generators with order $a$ and $b$ respectively. By homework 2 problem 3, the order of $(p, q)$ is the least common multiple of $a$ and $b$, $ab$. Then $(p, q)$ generates $\mathbb{Z}_a \times \mathbb{Z}_b$, along with every other pair of generators. Then there are $\varphi(a)\varphi(b)$ generators of $\mathbb{Z}_a \times \mathbb{Z}_b$ and thus of $\mathbb{Z}_{ab}$. Finally, we have shown that this number is precisely $\varphi(ab)$, so that $\varphi(ab) = \varphi(a)\varphi(b)$.

      Let $p$ be a prime number. Then the only divisors of $p$ are itself and one. Then every number $1, 2, \ldots, p-1$ is relatively prime with $p$ and $\varphi(p) = p - 1$.

      To calculate $\varphi(p^n)$, note that if we have $\gcd(m, p^n) > 1$ for some $1 \leq m \leq p^n$, then $m$ must be a multiple of $p$ less than or equal to $p^n$. There are $p^{n-1}$ such numbers. Then the remaining $p^n - p^{n-1}$ numbers are relatively prime to $p^n$ and $\varphi(p^n) = p^n - p^{n-1}$.

      Combining the above results, let $m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$. In the above result, notice that $\varphi(p^n) = p^n - p^{n-1} = p^n(1 - \frac{1}{p})$. Then we can write

      $$\varphi(m) = \prod_{i=1}^{n} \varphi(p_i^{a_i}) = \prod_{i=1}^{n} p_i^{a_i}(1 - \frac{1}{p_i}) = m \prod_{i=1}^{n}(1 - \frac{1}{p_i}).$$

      Let $a \in \mathbb{Z}$ and let $p$ be prime. If $a$ is a multiple of $p$, we have

      $$a^p \equiv 0 \bmod p = a \bmod p.$$

      Otherwise, $a$ is relatively prime with $p$, and we have $a^{\varphi(p)} = a^{p-1} = 1 \bmod p$ and thus

      $$a^p = a \bmod p.$$

2. Let $\mathfrak{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ be the upper half plane in the complex numbers. Let $G := SL(2, \mathbb{R})$.

$$\text{For } z \in \mathbb{C} \text{ and } \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ let } a.z = \frac{az+b}{cz+d}.$$

We will show that this defines an action on $\mathfrak{H}$. First we need to check that the action sends $\mathfrak{H}$ into $\mathfrak{H}$. Indeed, if $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL(2, \mathbb{R})$ and $z \in \mathfrak{H}$, then

$$\mathrm{Im}\, \alpha.z = \mathrm{Im} \left( \frac{az+b}{cz+d} \right) = \frac{ad-bc}{|cz+d|^2} \mathrm{Im}(z) > 0.$$

For $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, we have

$$e.z = \frac{z}{1} = z.$$

Finally, if $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $\beta = \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)$, then

$$\beta.(\alpha.z) = \frac{(ea+cf)z + (eb+fd)}{(ag+ch)z + (gb+dh)} = (\beta\alpha).z$$

as desired.

Now we will show the isotropy group of $i$ is the group

$$K := \left\{ \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} : \theta \in \mathbb{R} \right\}.$$

Suppose $\frac{ai+b}{ci+d} = i$. Then $ai + b = di - c$, and we must have

$$a = d$$
$$b = -c.$$

Then together with $ad - bc = 1$, we must have $a^2 + b^2 = 1$. Then it is clear that the values of $a, b$ must equal $\cos(\theta)$ and $\sin(\theta)$ respectively, with $c$ and $d$ determined by the above equations as well.

Finally we will show that $G$ acts transitively on $\mathfrak{H}$. We must show that there is only one orbit. Equivalently, we may show that any element of $\mathfrak{H}$ may be obtained from the action of $G$ on one element, namely $i$. This means that every element of $\mathfrak{H}$ is in the same orbit, and thus there is only one.

We need to solve $\frac{ai+b}{ci+d} = z$ for an arbitrary $z = p + qi \in \mathfrak{H}$. we have $ai + b = cpi - cq + dp + dqi$, and thus

$$b = dp - cq$$
$$a = cp + dq.$$

Here we may set $c = 0$ as not all four values $a, b, c, d$ are uniquely determined.

Then $b = dp, a = dq$, and thus using $ad - bc = 1$, we have $d^2 q = 1$. Here, the positivity of $q$ ensures that $d$ is a real number. In total, we get $d = \frac{1}{\sqrt{q}}$, $a = \sqrt{q}$, and $b = \frac{p}{\sqrt{q}}$, and indeed we get that

$$\frac{\sqrt{q}i + \frac{p}{\sqrt{q}}}{\frac{1}{\sqrt{q}}} = p + qi.$$

3. Let $G$ be a group and $H$ a subgroup. Let $\mathrm{core}(H)$ be the intersection of all conjugates of $H$ by elements of $G$. Let $S$ be the set of left cosets of $H$ in $G$. For $g \in G$, define $g_* : S \to S$ by $g_*(xH) = gxH$.

a. We will show that $g_*$ is an element of the symmetric group on $S$. We know that left multiplication by $g$ is a bijection on $G$, so it is clearly surjective on $S$. Also, it could not map two cosets to the same coset, as this would contradict the injectivity of left multiplication by $g$. Then we only must show that the map $g_*$ is well defined, sending different representatives of the same coset to the same coset. Suppose $aH = bH$, so that $b^{-1}a \in H$. Then $b^{-1}g^{-1}ga = (gb)^{-1}ga \in H$, and thus $g_*(aH) = g_*(bH)$.

b. Let $\varphi : G \to \mathrm{sym}(S)$ be the map $g \mapsto g_*$. To show that $\varphi$ is a homomorphism, we clearly have $\varphi(e) = I$, the identity map on $S$.

   Also, for any coset $aH$, we have $\varphi(gh)(aH) = (gh)_*(aH) = ghaH = g_*(h_*(aH)) = (g_* \circ h_*)(aH) = \varphi(g) \circ \varphi(h)(aH)$, and thus $\varphi(gh) = \varphi(g) \circ \varphi(h)$ and $\varphi$ is a homomorphism $G \to \mathrm{sym}(S)$.

   Lastly we will show that the kernel of $\varphi$ is exactly the core of $H$. Suppose $\varphi(g) = I$. Then $gaH = aH$ for all $a \in G$, and we have $ga \in aH$, or $g \in aHa^{-1}$. Then $g$ is in the core of $H$.

   Alternatively, suppose $g \in \mathrm{core}(H)$. Then $g \in aHa^{-1}$ for all $a \in G$, and thus $ga \in aH$ and we have $gaH = aH$. Then $\varphi(g) = I$.

   Then we have shown that $\ker \varphi = \mathrm{core}(H)$.