Algebra Autumn 2025
Frank Sottile
18 September 2025

Fifth Homework

Write your answers neatly, in complete sentences. I highly recommend recopying your work before handing it in. Correct and crisp proofs are greatly appreciated; oftentimes your work can be shortened and made clearer.

Hand in when you show up for your mid-term exam.

1. Let $m \geq 2$ be an integer. Recall that $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z} = \{0, 1, \ldots, m-1\}$.
   Set $\mathbb{Z}_m^* := \{k \in \mathbb{Z}_m \mid \gcd(k, m) = 1\}$. These are the cosets of integers that are relatively prime to m.
   (a) Show that $\mathbb{Z}_m^*$ is the set of generators of the cyclic group $\mathbb{Z}_m$.
   (b) Show that $\mathbb{Z}_m^*$ is a group under multiplication modulo m. Define $\phi(m) := |\mathbb{Z}_m^*|$, the order of this group. This is Euler's *totient function*, also called Euler's ϕ-function.
   (c) Deduce **Euler's Theorem:** If $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1$ mod m.
   (That is, m divides $a^{\phi(m)} - 1$, equivalently, $a^{\phi(m)} = 1$ as elements of $\mathbb{Z}_m$.)
   (d) Show that ϕ is multiplicative; if $a, b \in \mathbb{N}$ are relatively prime, $(\gcd(a, b) = 1)$, then $\phi(ab) = \phi(a) \cdot \phi(b)$.
   Let p be a prime number and show that $\phi(p) = p - 1$.
   Determine $\phi(p^n)$, where p is a prime and $n > 0$ is an integer.
   Deduce a formula for $\phi(m)$ in terms of the factorization of m into a product of powers of distinct primes. Express this in terms of m and its distinct prime divisors.
   (e) Use (d) to deduce **Fermat's Little Theorem:**
   If p is any prime number and $a \in \mathbb{Z}$, then $a^p \equiv a$ mod p.

2. Let $\mathfrak{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}$ be the upper half plane in the set of complex numbers. Let $G := SL(2, \mathbb{R})$, the group of real 2×2 matrices with determinant 1.

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

   Verify that this defines an action of G on $\mathfrak{H}$, and that the isotropy group of $\sqrt{-1}$ is the group

$$K\ :=\ \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \,\middle|\, \text{with } \theta \in \mathbb{R} \right\}\ .$$

   of rotation matrices. Show that G acts transitively on $\mathfrak{H}$.

3. Let H be a subgroup of a group G and define the *core of H* to be

$$\text{core}(H)\ :=\ \bigcap \{\, {}^{g}H \mid g \in G\}\,,$$

   the intersection of all conjugates of H by elements of G.
   Let $S := \{xH \mid x \in G\}$ be the set of left cosets of H in G. For each $g \in G$, define $g_*\colon S \to S$ by $g_*(xH) = gxH$.
   (a) Show that g_* is an element of the symmetric group on the set S, $\text{Sym}(S)$.
   (b) Show that the map $G \to \text{Sym}(S)$ given by $g \mapsto g_*$ is a group homomorphism with kernel $\text{core}(H)$.