Algebra Autumn 2023
Frank Sottile
6 September 2023

Third 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 for the grader Monday 11 September:

12. Let $x_1, \ldots, x_n$ be variables. Prove the following *Vandermonde identity* $\det(x_i^{j-1})_{i,j=1}^n = \prod_{1\leq a<b\leq n}(x_b - x_a)$. For example,

$$\det\begin{pmatrix} 1 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & x_4 \\ x_1^2 & x_2^2 & x_3^2 & x_4^2 \\ x_1^3 & x_2^3 & x_3^3 & x_4^3 \end{pmatrix} = (x_2-x_1)(x_3-x_1)(x_4-x_1)(x_3-x_2)(x_4-x_2)(x_4-x_3)\,.$$

13. What is the maximum order of an element of S_4? Use this to prove that D_{24}, the dihedral group of order 24, is not isomorphic to S_4.

14. Let $SL_2(\mathbb{Z}_3)$ be the group of 2×2 matrices of determinant 1 with entries in the field $\mathbb{Z}_3$ with three elements. Show that $SL_2(\mathbb{Z}_3)$ has order 24, and that it is not isomorphic to S_4. Is it isomorphic to D_{24}?

15. Let $m \geq 2$ be an integer. 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) 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.
    Show that ϕ is multiplicative; if $a, b \in \mathbb{N}$ are relatively prime, $(\gcd(a,b) = 1)$, then $\phi(ab) = \phi(a)\cdot\phi(b)$.
    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) Deduce Fermat's Little Theorem from the last part. If p is any prime number and $a \in \mathbb{Z}$, then $a^p \equiv a \mod p$.