Math 461 — Homework Assignment 5

Section F - group representation varieties

Due date: Friday April 27th
Please feel free to hand in parts before then if you would like feedback from the grader.

Question 21. (*Finite Fields — I*)

Suppose K is a finite field, that is to say a field with finitely many elements. Let q denote the number of elements of K.

21.1 Show that there is a morphism of rings

$$f : \mathbb{Z} \to K$$

that sends $a \in \mathbb{Z}_{>0}$ to $1 + 1 + \cdots + 1$ (a times).

21.2 Show that the kernel of f is an ideal of $\mathbb{Z}$. Show that it must be an ideal of the form $p\mathbb{Z} \subset \mathbb{Z}$ for a positive integer p.

21.3 Show that p is a prime number. (*Hint:* if $p = mn$ decomposes as a nontrivial product then $f(m) \cdot f(n) = 0$ in K, that isn't possible in a field.)

21.4 Conclude that K contains the subfield $\mathbb{F}_p \subset K$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. It is the image of the morphism f.

21.5 Show that multiplication by elements of this subfield gives K the structure of an $\mathbb{F}_p$-vector space. Conclude (using our theorem on bases of vector spaces) that K admits a basis $e_1, \ldots, e_k$ as a $\mathbb{F}_p$-vector space.

21.6 Use this basis to write any element of K in a unique way as $a_1e_1 + \ldots + a_ke_k$. Conclude the isomorphism of sets $K \cong \mathbb{F}_p^k$. Does this respect the field operation $+$? Does it respect the field operation $\times$ in any way?

21.7 Explain why the number of elements of $\mathbb{F}_p^k$ is p^k. Conclude that $q = p^k$.

Question 22. (*Finite cyclic groups*)

We are going to show that if G and H are finite cyclic groups of orders m and n respectively, and if $(m, n) = 1$ then $G \times H$ is a cyclic group of order mn.

22.1 Suppose $m, n \geq 2$. Define a map

$$p : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

by $p(\overline{a}) := \overline{na}$. Show that this is a group homomorphism. Similarly define the group homomorphism

$$q : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

by $q(\overline{a}) := \overline{ma}$.