GROUPS AND RINGS 2021. PROBLEM SHEET 5

QUESTIONS BY ALEXEI N. SKOROBOGATOV

For each $n \in \mathbb{N}$ define $\varphi(n)$ as the number of elements in the set $\{1, 2, \ldots, n-1\}$ that are coprime to n. Function $\varphi(n)$ is called *Euler's function*. It is clear that $\varphi(n) \geqslant 1$ for any $n \in \mathbb{N}$. The first few values of φ are

n	1	2	3	4	5	6	7	8
$\varphi(n)$	1	1	2	2	4	2	6	4

1. (a) Prove that $\varphi(n)$ is the number of elements of order n in $(\mathbb{Z}/n\mathbb{Z}, +)$.
(b) Prove that $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.
(c) Let p be a prime and let m be a positive integer. Prove that $\varphi(p^m) = p^m - p^{m-1}$.
(d) Prove that if $(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$. Deduce that

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

2. Prove that $d = \sum_{\delta|d} \varphi(\delta)$ for any $d \in \mathbb{N}$.

3. Let F be a field with q elements. Prove that the polynomial $x^{q-1} - 1$ has $q - 1$ distinct roots in F.

4. Let F be a field with q elements. Let d be a factor of $q - 1$. Prove that the polynomial $x^d - 1$ has d distinct roots in F.

5. Let F be a field with q elements. Prove that if $d|q-1$, then the number of elements of order d in $F^\times$ is $\varphi(d)$. (*Hint.* Proceed by induction on d using Questions 2 and 4.)

6. Deduce from Question 5 that the multiplicative group of any finite field is cyclic.

7. Let F be a field with p^n elements, where p is a prime. Prove that the additive group of F is cyclic if and only if $n = 1$.

8. Let k be a field of characteristic p, where p is a prime.
(a) Prove that for any $x, y \in k$ we have $(x + y)^p = x^p + y^p$. Deduce that

$$(x + y)^{p^m} = x^{p^m} + y^{p^m}$$

for any $x, y \in k$ and any positive integer m.
(b) The map $k \to k$ given by $x \mapsto x^p$ is called the *Frobenius map*. Conclude that for any field of characteristic p the Frobenius map is an endomorphism of k. Show that if k is finite, then the Frobenius map is an automorphism of k.
(c) Show that the set of fixed points of the Frobenius map $k \to k$ is the prime subfield $\mathbb{F}_p \subset k$.

9. What is the automorphism group of the field of rational numbers?

Date: October 10, 2021.