Math 212

Midterm 1
April 1999
Ali Nesin

1. Show that the group $\mathbb{Q}/\mathbb{Z}$ has a unique subgroup of order n for all $n \geq 1$.

2. Let R be a commutative ring with 1 and let S be a multiplicative subset (i.e. $SS \subseteq S$) of R not containing 0. Show that there is a prime ideal P of R such that $P \cap S = \emptyset$. (**Hint:** Use Zorn's Lemma).

3. Let F be a field. What are the automorphisms of the ring of polynomials $F[X]$. You may assume that you know the automorphisms of F.

4a. Let R be a domain (a commutative ring with 1 and without zerodivisors) and F a field. Assume that F is a subring of R. Then R is naturally a vector space over F. Show that if $\dim_F(R)$ is finite, then R is a field.

4b. Let R be a domain (a commutative ring with 1 and without zerodivisors) which is also a finite dimensional vector space over a field F. Show that R is a field.

5a. **(The Eisenstein Criterion)** Let $f(X) = X^n + a_1 X^{n-1} + ... + X_n \in \mathbb{Z}[x]$. Assume there is a prime p that divides $a_1, ..., a_n$ but that p^2 does not divide a_n. Show that $f(X)$ is irreducible in $\mathbb{Z}[X]$[1].

5b. Show that if p is a prime, then the polynomial $f(x) = x^{p-1} + x^{p-2} + ... + x + 1$ is irreducible in $\mathbb{Z}[x]$.

5c. Let $f(x) = 5x^4 - 7x + 7$. Show that f is irreducible in $\mathbb{Z}[x]$.

6. Find a domain R with two distinct primes p and q such that $rp + sq \neq 1$ for all $r, s \in R$.

7. Find the number of irreducible monic polynomials of degree 2 over $\mathbf{F}_q$. (q is a power of a prime, of course).

Find the number of irreducible monic polynomials of degree 3 over $\mathbf{F}_q$.

8. Let q be a power of the prime p and let $a \in \mathbf{F}_q$. Show that the polynomial map $f : \mathbf{F}_q \to \mathbf{F}_q$ defined by $x \to x^p - x + a$ is never onto.

---

[1] By Gauss' Lemma, to be irreducible in $\mathbb{Z}[X]$ is equivalent to be irreducible in $\mathbb{Q}[X]$. You don't need to use this fact for this question.