Math 212 Algebra Final
Ali Nesin
Spring 2008

1. Let K be a field. Show that a finite subgroup of K^* is cyclic. (6 pts.)
2. Let R be a domain. Let $G \subseteq R$ be a finite subset which is closed under multiplication. Show that G is a cyclic group. (3 pts.)
3. The ***characteristic*** char R of a ring R is the least integer $n > 0$ such that $nr = 0$ for all $r \in R$ if such an n exists; otherwise the characteristic is said to be 0. Show that the characteristic of a domain is either 0 or a prime. (3 pts.) Show that if char $R = n$ iff $\mathbb{Z}/n\mathbb{Z}$ embeds (in a unique way) in R (3 pts.).

From now on we will assume without warning that $\mathbb{Z}/n\mathbb{Z} \subseteq R$ if char $R = n$. Also p will always stand for a positive prime number. We let $\mathbf{F}_p = \mathbb{Z}/p\mathbb{Z}$.

4. Show that up to isomorphism there is a unique field with p elements. (p is a prime). (1 pts.)
5. Let F be a finite field. Show that the additive group F^+ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$ for some prime p (= char F) and some positive natural number n. (3 pts.)
6. Show that if R is a commutative ring with prime characteristic p then $r \mapsto r^p$ is a ring homomorphism. (2 pts.) Is this still true if the characteristic is not a prime but still positive? (3 pts.)
7. Show that a finite field F of characteristic $p > 0$ is multiplicatively p-divisible, i.e. for every $x \in F$ there is a $y \in F$ such that $y^p = x$. (3 pts.)
8. Find a field of characteristic $p > 0$ which is not multiplicatively p-divisible. (3 pts.)
9. Show that in any finite field with q elements for any x, $x^q = x$. (2 pts.)
10. Show that a field can contain at most one subfield of a given finite cardinality. (4 pts.)
11. Let F be a finite field with q elements. How many elements of F are squares in F? (3 pts.)
12. Let F be a finite field with q elements. How many elements of F are cubes in F? (3 pts.)
13. Show that in a field with p^{2n} elements the equation $x^2 = -1$ has a solution. (2 pts.)
14. Show that any field with p^n elements has at least n automorphism. (3 pts.)
15. Show that if a field with p^n elements has a subfield with p^m elements then $m \mid n$. (3 pts.)
16. Let F be a finite field of characteristic p. Show that there is an element x such that $F = \mathbf{F}_p[x]$. (3 pts.) If $|F| = p^n$ can you find a (good) lower bound for the number of such elements? (4 pts.) If n is a prime show that there are exactly $p^n - p$ such elements. (2 pts.)
17. Show that a finite field F is isomorphic to $\mathbf{F}_p[X]/\langle f\rangle$ for some prime p and some irreducible polynomial f. Show that $|F| = p^{\deg f}$. (4 pts.)
18. Show that a finite field with p^n elements has exactly n automorphisms. (4 pts.)
19. Let F be a field and $f \in F[X]$ be a polynomial. Show that there is a field K which contains F in which $f = a(X - a_1) \ldots (X - a_n)$ for some $a \in F$ and $a_1, \ldots, a_n \in K$. (5 pts.)
20. Let F be a field of characteristic p and $a \in F$. Show that there is a field $K \geq F$ such that $X^p - a = (X - b)^p$ for some $b \in K$. (4 pts.) Conclude that a is not a p^{th} power in F, then $X^p - a$ is irreducible in $F[X]$. (5 pts.)
21. Show that for any prime p and any integer $n > 0$ there is a field with p^n elements. (4 pts.)

22. Show that any two finite fields with the same number of elements are isomorphic. (5 pts.)

23. Show that in any finite field every element is a sum of two squares. (10 pts.)