
620-321 Algebra, Semester 1, 2009
Answers to Problem Sheet 9

2. (c) The group is cyclic of order 8. $(1 + a)$ is a generator.
3. 3
5. Using the binomial formula we get: $(a + b)^p = a^p + b^p$. That it is injective follows from the fact that K has no zero divisors. Since K is finite, it must also be surjective.
6. Let $K = \mathbb{Z}_p(u)$. Note that K is a finite field (having $p^{\deg(u, \mathbb{Z}_p)}$ elements) of characteristic p . Then $a \mapsto a^p$ defines an isomorphism φ of K by the previous question. This isomorphism fixes \mathbb{Z}_p (pointwise) by Fermat's Little Theorem. So u^p is also a root of f , since $f(u^p) = f(\varphi(u)) = \varphi(f(u)) = \varphi(0) = 0$.
7. If u_1, \dots, u_q are the elements of a finite field K , consider the polynomial $f(x) = (x - u_1) \dots (x - u_q) + 1$. None of the u_i is a root of f , and so K cannot be algebraically closed.
8. Suppose $n = qd + r$. Then the identity $(x^n - 1) = (x^d - 1)(x^{n-d} + x^{n-d-1} + \dots + x^{n-qd}) + (x^r - 1)$ shows that $(x^d - 1) \mid (x^n - 1)$ in $\mathbb{Z}[x]$ if and only if $d \mid n$. The same formula shows $(p^d - 1) \mid (p^n - 1)$ in \mathbb{Z} if and only if $d \mid n$.

If K is a finite field with p^n elements and E is a subfield with p^d elements, then the multiplicative group of E is a subgroup of the multiplicative group of K and so $(p^d - 1) \mid (p^n - 1)$ and hence $d \mid n$.

Conversely suppose $d \mid n$. Since the multiplicative group of K is cyclic of order $p^n - 1$, it has a unique subgroup of order $p^d - 1$. Let E denote that subgroup together with 0. Then the elements of E are those elements of K that satisfy $x^{p^d} - x = 0$. Using the formula $(a \pm b)^{p^d} = a^{p^d} \pm b^{p^d}$ it follows that E is the (unique) subfield with p^d elements.