Algebra III M3P8, M4P8

Solutions Sheet 4

1. (a) By Lagrange's theorem $x^{p^n-1} = 1$ for any $x \in F^*$, hence the result.

(b) We need to check that f is a homomorphism, i.e. $f(xy) = f(x)f(y)$ (obvious) and $f(x+y) = f(x) + f(y)$ for any x, $y \in F$. The latter follows from the binomial formula and the fact that

$$\binom{p}{n} \equiv 0 \bmod p$$

if $0 < n < p$.

2. Since $169 = 13^2$ we need an irreducible quadratic polynomial $f(x)$ over $\mathbb{Z}/13$, then the desired field is $\mathbb{Z}/13[x]/(f(x))$. Check that 2 is not a square mod 13. Hence take $f(x) = x^2 - 2$.

A field with 16 elements can be constructed from a field F with 4 elements. Recall that $F = \{0, 1, \omega, \omega+1\}$, where $\omega^2 = \omega + 1$. The polynomial $x^2 + x + \omega$ has no roots in F, so $F[x]/(x^2 + x + \omega)$ is a quadratic extension of F, and hence has 16 elements.

Alternatively, $g(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Z}/2$. Indeed, this polynomial has no roots, so is not divisible by a linear polynomial, neither is it divisible by a unique irreducible quadratic polynomial over $\mathbb{Z}/2$, namely $x^2 + x + 1$. Thus $\mathbb{Z}/2[x]/(g(x))$ is a field with 16 elements.

3. (1) $x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$.

(2) $x^4 + 1$ is irreducible over $\mathbb{Q}$.

(3) $x^3 - 5 = (x-3)(x^2 + 3x + 9)$ over $\mathbb{Z}/11$. The quadratic factor here has no roots in $\mathbb{Z}/11$ (its discriminant is $-3 \cdot 9$, but -3 is not a square mod 11) hence it is irreducible.

(4) $x(x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$ over $\mathbb{Z}/2$.

(5) $(x+1)(x+\omega^2)$ over the field F with four elements.

4. For any a, $b \in R$ we have $(a+b)^2 = a + b$, hence $a^2 + b^2 + ab + ba = a + b$. It follows that $ab = -ba$. Squaring both sides we obtain $ab = ba$.

5. (a) Consider the surjective homomorphism $R \to \mathbb{R}$ that sends $f(x)$ to $f(a)$. Its kernel is I, hence $R/I \simeq \mathbb{R}$. This is a field so that I is maximal.

(b) This is easy.

6. (a) As in the lectures, we show that the set of roots R of $x^{p^m} - x = 0$ in F is closed under addition, multiplication and subtraction. Since F has no zero divisors, R must be a subfield of F. The non-zero roots satisfy $x^{p^m-1} - 1 = 0$, but in lectures

we proved that this polynomial has $p^m - 1$ roots in F (since $p^m - 1$ divides $p^n - 1$). Hence R is a field with p^m elements.

(b) If $K \subset F$ is a subfield, then F is a vector space over K, hence $|F| = |K|^r$ for a positive integer r. Therefore, K must have p^m elements, where $m|n$. By part (a) all such m show up.