MA2215: Fields, rings, and modules
Homework problems due on December 3, 2012

1. Clearly, $x^4 - 4x^2 - 5 = (x^2+1)(x^2-5)$, so the splitting field is $\mathbb{Q}(i, \sqrt{5})$. Furthermore, $\mathbb{Q}(\sqrt{5})$ is a subfield of $\mathbb{R}$ so it does not contain i, therefore $[\mathbb{Q}(i,\sqrt{5})\colon \mathbb{Q}(\sqrt{5})] > 1$, so $[\mathbb{Q}(i,\sqrt{5})\colon \mathbb{Q}(\sqrt{5})] = 2$, and $[\mathbb{Q}(i,\sqrt{5})\colon \mathbb{Q}] = 4$ by Tower Law.

2. Since $x^4 - 4x^2 - 5 = (x^2+1)(x^2-5)$, the splitting field over $\mathbb{R}$ is $\mathbb{R}(i) = \mathbb{C}$ of degree 2, and the degree over $\mathbb{C}$ is 1.

3. First of all, $x^{11} - 5$ is irreducible (Eisenstein), so $[\mathbb{Q}(\sqrt[11]{5})\colon \mathbb{Q}] = 11$. Second, clearly the complex roots of our polynomial are obtained from $\sqrt[11]{5}$ multiplying it by all 11th roots of 1. Obviolusly $x^{11} - 1 = (x-1)(x^{10} + x^9 + \ldots + x + 1)$. Since 11 is a prime, $x^{10} + x^9 + \ldots + x + 1$ is irreducible (proved in class), so the splitting field of $x^{11} - 1$ is of degree 10 over $\mathbb{Q}$. Altogether, since we have a subfield of degree 11 and a subfield of degree 10 (and they together generate everything), the total degree is 110.

4. Over $\mathbb{F}_3$ we have $x^8 + 2 = x^8 - 1$, so the splitting field of $x^8 + 2$ is the same as the splitting field of $x^8 - 1$ is the same as the splitting field of $x(x^8-1) = x^9 - x$. The latter is clearly $\mathbb{F}_9$, as we know from class.

5. (**a**) We have $(x+1)^p - x - 1 \equiv (x^p + 1) - x - 1 = x^p - x \pmod p$ since all middle binomial coefficients in $(x+1)^p$ are divisible by p.

(**b**) We have $f(x) = f(x+1)$, so $f(x+1) = f(x+2)$ etc. Let $a = f(0)$. The equation $f(x) = a$ has all elements of $\mathbb{F}_p$ as roots, so its degree should be at least p.

(**c**) From the first part of this problem, $g(x) = g(x+1)$. Suppose that $g(x)$ has a nontrivial factorisation into irreducibles. Clearly, for each of those irreducibles $h(x)$ the element $h(x+1)$ is also irreducible, so it has to appear in the factorisation. Hence we either have $h(x) = h(x+1)$ or it is a factor different from $h(x)$. It is impossible to have $h(x) = h(x+1)$, since all factors are of degree less than p. Suppose that there are repetitions among $h(x)$, $h(x+1)$, $\ldots$, $h(x+p-1)$. Then $h(x) = h(x+l)$, and since integers modulo p form a field, there exists m such that $lm \equiv 1 \pmod p$, hence $h(x) = h(x+l) = h(x+2l) = \cdots = h(x+lm) = h(x+1)$, a contradiction. Therefore all these polynomials are different irreducible factors of $g(x)$. The latter would mean that $g(x)$ factorises into linear factors, hence has roots. But for each $a \in \mathbb{F}_p$ we have $g(a) = -1$, a contradiction.