MATH 3030, Abstract Algebra
FALL 2012
Toby Kenney
Homework Sheet 12
Model Solutions

Basic Questions

1. *Show that it is not possible to trisect an angle of* $\cos^{-1}(0.6)$. *[An angle of* $\cos^{-1}(0.6)$ *is constructable.]*

   Trisecting an angle of $\cos^{-1}(0.6)$ means constructing a line segment of length $\cos\left(\frac{\cos^{-1}(0.6)}{3}\right)$. However, we know that $\cos(3x) = 4\cos^3 x - 3\cos x$, so $\cos\left(\frac{\cos^{-1}(0.6)}{3}\right)$ is a zero of $4x^3 - 3x - 0.6$, or equivalently, a zero of $20x^3 - 15x - 3$, which is irreducible by Eisenstein's criterion for $p = 3$. Therefore, this length has degree 3 over $\mathbb{Q}$, and so is not constructible, since 3 is not a power of 2.

2. *Show that* $x^3 + 2x^2 + 4x + 3$ *has distinct zeros in the algebraic closure of* $\mathbb{Z}_5$.

   By checking all values, we see that $x^3 + 2x^2 + 4x + 3$ has no zeros in $\mathbb{Z}_5$. Let α be a zero in the algebraic closure of $\mathbb{Z}_5$. We factorise in the algebraic closure of $\mathbb{Z}_5$ using long division. $x^3 + 2x^2 + 4x + 3 = (x - \alpha)(x^2 + (\alpha + 2)x + (\alpha^2 + 2\alpha + 4))$. To show that α is not a repeated zero, we need to show that $\phi_\alpha(x^2 + (\alpha + 2)x + (\alpha^2 + 2\alpha + 4)) \neq 0$. However, we have that $\phi_\alpha(x^2 + (\alpha + 2)x + (\alpha^2 + 2\alpha + 4)) = 3\alpha^2 + 4\alpha + 4$. Clearly, this is not zero, because if it were, then α would be a zero of $3x^2 + 4x + 3$, so we would not have that $x^3 + 2x^2 + 4x + 3$ is the smallest-degree irreducible polynomial of which α is a zero.

3. *How many primitive 15th roots of unity are there in GF(16)?*

   The multiplicative group of GF(16) is cyclic of order 15. The primitive roots of unity are the generators of this group. There are $\phi(15) = 8$ generators, so GF(16) has 8 primitive 15th roots of unity.

4. *Find a basis for the field extension* $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ *over* $\mathbb{Q}$.

   One such basis is $\{1, \sqrt{2}, \sqrt[3]{3}, \sqrt{2}\sqrt[3]{3}, \sqrt[3]{9}, \sqrt{2}\sqrt[3]{9}\}$.

Theoretical Questions

5. *Let* E *be algebraically closed, and let* F *be a subfield of* E. *Show that the algebraic closure of* F *in* E *is also algebraically closed. [So for example,*

the field of algebraic numbers (that is, complex numbers that are algebraic over $\mathbb{Q}$) is algebraically closed.

Let $f \in F[x]$. We need to show that the algebraic closure of F in E contains a zero of f. However, since E is algebraically closed and F is a subfield of E, we know that f is a polynomial in $E[x]$, so, since E is algebraically closed, there is a zero of f in E. However, any zero of f must be algebraic over F, by definition. Therefore, this zero of f must be in the algebraic closure of F in E.

6. *Let F be a field. Let α be transcendental over F. Show that any element of $F(\alpha)$ is either in F or transcendental over F.*

   Let $\beta \in F(\alpha)$. Then β is a rational function in α. Suppose $\beta = \frac{f(\alpha)}{g(\alpha)}$, for polynomials $f, g \in F[x]$. Now suppose β is algebraic over F, so β is a zero of some polynomial $h \in F[x]$. Suppose h has degree n. Then we see that $g(\alpha)^n h(\beta)$ is a polynomial k in α. However, since $h(\beta) = 0$, we get that $k(\alpha) = 0$. Since α is transcendental over F, k must be the zero polynomial. This can only happen if f and g are constant polynomials, in which case, we have that $\beta \in F$.

7. *Is it possible to duplicate a cube if we are given a unit line segment and a line segment of length $\sqrt[3]{3}$?*

   This is still impossible, because $[\mathbb{Q}(\sqrt[3]{3}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{3})] = 3$ is not a power of 2.

8. *Show that every irreducible polynomial in $\mathbb{Z}_p[x]$ divides $x^{p^n} - x$ for some n.*

   Let f be an irreducible polynomial in $\mathbb{Z}_p[x]$. Let E be an extension field of $\mathbb{Z}_p$ containing a zero α of f, and such that $[E : \mathbb{Z}_p]$ is finite. (Such a field exists because adjoining a zero of f only requires an extension field of finite degree.) Now since E is finite of order p^n for some n, so its multiplicative group of non-zero elements has order $p^n - 1$. Therefore, every non-zero element of E has order a factor of $p^n - 1$ in this multiplicative group. This means that every non-zero element of E is a zero of $x^{p^n-1} - 1$. In particular α is a zero of $x^{p^n} - x$. Let I be the ideal in $\mathbb{Z}_p[x]$ generated by f and $x^{p^n} - x$. Since $(x - \alpha)$ is a factor of both f and $x^{p^n} - x$ in $E[x]$, the ideal generated by them in $E[x]$ must not contain 1. Therefore, I must not contain 1, since I is contained in this ideal. Since I contains (f), and (f) is a maximal ideal, we must have $I = (f)$. Therefore, we have $x^{p^n} - x \in (f)$, so f must divide $x^{p^n} - x$.

9. *Show that a finite field of p^n elements has exactly one subfield of p^m elements for any divisor m of n.*

   Let F be a field of p^n elements. Consider the set $\{z \in F | z$ is contained in a subfield of F with p^m elements
   To be in this set, z must be a zero of $x^{p^m} - x$. This polynomial has p^m zeros in F. Therefore, this set has at most p^m elements. If F had two

subfields of p^m elements, their unions would be contained in this set, and would have more than p^m elements, so F has at most one subfield of p^m elements.

Conversely, to show that F has a subfield of p^m elements, we know show that the zeros of $x^{p^m} - x$ in $\overline{\mathbb{Z}_p}$ form a field of p^m elements, so we just need to show that all these zeros are in F. We know that the multiplicative group of non-zero elements of F is cyclic. Let a be a generator. Now the elements of F are all of the form a^i for some i. An element a^i is a zero of $x^{p^m} - x$ if and only if $ip^m \equiv i \pmod{p^n - 1}$, or equivalently $i(p^m - 1) \equiv 0 \pmod{p^n - 1}$. This happens only if i is divisible by $\frac{p^n-1}{p^m-1}$. There are $p^m - 1$ such elements modulo $p^n - 1$, so all $p^m - 1$ non-zero elements of $\overline{\mathbb{Z}_p}$ that are zeros of $x^{p^m} - x$ are all in F. Furthermore, 0 is in F, so all zeros of $x^{p^m} - x$ are in F, and these form a subfield with p^m elements.

Bonus Questions

10. *Let F_q be the finite field with q elements.*

(a) Show that an irreducible polynomial of degree m in $F_q[X]$ divides $x^{q^n} - x$ if and only if m divides n.

Let f be an irreducible polynomial of degree m in $F_q[x]$. Let α be a zero of f. We know that $[F_q(\alpha) : F_q] = m$. Let E be the extension field of zeros of $x^{q^n} - x$, so that $[E : F_q] = n$. If f divides $x^{q^n} - x$, then it $F_q(\alpha)$ must be a subfield of E, so we have $n = [E : F_q] = [E : F_q(\alpha)][F_q(\alpha) : F]$, which gives that m divides n.

Conversely, suppose that m divides n. Then $F_q(\alpha)$ is a field with q^m elements, all of which must be zeros of $x^{q^m} - x$, so the zeros of f are all zeros of $x^{q^m} - x$, which are also all zeros of $x^{q^n} - x$. Therefore, f and $x^{q^n} - x$ have a common factor in $F_q[x]$, so the ideal they generate is not the whole of $F_q[x]$. Therefore, since it contains the irreducible polynomial f, it must be the ideal generated by f. This means that f divides $x^{q^n} - x$.

(b) If $a_n(q)$ is the number of irreducible polynomials of degree n over F_q, show that

$$\sum_{d|n} da_d(q) = q^n$$

We know that $x^{q^n} - 1$ has no repeated zeros, so it is not divisible by the square of any polynomial in $F_q[x]$. Therefore, it must be the product of all irreducible monic polynomials of degrees dividing n in $F_q[x]$ (up to a constant multiple). The total degree of this product is

$$\sum_{d|n} da_d(q)$$

and the degree of $x^{q^n} - x$ is q^m. Equal polynomials must have equal degrees, so we get

$$\sum_{d|n} da_d(q) = q^n$$

(c) How many irreducible polynomials of degree 6 are there over $\mathbb{Z}_3$.

Using the formula from (b), we know there are 3 irreducible polynomials of degree 1 over $\mathbb{Z}_3$, so $a_1(3) = 3$. This gives $3 + 2a_2(3) = 3^2$, giving $a_2(3) = 3$. Similarly, $3 + 3a_3(3) = 3^3$, giving $a^3(3) = 8$. Finally, we get $3 + 6 + 24 + 6a_6(3) = 3^6$, giving $a_6(3) = 116$. Therefore, there are 116 irreducible polynomials of degree 6 over $\mathbb{Z}_3$.