

## Assignment M2

Due 6pm Wednesday 15 September 2004.

1. Prove that these polynomials are irreducible over the rationals.

a)  $t^3 - t - 7$     b)  $t^4 + t + 7$     c)  $t^{73} + 30t^{45} + 42t^{19} + 420$     d)  $72t^3 + 7t + 72$

2. Let  $f(t)$  be in  $\mathbf{Q}[t]$  and let  $\alpha$  be a complex number. Show that  $(t - \alpha)^2 \mid f(t)$  if and only if  $f(\alpha) = f'(\alpha) = 0$ .

3. Let  $a$  and  $b$  be integers. Show that  $\mathbf{Q}(\sqrt{a}, \sqrt{b})/\mathbf{Q}$  is a simple extension.

4. Find the irreducible polynomial for  $\sqrt[4]{2}$  over  $\mathbf{Q}(\sqrt{2})$ .

5. Let  $p(t)$  be the irreducible polynomial for  $\sqrt{4 + \sqrt{7}} - 3$  over the rationals. Find  $p(t)$ . Find all the zeros of  $p(t)$ , and show that they are all in  $\mathbf{Q}(\sqrt{4 + \sqrt{7}})$ .

6. Let the irreducible polynomials for  $\alpha$  and  $\beta$  over the rationals be  $t^2 + t - 1$  and  $t^2 + 6t + 4$ , respectively. Prove that  $\mathbf{Q}(\alpha)/\mathbf{Q}$  and  $\mathbf{Q}(\beta)/\mathbf{Q}$  are isomorphic.

## Assignment M2 Solutions

1. Prove that these polynomials are irreducible over the rationals.

a)  $t^3 - t - 7$

**Solution.** It suffices (in all parts of this problem) to prove that the given polynomial is irreducible over the integers.

Since this polynomial is of degree 3, it suffices to prove that it has no rational zeros. By the rational root theorem, if there is a rational zero, it must be a divisor of  $-7$ , that is, it must be  $1, 7, -1,$  or  $-7$ . But in fact none of these is a zero of the polynomial.

b)  $t^4 + t + 7$

**Solution.** Again if there's a rational zero it must be  $1, 7, -1,$  or  $-7$ , and again none of these is a zero. Since the polynomial is of degree 4, we must also check to see that it isn't a product of two quadratics.

If it is, we can assume both quadratics are monic, so we have

$$(t^2 + at + b)(t^2 + ct + d) = t^4 + t + 7$$

for some integers  $a, b, c,$  and  $d$ . Multiplying out and equating coefficients we get the equations  $a + c = 0, b + ac + d = 0, ad + bc = 1, bd = 7$ . Eliminate  $c$  from these equations to get  $b - a^2 + d = 0, a(d - b) = 1, bd = 7$ . All the integer solutions of the third equation have  $d - b = \pm 6$ , which is inconsistent with the second equation.

c)  $t^{73} + 30t^{45} + 42t^{19} + 420$

**Solution.** The prime number 3 divides all coefficients except the leading coefficient, and its square, 9, doesn't divide the constant term. Thus, by the Eisenstein criterion, the polynomial is irreducible.

d)  $72t^3 + 7t + 72$

**Solution.** Reduced modulo 5, this polynomial is  $2t^3 + 2t + 2$ . Substituting in turn  $t = 0, 1, \dots, 4$  we find the polynomial has no roots modulo 5, so it has no rational roots. Since it has degree 3, we can conclude that it is irreducible over the rationals.

2. Let  $f(t)$  be in  $\mathbf{Q}[t]$  and let  $\alpha$  be a complex number. Show that  $(t - \alpha)^2 \mid f(t)$  if and only if  $f(\alpha) = f'(\alpha) = 0$ .

**Solution.** First assume  $(t - \alpha)^2 \mid f(t)$ . Then  $f(t) = (t - \alpha)^2 q(t)$  for some  $q(t)$  in  $\mathbf{Q}[t]$ . Thus  $f(\alpha) = (\alpha - \alpha)^2 q(\alpha) = 0$ ; also,  $f'(t) = 2(t - \alpha)q(t) + (t - \alpha)^2 q'(t) = (t - \alpha)r(t)$  where  $r(t) = 2q(t) + (t - \alpha)q'(t)$ , whence  $f'(\alpha) = (\alpha - \alpha)r(\alpha) = 0$ .

Now assume  $f(\alpha) = f'(\alpha) = 0$ . Then  $f(t) = (t - \alpha)q(t)$  for some  $q(t)$  in  $\mathbf{Q}[t]$ . Thus  $f'(t) = q(t) + (t - \alpha)q'(t)$ , and  $0 = f'(\alpha) = q(\alpha)$ . But then  $q(t) = (t - \alpha)r(t)$  for some  $r(t)$  in  $\mathbf{Q}[t]$ . Then  $f(t) = (t - \alpha)^2 r(t)$ , and  $(t - \alpha)^2 \mid f(t)$ .

3. Let  $a$  and  $b$  be integers. Show that  $\mathbf{Q}(\sqrt{a}, \sqrt{b})/\mathbf{Q}$  is a simple extension.

**Solution.** We'll prove that  $\mathbf{Q}(\sqrt{a}, \sqrt{b}) = \mathbf{Q}(\sqrt{a} + \sqrt{b})$ .

It's clear that  $\mathbf{Q}(\sqrt{a} + \sqrt{b})$  is contained in  $\mathbf{Q}(\sqrt{a}, \sqrt{b})$ , so we just have to prove containment in the other direction.

Let  $\alpha = \sqrt{a} + \sqrt{b}$ . Then  $\alpha^3 = (a+3b)\sqrt{a} + (3a+b)\sqrt{b}$ , so  $(2a-2b)\sqrt{a} = (3a+b)\alpha - \alpha^3$  is in  $\mathbf{Q}(\alpha)$ , so  $\sqrt{a}$  is in  $\mathbf{Q}(\alpha)$  (or else  $a = b$ , in which case the whole problem is trivial). Then  $\sqrt{b} = \alpha - \sqrt{a}$  is in  $\mathbf{Q}(\alpha)$ , and we're done.

4. Find the irreducible polynomial for  $\sqrt[4]{2}$  over  $\mathbf{Q}(\sqrt{2})$ .

**Solution.** The irreducible polynomial for  $\sqrt[4]{2}$  over  $\mathbf{Q}$  is  $t^4 - 2$ , but over  $\mathbf{Q}(\sqrt{2})$  this factors as  $t^4 - 2 = (t^2 - \sqrt{2})(t^2 + \sqrt{2})$ . By the tower law  $[\mathbf{Q}(\sqrt[4]{2}) : \mathbf{Q}(\sqrt{2})] = 2$  (since  $[\mathbf{Q}(\sqrt[4]{2}) : \mathbf{Q}] = 4$  and  $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$ ), so we are looking for a quadratic polynomial. It must be  $t^2 - \sqrt{2}$ , since this vanishes at  $\sqrt[4]{2}$  and the other quadratic doesn't.

5. Let  $p(t)$  be the irreducible polynomial for  $\sqrt{4 + \sqrt{7}} - 3$  over the rationals. Find  $p(t)$ . Find all the zeros of  $p(t)$ , and show that they are all in  $\mathbf{Q}(\sqrt{4 + \sqrt{7}})$ .

**Solution.** Let  $\alpha = \sqrt{4 + \sqrt{7}} - 3$ . Add 3 to both sides, square, subtract 4, square again, and subtract 7 to get  $\alpha^4 + 12\alpha^3 + 46\alpha^2 + 60\alpha + 18 = 0$ . Let  $p(t) = t^4 + 12t^3 + 46t^2 + 60t + 18$ . Then  $p$  is monic, irreducible over  $\mathbf{Q}$  by Eisenstein with prime 2, and  $p(\alpha) = 0$ , so it is the polynomial we are looking for.

Retracing the algebraic steps above, the zeros of  $p$  are  $\pm\sqrt{4 \pm \sqrt{7}} - 3$ .

Clearly  $\pm\sqrt{4 + \sqrt{7}}$  are in  $\mathbf{Q}(\sqrt{4 + \sqrt{7}})$ , so  $\pm\sqrt{4 + \sqrt{7}} - 3$  are in  $\mathbf{Q}(\sqrt{4 + \sqrt{7}})$ . Now  $\sqrt{4 + \sqrt{7}}\sqrt{4 - \sqrt{7}} = 3$  is in  $\mathbf{Q}$ , so  $\sqrt{4 - \sqrt{7}}$  is in  $\mathbf{Q}(\sqrt{4 + \sqrt{7}})$ , so all the zeros of  $p$  are in there.

6. Let the irreducible polynomials for  $\alpha$  and  $\beta$  over the rationals be  $t^2 + t - 1$  and  $t^2 + 6t + 4$ , respectively. Prove that  $\mathbf{Q}(\alpha)/\mathbf{Q}$  and  $\mathbf{Q}(\beta)/\mathbf{Q}$  are isomorphic.

**Solution.** Since  $\alpha$  is a zero of  $t^2 + t - 1$  it is one of the numbers  $(-1 \pm \sqrt{5})/2$ ; since  $\beta$  is a zero of  $t^2 + 6t + 4$  it is one of the numbers  $-3 \pm \sqrt{5}$ ; thus  $\mathbf{Q}(\alpha) = \mathbf{Q}(\beta) = \mathbf{Q}(\sqrt{5})$  and the two extensions are equal. An explicit isomorphism can be given by

$$\phi : \mathbf{Q}(\beta) \rightarrow \mathbf{Q}(\alpha), \quad \phi(a + b\beta) = a - 2b + 2b\alpha$$

This works because (as you can check)  $a + b(-3 \pm \sqrt{5}) = a - 2b + 2b(-1 \pm \sqrt{5})/2$ ; you can also check directly that  $\phi$  preserves addition and multiplication.