620-321 Algebra, Semester 1, 2009

Answers to Problem Sheet 4

1. Observe that the "long division" scheme still allows one to divide g into f since it is only the leading coefficient of g that needs to have an inverse.

2. $x^3 - 6x^2 + x + 4 = (x-1)(x^2 - 5x - 4)$ and the later has irrational roots. Neither divides $x^5 - 6x + 1$ so the two polynomials have no irreducible factors in common in $\mathbb{Q}[x]$. Hence their gcd is 1.

4. gcd $= 5x - 5 = (x^3 + 2x^2 + 4x - 7) - (x+1)(x^2 + x - 2)$

5. Suppose that $R[x]$ is a PID. We want to show any element $0 \neq a \in R$ is a unit. Let I be the ideal in $R[x]$ generated by the two polynomials a and x. Then I consists of all polynomials whose constant term is a multiple of a. By hypothesis I must be principal, say $I = (f)$. Since $a \in I$ the polynomial f must be a constant, that is $f \in R$. Then f is a multiple of a, so $(a) = (f)$ and we may assume $f = a$. Now $x = a \cdot g$ for some polynomial $g \in R[x]$. But this equation implies $g = bx$ for some $b \in R$ and hence $ab = 1$ Hence a is a unit.

7. Eisenstein.

9. Irreducible in both.

12. $(1+2i)(1-2i)$, 7, $(1+2i)(2-i)$

13. Substituting $x = \frac{r}{s}$ and multiplying by s^n gives

$$a_0 s^n + a_1 r s^{n-1} + \cdots + a_n r^n = 0$$

Since s divides the first n terms, it must also divide $a_n r^n$. As s and r are relatively prime we conclude that $s|a_n$. Similarly, r divides the last n terms and therefore must divide $a_0 s^n$ and hence $r|a_0$.

14. (a) The polynomial has no rational roots. Therefore if it is reducible, it must factor into a product of two monic quadratic polynomials with integer coefficients. Suppose $x^4 - 16x^2 + 4 = (x^2 + ax + b)(x^2 + \alpha x + \beta)$. Expanding and equating coefficients gives

$$b\beta = 4 \qquad (1)$$
$$a\beta + b\alpha = 0 \qquad (2)$$
$$b + \beta + a\alpha = -16 \qquad (3)$$
$$a + \alpha = 0 \qquad (4)$$

Notice that we must have $a \neq 0$, since otherwise $b\beta = 4$ and $b + \beta = -16$ which has no (integral) solutions. Multiplying 4 by b and subtracting from 2 yields $\alpha(\beta - b) = 0$. Hence $\beta = b = \pm 2$. The third equation then gives $-a^2 = -16 \pm 4$. Since this has no integer solutions, the original polynomial is irreducible.
(b) $x^4 - 32x^2 + 4 = (x^2 - 6x + 2)(x^2 + 6x + 2)$ is not irreducible.

15. (a) $(x+1)$ is a factor (b) $(x+1)$ is a factor
(c) Irreducible. Reducing mod 5 gives $2x^3 + x^2 - x - 1$ which has no roots in $\mathbb{Z}_5$.
(d) Irreducible. Reducing mod 2 gives $x^4 + x + 1$ which has no linear factors since it has no roots in $\mathbb{Z}_2$. It also has no quadratic factors. The only irreducible quadratic in $\mathbb{Z}_2$ is $x^2 + x + 1$.

16. Use Eisenstein's criterion.
(a) irreducible (b) irreducible (c) Substitute $x = y + 1$ to get irreducible.

18. Irreducible in $\mathbb{Z}_2[x]$ since it has no roots. In $\mathbb{Z}_3[x]$ we have $x^3 + x^2 + 1 = (x-1)(x^2 - x - 1)$.

19. The irreducibles are: $x, x+1, x-1, x^2+1, x^2+x-1, x^2-x-1$.

20. $x, x+1, x^2+x+1, x^3+x^2+1, x^3+x+1, x^4+x^3+1, x^4+x+1, x^4+x^3+x^2+x+1$.