PMATH 347 Groups and Rings, Solutions to the Exercises for Chapter 12

1: (a) Let $f = 5x^4 + 3x^3 + 1$ and $g = 3x^2 + 2x + 1$ in $\mathbb{Z}_7[x]$. Find q and r in $\mathbb{Z}_7[x]$ with $\deg r < \deg g$ such that $f = gq + r$.

Solution: Make a multiplication table for $\mathbb{Z}_7$, then use long division:

$$\begin{array}{r} 4x^2 + 3x + 6 \\ 3x^2+2x+1 \overline{\big) \; 5x^4 + 3x^3 + 0x^2 + 0x + 1} \\ \underline{5x^4 + \;x^3 + 4x^2} \qquad\qquad \\ 2x^3 + 3x^2 + 0x \qquad \\ \underline{2x^3 + 6x^2 + 3x} \qquad \\ 4x^2 + 4x + 1 \\ \underline{4x^2 + 5x + 6} \\ 6x + 2 \end{array}$$

We find $q = 4x^2 + 3x + 6$ and $r = 6x + 2$.

(b) Find a monic polynomial of degree 2 with 4 roots in $\mathbb{Z}_{10}$.

Solution: In $\mathbb{Z}_{10}$ we have $2 \times 5 = 4 \times 5 = 6 \times 5 = 8 \times 5 = 0$, so the polynomial $f = x(x+3)$ will have 4 roots (namely 0 and 7=-3 and also 2 and 5). Other such functions are given by $f = (x+a)(x+a+3)$ and also by $f = (x+a)(x+a+1)$, where $a \in \mathbb{Z}_{10}$.

2: (a) List all the irreducible polynomials of degree less than 4 in $\mathbb{Z}_2[x]$.

Solution: The linear polynomials x and $x+1$ are both irreducible. The reducible quadratic polynomials are all products of two linear factors; x^2, $x(x+1) = x^2 + x$ and $(x+1)^2 = x^2 + 1$. The other quadratic polynomial $x^2 + x + 1$ is irreducible. Each reducible cubic polynomial is either a product of 3 linear factors, or the product of a linear factor with the irreducible quadratic $x^2 + x + 1$; so the reducible cubics are x^3, $x^2(x+1) = x^3 + x^2$, $x(x+1)^2 = x^3 + x$, $(x+1)^3 = x^3 + x^2 + x + 1$, $x(x^2+x+1) = x^3 + x^2 + x$ and $(x+1)(x^2+x+1) = x^3 + 1$. The other 2 cubics, $x^3 + x + 1$ and $x^3 + x^2 + 1$ are irreducible.

(b) Determine the number of irreducible polynomials of degree 4 in $\mathbb{Z}_2[x]$.

Solution: The reducible quartic polynomials may be factored in one of the following ways; 5 of the reducible quartics factor into 4 linear factors (namely x^4, $x^3(x+1)$, $x^2(x+1)^2$, $x(x+1)^3$ and $(x+1)^4$); 3 of them factor into 2 linear factors and 1 irreducible quadratic factor (namely $x^2(x^2+x+1)$, $x(x+1)(x^2+x+1)$ and $(x+1)(x^2+x+1)$); 4 of them factor into 1 linear factor and one irreducible cubic factors (namely $x(x^3+x+1)$, $x(x^3+x^2+1)$, $(x+1)(x^3+x+1)$ and $(x+1)(X^3+x^2+1)$); and 1 of them factors into 2 irreducible quadratic factors (namely $(x^2+x+1)^2$). Thus there are $5+3+4+1 = 13$ reducible quartics, and so there are $16 - 13 = 3$ irreducible quartics. (If you *do* list them, you will find that the irreducible quartics are $x^4 + x + 1$, $x^4 + x^3 + 1$ and $x^4 + x^3 + x^2 + x + 1$).

Alternate Solution: If f is irreducible then f has no roots, so $f(0) \neq 0$ and $f(1) \neq 0$. Since $f(0) = 1$, the constant coefficient of f is 1, so $f = x^4 + ax^3 + bx^2 + cx + 1$ for some $a, b, c \in \mathbb{Z}_2$. Since $f(1) = 1$ we have $1 + a + b + c + 1 = 1$ so $c = a + b + 1$. There are 4 ways to choose a and b in $\mathbb{Z}_2$, so there are 4 polynomials f with no roots hence no linear factors (namely $x^4 + x + 1$, $x^4 + x^2 + 1$, $x^4 + x^3 + 1$ and $x^4 + x^3 + x^2 + x + 1$). Of these 4, the only reducible one is $(x^2 + x + 1)^2 = x^4 + x^2 + 1$.

(c) Determine the number of irreducible polynomials of degree 2 in $\mathbb{Z}_p[x]$ where p is prime.

Solution: In $\mathbb{Z}_p[x]$ there are p monic linear polynomials (namely $x - a$, $a \in \mathbb{Z}_p$). The reducible monic quadratics have 2 linear factors; there are p of these with a repeated factor (namely $(x-a)^2$, $a \in \mathbb{Z}_p$) and there are $\binom{p}{2} = \frac{p(p-1)}{2}$ with two distinct linear factors (namely $(x-a)(x-b)$, $a \neq b \in \mathbb{Z}_p$). Thus there are $p + \frac{p(p-1)}{2} = \frac{p(p+1)}{2}$ reducible monic quadratics. Altogether, there are p^2 monic quadratics, and so we have $p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}$ irreducible monic quadratics. We can multiply any of these by a unit, and in $\mathbb{Z}_p$ there are $p-1$ units, so we obtain $\frac{p(p-1)^2}{2}$ irreducible quadratics.

3: Determine which of the following polynomials are irreducible in $\mathbb{Q}[x]$.

(a) $x^5 + 9x^4 + 12x^2 + 6$

Solution: This is irreducible by Eisenstein's criterion (with $p = 3$).

(b) $x^4 + x + 1$

Solution: This is irreducible, since it is irreducible in $\mathbb{Z}_2[x]$.

(c) $x^4 + 3x^2 + 3$

Solution: The only possible roots in $\mathbb{Q}$ are ± 1 and ± 3. These are not roots, so there are no linear factors. If it is reducible, then it must have 2 monic quadratic factors in $\mathbb{Z}[x]$. Say $x^4+3x^2+3 = (x^2+ax+b)(x^2+cx+d) = x^4+(a+c)x^3+(d+ac+b)x^2+(ad+bc)+bd$. Equating coefficients we find that $a+c = 0$ (1), $b+ac+d = 3$ (2), $ad+bc = 0$ (3) and $bd = 3$ (4). From equation (1) we have $c = -a$. Put this in equation (3) to get $a(d-b) = 0$. We cannot have $d = b$ (equation (4) would imply $b = d = \pm\sqrt{3} \notin \mathbb{Z}$), so we must have $a = 0$. So c is also 0, and equation (2) becomes $b+d = 3$. We cannot have $b+d = 3$ and $bd = 3$ for $b, d \in \mathbb{Z}$, and so x^4+3x^2+3 is irreducible over $\mathbb{Q}[x]$. (We remark that $x^4+3x+3 = (x^2+\sqrt{2\sqrt{3}-3}x+\sqrt{3})(x^2-\sqrt{2\sqrt{3}-3}x+\sqrt{3}) \in \mathbb{R}[x]$).

(d) $x^5 + 5x^2 + 1$

Solution: Let $f = x^5 + 5x^2 + 1$. In $\mathbb{Z}_2[x]$ we have $f = x^5 + 5x^2 + 1$. Since $f(0) = 1$ and $f(1) = 1$, f has no roots and hence no linear factors. If f is reducible in $\mathbb{Z}_2[x]$ then it must factor into an irreducible quadratic factor and an irreducible cubic factor. From question 3, the only possibilities are $(x^2 + x + 1)(x^3 + x + 1)$ and $(x^2 + x + 1)(x^3 + x^2 + 1)$. Neither of these is equal to f, so f is irreducible in $\mathbb{Z}_2[x]$ hence also in $\mathbb{Z}[x]$ and in $\mathbb{Q}[x]$.

4: Factor each of the following polynomials into irreducible factors.

(a) $f = 4x^4 + x^3 - 3x^2 + 4x - 3 \in \mathbb{Q}[x]$

Solution: The only possible rational roots are ± 1, $\pm\frac{1}{2}$, $\pm\frac{1}{4}$, ± 3, $\pm\frac{3}{2}$ and $\pm\frac{3}{4}$. By trying some of these (sketching a graph helps to see where the roots are) we find $f(\frac{3}{4} = 0$. Using long division, we obtain $f = (4x - 3)(x^3 + x^2 + 1)$. The only possible rational roots of $g = x^3 + x^2 + 1$ are ± 1, and these are not roots, so g is irreducible.

(b) $f = x^4 + x^3 + 3x^2 + 2x + 2 \in \mathbb{Q}[x]$

Solution: The only possible roots are ± 1 and ± 2. These are not roots, so f has no linear factors. If f is reducible then it must factor into 2 irreducible monic quadratics in $\mathbb{Z}[x]$. Say $f = (x^2 + ax + b)(x^2 + cx + d)$. Expand and equate coefficients and solve the resulting 4 equations (as in 6.c) to find that $f = (x^2 + x + 1)(x^2 + 2)$.

(c) $f = x^3 + 2x^2 + 2x + 1 \in \mathbb{Z}_7$

Solution: We have $f(0) = 1$, $f(1) = 6$, $f(2) = 0$, $f(3) = 6$, $f(4) = 0$, $f(5) = 4$ and $f(6) = 0$. Thus $f = (x - 2)(x - 4)(x - 6) = (x + 5)(x + 3)(x + 1)$.

5: Find an irreducible polynomial in $\mathbb{Z}[x]$ which is reducible over $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$ and $\mathbb{Z}_7$.

Solution: A nice easy example is $x^2 + 2 \cdot 3 \cdot 5 \cdot 7 = x^2 + 210$.