MAT 3343, APPLIED ALGEBRA, FALL 2003

Answers to Problem Set 5

Peter Selinger

Problem 1. In $\mathbb{Z}_{10}$, we calculate: $p(0) = 8$, $p(1) = 0$, $p(2) = 4$, $p(3) = 0$, $p(4) = 8$, $p(5) = 8$, $p(6) = 0$, $p(7) = 4$, $p(8) = 0$, $p(9) = 8$. Thus, there are 4 roots. This does not contradict the root theorem, because $\mathbb{Z}_{10}$ is not a field.

Problem 2. (a) First note that $p(x)$ is not a unit nor zero; thus, it is either irreducible or reducible. $p(x)$ has a root iff it has a linear factor. Clearly, if $p(x)$ has a linear factor, it is reducible. Conversely, if $p(x)$ is reducible, then one of its factors must be of degree 1, since $p(x)$, as a third-degree polynomial, cannot have two factors of degree 2.

(b) Let $F = \mathbb{R}$, the field of real numbers. Let $q(x) = (x^2 + 1)(x^2 + 2)$. Clearly, $q(x)$ is reducible; on the other hand, $q(x) > 0$ for all $x \in \mathbb{R}$, thus q has no roots in $\mathbb{R}$.

Problem 3. We use the Euclidean Algorithm in the Euclidean ring $\mathbb{Z}_2[x]$. By repeated long division (details not shown), we find that

$$
\begin{array}{llll}
 & \text{quotient:} & & \text{remainder:} \\
x^8 + x^7 + x^5 + x^3 + x^2 + x + 1 & & & \\
\quad = \ (x^7 + x^6 + x^4 + x^3 + 1) & (x) & + & (x^4 + x^3 + x^2 + 1) \\
 & & & \\
x^7 + x^6 + x^4 + x^3 + 1 & & & \\
\quad = \ (x^4 + x^3 + x^2 + 1) & (x^3 + x) & + & (x^3 + x + 1) \\
 & & & \\
x^4 + x^3 + x^2 + 1 & & & \\
\quad = \ (x^3 + x + 1) & (x + 1) & + & 0
\end{array}
$$

Thus the gcd is $x^3 + x + 1$.

Problem 4. (a) The irreducible polynomials of degree up to 4 in $\mathbb{Z}_2$ were given in class. They are:

linear:	$x, \quad x + 1$
quadratic:	$x^2 + x + 1$
cubic:	$x^3 + x^2 + 1, \quad x^3 + x + 1$
quartic:	$x^4 + x^3 + x^2 + x + 1, \quad x^4 + x^3 + 1, \quad x^4 + x + 1$

An irreducible polynomial of degree 5 must have highest and lowest coefficient 1, so it must be of the form $x^5 + ax^4 + bx^3 + cx^2 + dx + 1$. Moreover, it must have an odd number of non-zero coefficients (or else $x + 1$ will be a factor). This leaves 8 possibilities. Of these 8 possible choices, 2 are divisible by $x^2 + x + 1$. The remaining ones are irreducible:

$$
\begin{array}{lll}
x^5 + x^4 + x^3 + x^2 + 1, & x^5 + x^4 + x^3 + x + 1, & x^5 + x^4 + x^2 + x + 1, \\
x^5 + x^3 + x^2 + x + 1, & x^5 + x^3 + 1, & x^5 + x^2 + 1,
\end{array}
$$

(b) We check whether any of the polynomials from (a) are factors of $p(x) = x^{12} + x^{10} + x^7 + x^6 + 1$:

Degree 1: x and $x + 1$ are not factors, because neither 0 nor 1 is a root of $p(x)$.

Degree 2: The only irreducible quadratic polynomial in $\mathbb{Z}_2[x]$, $x^2 + x + 1$, is not a factor (the remainder of the division is 1).

Degree 3: Of the two irreducible polynomials of degree 3, only $x^3 + x^2 + 1$ and $x^3 + x + 1$ is a factor of $p(x)$, with quotient $q(x) = x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + 1$. The quotient $q(x)$ has no more factors of degree 3.

Degree 4: Of the three irreducible polynomials of degree 4, only $x^4 + x^3 + 1$ is a factor of $q(x)$, with quotient $q'(x) = x^5 + x^2 + 1$. The quotient is irreducible.

We therefore obtain $p(x) = (x^5 + x^2 + 1)(x^4 + x^3 + 1)(x^3 + x^2 + 1)$.

Problem 5. (a) In $\mathbb{Q}[x]$, the polynomial $p(x) = x^5 - 1$ has a root $x = 1$, so $x - 1$ is a factor. We have $p(x) = (x - 1)(x^4 + x^3 + x^2 + x + 1)$. Let $q(x) = x^4 + x^3 + x^2 + x + 1$. Then $q(x)$ is a cyclotonic polynomial; by a theorem proved in class, $q(x)$ is irreducible in $\mathbb{Q}[x]$. [Recall the proof: Let $y + 1 = x$, then

$$
\begin{array}{rcl}
q(y+1) & = & ((y+1)^5 - 1)/(y + 1 - 1) \\
 & = & (y^5 + 5y^4 + 10y^3 + 10y^2 + 5y + 1 - 1)/y \\
 & = & y^4 + 5y^3 + 10y^2 + 10y + 5.
\end{array}
$$

Then $q(y + 1)$ is irreducible in $\mathbb{Q}[y]$ by Eisenstein's criterion (with $p = 5$). It follows that $q(x)$ is irreducible in $\mathbb{Q}[x]$.]

(b) In $\mathbb{Z}_2[x]$, the polynomial $p(x) = x^5 + 1$ has a root $x = 1$, and thus $p(x) = (x+1)(x^4+x^3+x^2+x+1)$. The polynomial $q(x) = x^4+x^3+x^2+x+1$ has no roots, and therefore it has no linear factors. So if $q(x)$ was reducible, it would have to have a quadratic factor; the only irreducible quadratic is $x^2 + x + 1$, which is not a factor of $q(x)$, thus $q(x)$ is irreducible.

(c) if $\mathbb{Z}_5[x]$, the polynomial $p(x) = x^4 + 1$ has no roots ($p(0) = 1$, $p(1) = 2$, $p(2) = 2$, $p(3) = 2$, $p(4) = 2$). Thus it has no linear factor. However, y^2+1 has roots $y = \pm 2$, thus $y^2+1 = (y+2)(y-2)$. It follows, by letting $y = x^2$, that $x^4 + 1 = (x^2 + 2)(x^2 - 2)$.

(d) The polynomial $p(x) = 2x^3 + x^2 + 4x + 2$ in $\mathbb{Q}[x]$, if reducible, must have a linear factor (since $\deg p = 3$). By the rational roots theorem, the only possible roots are of the form r/s, where $r|2$ and $s|2$. This leaves as possible roots $x = \pm 1/2, \pm 1, \pm 2$. Of these, we find that only $x = -1/2$ is a root. We have $p(x) = (x + 1/2)(2x^2 + 4) = (2x + 1)(x^2 + 2)$. Since $x^2 + 2$ has no more rational roots, it is irreducible.

(e) In $\mathbb{Q}[x]$, the polynomial $p(x) = x^4 - 9x + 3$ is irreducible by Eisenstein's criterion, with $p = 3$.

(f) The polynomial $p(x) = x^8 - 16$ has no rational roots; in fact, its only real roots are $\pm\sqrt{2}$. The complex roots of $p(x)$ lie on a circle of radius $\sqrt{2}$; they are $\sqrt{2}e^{2\pi i\theta/8}$, where $\theta = 0, 1, 2, \ldots, 7$. Or concretely, these roots are $\pm\sqrt{2}$, $\pm i\sqrt{2}$, $1 \pm i$, $-1 \pm i$. We know that each conjugate pair of complex linear factors determines a real quadratic factor, so $p(x)$ factors into irreducible factors over $\mathbb{R}[x]$ as $p(x) = (x+\sqrt{2})(x-\sqrt{2})(x^2+2)(x^2+2x+2)(x^2-2x+2)$. Only the first two factors are not rational; they combine to a rational factor $(x^2 - 2)$. So we have $p(x) = (x^2 - 2)(x^2 + 2)(x^2 + 2x + 2)(x^2 - 2x + 2)$. These four factors are irreducible over $\mathbb{Q}[x]$ (because their roots, as we saw, are irrational, or also by Eisenstein's criterion).

Problem 6. Over $\mathbb{Z}_5$, a quadradic polynomial $x^2 + ax + b$ is reducible iff it is of the form $(x + c)(x + d)$, for some $c, d \in \mathbb{Z}_5$. Here, the order of c, d does not matter, so there are 15 possibilities for c, d:

c	d	$(x+c)(x+d)$	c	d	$(x+c)(x+d)$	c	d	$(x+c)(x+d)$
0	0	x^2+0x+0	1	1	x^2+2x+1	2	3	x^2+0x+1
0	1	x^2+1x+0	1	2	x^2+3x+2	2	4	x^2+1x+3
0	2	x^2+2x+0	1	3	x^2+4x+3	3	3	x^2+1x+4
0	3	x^2+3x+0	1	4	x^2+0x+4	3	4	x^2+2x+2
0	4	x^2+4x+0	2	2	x^2+4x+4	4	4	x^2+3x+1

Thus these 15 polynomials are reducible. The 10 remaining ones are irreducible:

$$\begin{array}{lllll} x^2+2 & x^2+x+1 & x^2+2x+3 & x^2+3x+3 & x^2+4x+1 \\ x^2+3 & x^2+x+2 & x^2+2x+4 & x^2+3x+4 & x^2+4x+2 \end{array}$$

Problem 7. (a) $x^3 + x^2 + x + 1 = (x^2 + 1)(x + 1)$: not irreducible in $\mathbb{Q}[x]$.

(b) $3x^8 - 4x^6 + 8x^5 - 10x + 6$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion, with $p = 2$.

(c) $x^4 + x^2 - 6$. Note that $y^2 + y - 6$ has roots $y = 2$ and $y = -3$, thus $y^2 + y - 6 = (y + 3)(y - 2)$, thus $x^4 + x^2 - 6 = (x^2 + 3)(x^2 - 2)$. Thus not irreducible in $\mathbb{Q}[x]$.

(d) $p(x) = 4x^3+3x^2+x+1$ has no roots in $\mathbb{Z}_5[x]$, because $p(0) = 1$, $p(1) = 4$, $p(2) = 2$, $p(3) = 4$, $p(4) = 4$. Therefore it has no linear factors. Since $p(x)$ is of degree 3, it must be irreducible.

Problem 8. (a) $a = \sqrt{2}/\sqrt[3]{5}$. We find that $a^6 = 8/25$, hence a is a root of $x^6 - 8/25$, or of $25x^6 - 8$. By Eisenstein's criterion with $p = 2$, this is irreducible in $\mathbb{Q}[x]$, hence it has no rational root. Therefore a is irrational.

(b) $a = \sqrt{2} + \sqrt{3}$. We find that $a^2 = 2 + 2\sqrt{6} + 3$, therefore $a^2 - 5 = 2\sqrt{6}$. Squaring again, we get $(a^2 - 5)^2 = 24$, or $a^4 - 10a^2 + 25 = 24$. Therefore, a is a root of $x^4 - 10x^2 + 1$. By the rational roots theorem, the only possible rational roots are ± 1; however, these are not actually roots. Thus, $x^4 - 10x^2 + 1$ has no rational roots. This proves that a is irrational.

Problem 9. Let $p(x) = 3x^3 + 4x^2 - x - 2$. By the rational roots theorem, all possible rational roots of $p(x)$ are of the form r/s, where $r|2$ and $s|3$. Thus, $r = \pm 1, \pm 2$ and $s = \pm 1, \pm 3$. This leaves eight potential rational roots: ± 1, ± 2, $\pm 1/3$, $\pm 2/3$. Of these, we find that only $2/3$ and -1 are actual roots. [In fact, $p(x) = (3x - 2)(x + 1)(x + 1)$.]