MATH 258: Homework #6

Jesse Farmer

16 February 2005

1. *Let K be a field and $f \in K[x]$ where* $\deg f$ *is* 2 *or* 3. *Show that f is irreducible if and only if f has no root in K.*

   We will show instead that f is reducible if and only if it has a root.

   Lemma 1. *Let F be a field and let $p(x) \in F[x]$. p has a factor of degree one if and only if there exists some $\alpha \in F$ such that $p(\alpha) = 0$.*

   Proof. If $p(x)$ has a factor of degree one then there exists some $\alpha \in F$ such that $p(x) = q(x)(x - \alpha)$ for some $q(x) \in F[x]$. The factor may be assume to be monic since F is a field. But then $p(\alpha) = 0$. Similarly, $F[x]$ is a Eudlidean domain, so there exists some constant r such that $p(x) = q(x)(x-\alpha)+r$ for any $\alpha \in F$. If $p(\alpha) = 0$ then $r = 0$ and hence $x - \alpha$ is just such a factor. □

   A polynomial of degree 2 or 3 is reducible if and only if it has a linear factor since the only pairs of positive integers which add to 2 and 3 are $1, 1$ and $1, 2$. Hence such a polynomial is reducible if and only if it has a root by the above lemma.

2. *Prove or disprove that $x^4 + 4$ is irreducible in $\mathbb{Q}[x]$ and $\mathbb{R}[x]$.*

   $x^4 + 4 = (x^2 + 2x + 2)(x^2 + 2x - 2)$, so it is reducible in both $\mathbb{Q}[x]$ and $\mathbb{R}[x]$.

3. *Let $A = \mathbb{Z}[\sqrt{-5}]$.*

   (a) *Show that the field of fractions of A is $\mathbb{Q}[\sqrt{-5}]$.*
   Denote the field of fractions of A by A'. Let $p/q + r/s\sqrt{-5} \in \mathbb{Q}[\sqrt{-5}]$. Then

   $$\frac{p}{q} + \frac{r}{s}\sqrt{-5} = \frac{sp + qr\sqrt{-5}}{qs} \in A'$$

   To see the other direction let $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$. Then

   $$\frac{\alpha}{\beta} = (a + b\sqrt{-5})\frac{c - d\sqrt{-5}}{c^2 + 5d^2} = \frac{ac + 5bd + (bc - ad)\sqrt{-5}}{c^2 + 5d^2} = \frac{ac + 5bd}{c^2 + 5d^2} + \frac{bc - ad}{c^2 + 5d^2}\sqrt{-5} \in \mathbb{Q}[\sqrt{-5}]$$

   (b) *Show that the Euclidean norm $N(\alpha) = a^2 + 5b$ for $\alpha = a + b\sqrt{-5} \in A$ is multiplicative.*
   Let $\alpha = a + b\sqrt{-5}$ and $\beta = c + d\sqrt{-5}$. Then

   $$\begin{aligned} N(\alpha\beta) &= N(ac - 5bd + (ad + bc)\sqrt{-5}) \\ &= (ac - 5bd)^2 + 5(ad + bc)^2 \\ &= a^2c^2 + 25b^2d^2 + 5b^2c^2 + 5a^2d^2 + 10abcd - 10abcd \\ &= (a^2 + 5b^2)(c^2 + 5d^2) \\ &= N(\alpha)N(\beta) \end{aligned}$$

(c) *Show that $\alpha \in A$ is a unit if and only if $N(\alpha) = 1$. Deduce that ± 1 are the only units of A.*

If α is a unit then there exists some $\beta \in A$ such that $\alpha\beta = 1$, but then $N(\alpha)N(\beta) = 1$. Since the associated field norm on $\mathbb{Z}[\sqrt{-5}]$ is always positive, it follows that $N(\alpha) = 1$. Similarly, if $N(\alpha) = 1$ then define $\beta = a - b\sqrt{-5}$ where $\alpha = a + b\sqrt{5}$. Then $\alpha\beta = a^2 + 5b^2 = 1$.

Both ± 1 are units, so let $a + b\sqrt{-5}$ be a unit in A. Then $a^2 + 5b^2 = 1$. But then $b = 0$ since if $|b| > 0$, $a^2 + 5b^2 > 1$. Then $a^2 = 1$, which implies $a = \pm 1$.

(d) *Show that 2 is irreducible but not prime in A. Conclude that A neither a UFD or a PID.*

Every PID is a UFD, so if A is not a UFD then it is not a PID. 2 is not prime since it divides $(3+\sqrt{-5})(3-\sqrt{-5}) = 14$, but divides neither of the elements on the left-hand side. 2 is irreducible since if $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ then

$$4 = N(2) = N(a + b\sqrt{-5})(c + d\sqrt{-5}) = a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2$$

Hence $(ac)^2 = 4$ and $ac = \pm 2$. From the properties of the integers this implies that $a = \pm 2$ or $c = \pm 1$, or vice versa, and hence one of the factors must be a unit, i.e., 2 is irreducible. In a UFD an element if prime if and only if it is irreducible, but since 2 is irreducible and not prime A cannot be a UFD.

4. *Let $\mathbb{Z}_p$ denote the field $\mathbb{Z}/p\mathbb{Z}$, where p is a prime integer. Write down all irreducible polynomials of degree 2 and degree 3 in $\mathbb{Z}_2[x]$, and all irreducible polynomials of degree 2 in $\mathbb{Z}_3[x]$.*

From above a polynomial of degree two or three over either of these fields is irreducible if and only if it has no roots. Therefore it suffices to find all polynomials that have no roots. In $\mathbb{Z}_2$ these are

$$x^2 + x + 1, x^3 + x + 1, \text{ and } x^3 + x^2 + x + 1$$

Over $\mathbb{Z}_3$ the same principle applies, and the only irreducible polynomials of degree two are

$$x^2 + 1, 2x^2 + 2$$

5. *Let A be a UFD and K its field of fractions. Let $f \in A[x]$ where f is monic and $\alpha \in K$. Show that if $f(\alpha) = 0$ then $\alpha \in A$.*

Let $f(x) = \sum_{k=0}^{n} a_k x^k$ and write $\alpha = \frac{p}{q}$ for appropriate $p, q \in A$ with $\gcd(p, q) = 1$. Since A is a UFD there is a notion of a *gcd*, and, in particular, if $\gcd(p, q) = 1$ and $p \mid qa$ for some $a \in A$, then $p \mid a$. Assume $f(\alpha) = 0$, then since $a_n = 1$ (f is monic),

$$\sum_{k=0}^{n} a_k (p/q)^k = 0 \Rightarrow p^n = q \sum_{k=0}^{n-1} q^{n-k-1} a_k$$

So $q \mid p$, but by hypothesis $\gcd(p, q) = 1$, so $q = 1$ and $p \in A$.

6. *Let K be a field and $A = K[x_1, x_2]$. Show that $a_1x_1 + a_2x_2 \in A$ with $(a_1, a_2) \neq (0, 0)$ is prime in A.*

7. *Show that $x^2 - y^5$ is irreducible in $K[x, y]$ where K is a field.*

Consider $f(x) = x^2 - y^5$ as a polynomial over $K[y]$, and note that $K[x, y]$ is a UFD since K is a field. If f were reducible then f would have a root since f is of degree 2. Assume there exist some $a + by \in K[y]$ that is a root of f, then

$$0 = f(a + by) = (a + by)^2 - y^5 \Rightarrow (a + by)^2 = y^5$$

But this is impossible as the left-hand side has degree 2 and the right-hand side has degree 5. Therefore $x^2 - y^5$ is irreducible over $K[x, y]$.