MATH 258: Homework #5

Jesse Farmer

09 February 2005

1. *Let K be a field an $R = K[x]$. Let $S = \{f \in K[x] \mid f = \sum a_i x_i, a_1 = 0\}$.*

   (a) *Show that S is a subring of R.*

   Any polynomial with $a_i = 0$ for $i > 0$ is in S, so it suffices to show that S is closed under addition and multiplication. Let $f, g \in S$. Then $f + g = \sum(a_i + b_i)x^i$, so if $a_1, b_1 = 0$, then $a_1 + b_1 = 0$. Similarly, $f \cdot g = \sum c_i x_i$ where $c_i = \sum k = 0^i a_k b_{i-k}$. If $i = 1$, then $c_1 = a_0 b_1 + a_1 b_0 = 0$. Therefore S is closed under addition and multiplication, and hence is a subring.

   (b) *Let $I = \{f \in S \mid f(0) = 0\}$. Show that $I = (x^2, x^3)$. Show that S is not a principal ideal domain by showing that I is not a principal ideal.*

   Let $f(x) = \sum_i a_i x^i$. Then $f(0) = 0$, so $f \in I$ if and only if $a_0 = a_1 = 0$. Clearly any element of I is such that $a_0 = a_1 = 0$, since there are no terms of degree less than 2 in the polynomial. To show the converse it suffices to show that any x^i with $i \neq 1$ can be written as $(x^2)^j (x^3)^k$ for some $j, k \in \mathbb{N}$, since then f will be the finite sum of such terms with coefficients in K. So consider x^i. If i is even then we are done since $i = 2k$ and $x^i = (x^2)^k$. So assume i is odd with $i \neq 1$. Then $i = 2k + 1 = 2(k - 1) + 3$ and hence $x^i = (x^2)^{k-1} x^3$. Therefore $I = (x^2, x^3)$.

   To see that the idea is not principal assume for contradiction that there exists some $p \in S$ such that $(p(x)) = (x^2, x^3)$. Then there exist $r, q \in I$ such that $x^2 = q(x)p(x)$ and $x^3 = r(x)p(x)$. Since none of the polynomials are zero, $\deg q + \deg p = 2$, and hence $\deg p = 2$ since it is impossible that $\deg p$ is 1 or 2. Moreover, $\deg r = 1 + \deg q$ since $\deg x^3 = 3$. Then $\deg r = 1$, which is impossible by virtue of being in I. Therefore I cannot be principal.

   (c) *Show that $S = K[x^2, x^3]$.*

   $K[x^2, x^3] = \{\sum a_{ij}(x^2)^i (x^3)^j \mid a_{ij} \in K, i, j \in \mathbb{N}\}$. But, from above, any x^k with $k \neq 1$ can be generated by products of powers of x^2 and x^3, and no product of such powers has a degree of 1 from the fact that there are no positive integral solutions to the equation $2k + 3j = 1$. Therefore $S = K[x^2, x^3]$.

2. *Show that $R = \mathbb{Z}[2i]$ is not a principal ideal domain.*

   From Theorem 14 on pp. 287 it suffices to show that R is not a unique factorization domain. This is obvious since $i \notin R$ and $4 = 2 \cdot 2 = (2i) \cdot (-2i)$, i.e., 4 does not have a unique factorization.

   Alternatively, consider the ideal $(2, 2i) = \{2a + 2bi \mid a, b \in \mathbb{Z}\}$. Assume this ideal were principal, i.e., there exists some $a + 2bi$ such that $(2, 2i) = (a + 2bi)$. Then there would also exist $\alpha, \beta \in R$ with $2 = \alpha(a + 2bi)$ and $2i = \beta(a + 2bi)$. Let N be the associated field norm so that $4 = N(\alpha)(a^2 + 4b^2)$ and $4 = N(\beta)(a^2 + 4b^2)$. Then $a^2 + 4b^2$ must be one of 1, 2, or 4. If it is 4, then $N(\alpha) = N(\beta) = 1$ and $\beta = \pm 1$ and $\alpha = \pm 1$. But clearly this is a contradiction since this implies $2 = \pm 2i$. $a^2 + 4b^2$ cannot be 2 since there are no integral solutions. If $a^2 + 4b^2 = 1$ then $a + 2bi = \pm 1$ and therefore $1 \in (2, 2i)$. Then there exist j, k such that $1 = 2k + 2ij$. Multiplying by $-2i$ shows that i must be a multiple of 2, a contradiction. Therfore $(2, 2i)$ is not principal and R is not a principal ideal domain.

3. *Let $A = \mathbb{Z}[\sqrt{2}]$. Show that A is a Euclidean Domain with norm $\nu : A \to \mathbb{N}$ defined by*

$$\nu(a + b\sqrt{2}) = |a^2 - 2b^2|$$

Recall that a Euclidean Domain A is an integral domain with a Euclidean norm defined such that, for any $\alpha, \beta \in A$ there exist $q, r \in A$ with $\alpha = q\beta + r$ and $N(r) < N(q)$. Let $A = \mathbb{Z}[\sqrt{2}]$ and $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$. Define $N(a + b\sqrt{2}) = |a^2 - 2b^2|$.

Then the above definition is clearly equivalent to the following: For any $\delta \in \mathbb{Q}[\sqrt{2}]$ there exists a $\kappa \in \mathbb{Z}[\sqrt{2}]$ such that $N(\delta - \kappa) < 1$. On $\mathbb{Q}[\sqrt{2}]$ we define N in the obvious way: $N(a/b) = N(a)/N(b) \in \mathbb{Q}$. Letting $\delta = r + s\sqrt{2}$ and $\kappa = x + y\sqrt{2}$, then we must choose x, y such that

$$|(r - x)^2 - 2(s - y)^2| < 1$$

But this is easy to do: simply choose the integers closest to r and s, so that $|r - x| \leq 1/2$ and $|s - y| \leq 1/2$. Incidentally, this works also for any $\mathbb{Z}[\sqrt{m}]$ where $m < 5$, i.e., $\mathbb{Z}[\sqrt{3}]$ is also a Euclidean Domain.

4. *Let $A = \{a + wb \mid a, b \in \mathbb{Z}\}$ where $w = \frac{-1+i\sqrt{3}}{2}$. Show that A is a Euclidean Domain with norm $\nu : A \to \mathbb{N}$ defined by*

$$\nu(a + bw) = a^2 - ab + b^2$$

As above, it is sufficient to find $\kappa \in \mathbb{Z}[w]$ such that for any $\delta \in \mathbb{Q}[w]$ we have $N(\delta - \kappa) < 1$. Letting $\delta = r + sw$ and $\kappa = x + yw$, then

$$N(\delta - \kappa) = (r - x)^2 - (r - x)(s - y) + (s - y)^2$$

Choosing x, y to be the cloest integers to r, s so that $|r - x| \leq 1/2$ and $|s - y| \leq 1/2$ gives the estimate

$$|N(\delta - \kappa)| = |(r - x)^2 - (r - x)(s - y) + (s - y)^2| \leq |r - x|^2 + |r - x||s - y| + |s - y|^2 \leq \frac{3}{4} < 1$$

Therefore N is indeed a Euclidean norm on $\mathbb{Z}[w]$ and $\mathbb{Z}[w]$ is a Euclidean Domain.

5. *Let K be a field and $f \in K[x]$ with $f(x) = \prod_{i=1}^{n}(x - a_i)$ and $a_i \neq a_j$ for $j \neq i$. Show that the map $K[x]/(K[x] \cdot f) \to \underbrace{K \times \cdots \times K}_{n \text{ times}}$ given by $\bar{g} \mapsto (g(a_1), \ldots, g(a_n))$ is a ring isomorphism.*

Let $\varphi(g) = (g(a_1), \ldots, g(a_n))$. We will first show that this is a ring homomorphism with kernel $K[x] \cdot f$, and then that it is surjective, proving the statement. That it is a homomorphism is almost too trivial for words, since

$$\varphi(g) + \varphi(h) = (g(a_1), \ldots, g(a_n)) + (h(a_1), \ldots, h(a_n)) = ((g + h)(a_1), \ldots, (g + h)(a_n)) = \varphi(g + h)$$

and *mutatis mutandis* for multiplication. $g \in \ker \varphi$ if and only if $g(a_i) = 0$ for $1 \leq i \leq n$. But this is equivalent to saying that $x - a_i \mid g$ for each a_i, and hence $f \mid g$. Therefore $\ker \varphi = K[x] \cdot f(x)$.

Showing that this map is surjective is more difficult, and requires (to my knowledge) some linear algebra. We wish to find a function g such that $g(x) = \sum_{i=1}^{n} g_i x^i$ and $g(a_i) = b_i$ for arbitrary $b_i \in K$. But this is equivalent to the following matrix equation

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^n \\ 1 & x_2 & x_2^2 & \cdots & x_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{pmatrix} \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

The determinant of this matrix is known to be $\prod_{i>j}(x_i - x_j)$. In our case, we have $x_i = a_i$ and $a_i \neq a_j$ for $i \neq j$, so that this matrix (the Vandermonde matrix) is nonsingular and our homomorphism is surjective.

6. (a) *Show that the ideal generated by $2, x$ in $\mathbb{Z}[x]$ is not a principal ideal.*

   Assume there exists a nonzero polynomial $p \in \mathbb{Z}[z]$ such that $(p(x)) = (2, x)$. Then there exist nonzero polynomials q_1, q_2 such that $2 = q_1(x)p(x)$ and $x = q_2(x)p(x)$. But then $0 = \deg 2 = \deg q_1 + \deg p$, which implies $\deg p = 0$ and $\deg q_2 = 1$. Then $x = \alpha x$ for some $\alpha \in \mathbb{Z}$ with $\alpha \neq 0$, which is a contradiction. Therefore $(2, x)$ is not a principal ideal.

   (b) *Let K be a field and $A = K[x_1, x_2]$. Show that the ideal generated by x_1, x_2 in A is not a principal ideal.*

   Assume (x_1, x_2) is principal, then there exists some $g \in A$ such that $x_1 = g \cdot a$ and $x_1 = g \cdot b$ for some $a, b \in A$. Since none of these are zero, it follows that the degree of g in x_1 must be at least 1. But then the degree of $x_2 = g \cdot b$ in x_1 must be at least 1, which is absurd.

7. (a) *Show that the ideal generated by $x^2 + 1$ in $\mathbb{R}[x]$ is a prime ideal.*

   By Proposition 11 on pp. 284, a nonzero element of a PID is irreducible if and only if it is prime, and by Proposition 10 on pp. 308 a polynomial of degree two or three over a field F is reducible if and only if it has a root in F. Therefore, since $x^2 + 1$ has no real root, it is irreducible and therefore generates a prime ideal.

   (b) *Decide if the ideal generated by $x^2 + 1$ in $\mathbb{C}[x]$ is a prime ideal.*

   $x^2 + 1$ is reducible in $\mathbb{C}[x]$ by $x^2 + 1 = (x - i)(x + i)$. By Proposition 10 on pp. 284, $(x^2 + 1)$ therefore is not a prime ideal.

8. *Let K be a field and $A = K[x, y]$. For $a, b \in K$ consider the ideal $M = A \cdot (x - a) + A \cdot (y - b)$. Show that M is a maximal ideal.*

   Consider the map $\varphi : A \to K$ defined by $\varphi(f) = f(a, b)$. This map is surjective since $f(x, y) = a$ maps to $a \in K$ for arbitrary a. Clearly $M \subset \ker \varphi$, so let $f \in \ker \varphi$. Then there exists a $g \in K[x, y]$ and constant r such that $f(x, y) = g(x, y)(x - a) + r(x, y)$. Apply this again to $r(x, y)$, and we see that there exists a $h \in K[x, y]$ and constant r' such that

$$f(x, y) = g(x, y)(x - a) + h(x, y)(x - b) + r'(x, y)$$

   Since $f(a, b) = 0$, $r = 0$, and therefore $f \in \ker \varphi$ and $M = \ker \varphi$. By the first isomorphism theorm for rings, $A/M \cong K$, and hence M is maximal in A.