MATH 258: Homework #7

Jesse Farmer

23 February 2005

1. *Let $R = \mathbb{Z} + x\mathbb{Q}[x] \subset \mathbb{Q}[x]$ be the set of polynomials in x with rational coefficients whose constant terms is an integer.*

   (a) *Prove that R is an integral domain and its units are ± 1.*

   R is a subring of $\mathbb{Q}[x]$ since the constant term in the product of any two polynomials is the product of their constant terms, the constant term in the sum of any two polynomials is the sum of their constant terms, and $\mathbb{Z}$ itself is a ring. Hence R is an integral domain, since a subring of an integral domain is itself an integral domain.

   If f is a unit and g its inverse in R then we can write $f(x)g(x) = \sum c_k x^k = 1$ where $c_k = \sum a_i b_{k_0}$ and a_k, b_k are the coefficients of f and g, respectively. Since R is an integral domain this implies that $a_k = b_k = 0$ for all $k > 0$, and $c_0 = a_0 b_0$, hence $a_0 b_0 = 1$ and $a_0 = \pm 1$. But then $f(x) = \pm 1$.

   (b) *Show that the irreducibles in R are $\pm p$ where p is a prime in $\mathbb{Z}$ and the polynomials $f(x)$ that are irreducible in $\mathbb{Q}[x]$ and have constant terms ± 1. Prove that these irreducibles are prime in R.*

   To prove the contrapositive assume that $f \in R$ is such that its constant term is composite. Then f can be written as the the product of primes, which are irreducible, and a polynomial in $\pm 1 + x\mathbb{Q}[x]$. Call this polynomial $a(x)$. If it is irreducible then we are done, so assume that $a(x)$ is reducible. Then in any factorization, its factors must have constant terms of ± 1 since its constant term is the product of the constant terms of its factors. This process will repeat until an irreducible polynomial (perhaps of degree one) is reached that has a constant term of ± 1. Hence f is reducible.

   (c) *Show that x cannot be written as the product of irreducibles in R and conclude that R is not a UFD.*

   In a UFD only a finite number of irreducibles can divide an element, but $x = \frac{x}{p} \cdot p$ where $p \in \mathbb{Z}$ is prime, and hence irreducible in R. As there are an infinite number of primes, there are an infinite number of irreducibles which divide x, and hence R cannot be a UFD.

   (d) *Show that x is not a prime in R and describe the quotient ring $R/(x)$.*

   $R/(x) = \{a + \frac{b}{x} \mid a \in \mathbb{Z}, b \in \mathbb{Q}, 0 < b < 1\}$ since $nx \in (x)$ but $x/n \notin (x)$ for all $n \in \mathbb{Z}$. To see that (x) is not prime, note that $(x/n)(x/n) = x^2/n^2 = (x/n^2)x = 0$, but $x/n \neq 0$. Hence $R/(x)$ is not an integral domain and (x) is not a prime ideal.

2. *Show that the polynomial $(x-1)(x-2)\cdots(x-n) - 1$ is irreducible over $\mathbb{Z}$ for all $n \geq 1$.*

   Denote this polynomial by f and assume it is reducible with $f = gh$. Then at each $k = 1, \ldots, n$ we have $f(k) = g(k)h(k) = -1$, which implies that whenever one is ± 1 the other is ∓ 1 at k. If neither are constant, then we have a contradiction since a nonconstant polynomial which assumes a value n times must at least be of degree n, so one polynomial must be a constant and another a polynomial of degree n.

3. *Show that the polynomial $(x-1)(x-2)\cdots(x-n) + 1$ is irreducible over $\mathbb{Z}$ for all $n \geq 1$ with $n \neq 4$.*

4. *Prove that* $K_1 = \mathbb{F}_{11}[x]/(x^2+1)$ *and* $K_2 = \mathbb{F}_{11}[y]/(y^2+2y+2)$ *are both fields with* 121 *elements. Prove that the map which sends the element* $p(\bar{x})$ *of* K_1 *to the element* $p(\bar{y}+1)$ *of* K_2 *is well defined and gives a ring isomorphism from* K_1 *to* K_2*.*

   Both polynomials are irreducible and therefore prime in $\mathbb{F}_{11}[x]$ and $\mathbb{F}_{11}[y]$, respectively. It follows that the quotients are finite integral domains, and therefore fields. Every element $\bar{b}$ of K_1 can be written as $b(x) + (x^2+1)\mathbb{F}_{11}[x]$, where b is a polynomial in $\mathbb{F}_{11}$ of at most degree 1. There are precisely 121 of these, counting the 11 possible coefficients in each position. The same applies to K_2, since y^2+2y+2 is also a polynomial of degree 2.

   The above map is well defined since, if $p(x) - q(x) \in (x^2+1)\mathbb{F}_{11}[x]$ then $p(y+1) - q(y+1) \in ((y+1)^2)\mathbb{F}_{11}[y] = (y^2+2y+2)\mathbb{F}_{11}[x]$. Furthermore, this map is obviously a homomorphism from the properties of addition and multiplication on functions (i.e., $(f+g)(x) = f(x)+g(x)$, $(fg)(x) = f(x)g(x)$. That is is an isomorphism follows from the fact that its inverse is simply $p(\bar{y}) \mapsto p(\bar{x}-1)$, since $\bar{1} = 1$.

5. *Let* $f \in \mathbb{Z}[x]$ *be a monic polynomial such that* $f = gh$ *for some* $g, h \in \mathbb{Q}[x]$*. If* f *and* g *are monic polynomials show that* $g, h \in \mathbb{Z}[x]$*.*

   From class there exist $c_1, c_2 \in \mathbb{Q} \setminus \{0\}$ such that $f_1 = c_1 g$, $f_2 = c_2 h$, $f = f_1 f_2$, and $f_1, f_2 \in \mathbb{Z}[x]$, since f is monic and therefore primitive. Also, since g and h are monic, it follows that $c_i = \pm 1$, and hence that $f_1 = \pm g$ and $f_2 = \pm h$, i.e., $g, h \in \mathbb{Z}[x]$.

6. *Let* $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$*. Let* p *be a prime number. Suppose* $\bar{f} = x^n + \bar{a}_{n-1}x^{n-1} + \cdots + \bar{a}_0 \in \mathbb{Z}/p\mathbb{Z}[x]$ *is irreducible. Show that* f *is irreducible in* $\mathbb{Q}[x]$*.*

   We will prove the contrapositive. Suppose f is reducible in $\mathbb{Q}[x]$ with $f = gh$, then $\bar{f} = \bar{g}\bar{h}$ modulo p. This is a factorization since g and h are monic, and hence are monic modulo p.

7. *Let* B *be a commutative ring and* A *a subring of* B*. Let* $h, f \in A[x]$ *and* $g \in B[x]$*. Suppose* f *is a monic polynomial and* $h = gf$*. Show that* $g \in A[x]$ *and deduce that* $fB[x] \cap A[x] = fA[x]$*.*

8. *Let* B *be an integral domain and* A *a subring of* B*. Let* f *be a prime element in* $B[x]$*, where* f *is a monic polynomial in* $A[x]$*. Show that* f *is a prime element in* $A[x]$*.*

   Let P be a prime ideal of B, then by the second ring isomorphism theorem

$$\frac{A+P}{P} \cong \frac{A}{A \cap P}$$

   $A+P$ is a subring of R containing P, so P is also a prime ideal of $A+P$, and hence $\frac{A+P}{P}$ is an integral domain. Therefore $\frac{A}{A \cap P}$ is also an integral domain and $A \cap P$ is a prime ideal of A. From above, $fB[x] \cap A[x] = fA[x]$, and therefore $fA[x]$ is a prime ideal in $A[x]$, i.e., f is prime in $A[x]$.

9. *Prove that* $x^{n-1} + x^{n-2} + \cdots + x + 1$ *is irreducible over* $\mathbb{Z}$ *if and only if* n *is prime.*

   If n is not prime then we can write $n = pq$ for some nontrivial integers p, q strictly less than n. Then

$$x^{n-1} + x^{n-2} + \cdots + 1 = \frac{x^n - 1}{x - 1} = \frac{(x^p)^q - 1}{x - 1} = (x^{p-1} + \cdots + 1)(x^{p(q-1)} + x^{p(q-2)} + \cdots + 1)$$

   so that $x^{n-1} + x^{n-2} + \cdots + x + 1$ is reducible, repeating this process for each prime dividing n.

   Let $f(x) = x^{n-1} + x^{n-2} + \cdots + 1$. We know that

$$f(x) = \frac{x^n - 1}{x - 1}$$

   So consider $xf(x+1)$,

$$xf(x+1) = (x+1)^n - 1 = \sum_{k=1}^{n} \binom{n}{n-k} x^k$$

   From previous homework we know that if n is prime then $n \mid \binom{n}{k}$ for $n \leq p$, and clearly $n^2 \nmid \binom{n}{n-1}$. Hence $f(x+1)$ satisfies Eisentein's criteria, and is therefore irreducible. It follows that $f(x)$ is also irreducible.

10. *Prove that $x^3 + nx + 2$ is irreducible over $\mathbb{Z}$ for all integers $n \neq 1, -3, -5$.*

    This is equivalent to proving that if $x^3 + nx + 2$ is reducible then $n = 1, -3, -5$, so assume $f(x) = x^3 + nx + 2$ is reducible. Since f is monic, reducible, and of degree three it must have a root in $\mathbb{Z}$ which divides 2. That is, if $f(x) = 0$ then $x = \pm 1, \pm 2$. But if $f(x) = 0$ then we can write

    $$n = -\frac{x^3 - 2}{x}$$

    For $x = \pm 1$ and $x = \pm 2$ we get $n = 1, -3, -5$, as desired.

11. *Factor each of the two polynomials $x^8 - 1$ and $x^6 - 1$ into irreducibles over each of the following rings:*

    (a) $\mathbb{Z}$
    Over $\mathbb{Z}$, $x^8 - 1 = (x+1)(x-1)(x^2+1)(x^4+1)$ and $x^6 - 1 = (x+1)(x-1)(x^2-x+1)(x^2+x+1)$.

    (b) $\mathbb{Z}/2\mathbb{Z}$
    Since $\mathbb{Z}/2\mathbb{Z}$ has characteristic 2, $x^8 - 1 = (1+x)^8$ and $x^6 - 1 = (1+x)^2(1+x+x^2)^2$.

    (c) $\mathbb{Z}/3\mathbb{Z}$
    Over $\mathbb{Z}/3\mathbb{Z}$, $x^8 - 1 = (x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2)$ and $x^6 - 1 = (1+x)^3(x+2)^3$.

12. *Let F be a field and let $f \in F[x]$ be of degree n. The polynomial $f(x) = x^n f(1/x)$ is called the* reverse *of $f(x)$.*

    (a) *Describe the coefficients of g in terms of the coefficients of f.*
    Let $f(x) = \sum a_k x^k$ be a polynomial of degree n, then the reverse of f is

    $$x^n f(1/x) = x^n \sum a_k x^{-k} = \sum a_k x^{n-k} = \sum a_{n-k} x^k$$

    If we write $g(x) = \sum b_k x^k$, then $b_k = a_{n-k}$.

    (b) *Prove that f is irreducible if and only if g is irreducible.*
    It is sufficient to prove that if f is reducible then so is g, since the reverse of g is f itself. Let $f = q \cdot r$ where $\deg q = a$ and $\deg s = b$, such that $a + b = n = \deg f$. Then g factors as

    $$g(x) = x^n q(1/x) s(1/x) = x^a q(1/x) \cdot x^b s(1/x)$$

    so that g is also reducible.

13. *Show that $6x^5 + 14x^3 - 21x + 35$ and $18x^5 - 30x^2 + 120x + 360$ are irreducible in $\mathbb{Q}[x]$.*

    Let $p = 7$, then by Eisenstein's criteria the first polynomial is irreducible. Similarly, for the second polynomial, let $p = 5$, then Eisenstein's criteria applies directy to show that it is irreducible. z

14. *Let A be an integral domain. Show that if $A[x]$ is a UFD then so is A.*

    The contrapositive is probably clearer to see. Assume there is some element in $\alpha \in A$ that has two different factorizations. Then α as an element of $A[x]$ can be factored in the same way, so that $A[x]$ is not a UFD either.

15. *Show that $f = z^{10} + xz^8 + yz^7 + y^2z^5 + x^3z + y^2 - x^3$ is irreducible in $K[x, y, z] = R$.*