MAT 3530: Selected Solutions to Assignment 6

Charles Delman

April 10, 2012

1. Here is the lemma to be proven, with the correct hypothesis explicitly stated. I note that commutativity of R is not essential (although usually assumed for convenience, and because it applies in all the usual examples). However, the fact that R is a domain is absolutely essential, and the proof should state where this hypothesis is used.

   Lemma. *Let R be an integral domain. If $P(x) \neq 0$ and $Q(x) \neq 0$ are polynomials in $R[x]$, then deg $P(x)Q(x) =$ deg $P(x)$ + deg $Q(x)$.*

   Proof. Let $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$ and $Q(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$, where neither polynomial is zero. (Note that it is possible that $n = 0$ or $m = 0$, making one or both polynomials constant, but $a_m \neq 0$ and $b_n \neq 0$.) Since $a_m \neq 0$ and $b_n \neq 0$ and the ring of coefficients is a domain, the highest degree term of $P(x)Q(x)$ is $a_mb_nx^{m+n}$ (because the coefficient a_mb_n cannot be zero). Thus $degP(x)Q(x) = m + n = degP(x) + degQ(x)$. □

2. Let R be any commutative ring, and consider R as a subring of the polynomial ring $R[x]$ by identifying its elements with constant polynomials.

   (a) Prove that the group of units of $R[x]$ is the same as the group of units of R. (Hint: Use an argument about the degree of a product to reduce to the constant case.)

   As noted in class, this proposition is untrue as stated. I was surprised that few of you took me up on my offer of extra credit for supplying the hypothesis, which is right in the previous problem! You simply need the lemma of problem 1 to hold, which means that we must assume R is a *domain*, not just "any commutative ring." With this added hypothesis, the reduction to constant polynomials is easy:

   $P(x)Q(x) = 1 \Rightarrow degP(x) + degQ(x) = deg1 = 0$; since degree is non-negative, this is only possible if $degP(x) = degQ(x) = 0$. Thus, $P(x)$ and $Q(x)$ must be constants, that is, elements of the ring of coefficients. (Since $0 \cdot Q(x) = P(x) \cdot 0 = 0 \neq 1$, we can assume neither polynomial is zero and restrict our attention to polynomials whose degree is defined.) Now that we know $P(x)$ and $Q(x)$ are elements of R, if they are units they must be units of R. Conversely, all units of R remain units in the polynomial ring, since multiplication of constants is the same.

   (b) In particular, what are the units of:

   i. $\mathbb{Z}[x]$? By the result of part (a), the units of $\mathbb{Z}[x]$ are the units of $\mathbb{Z}$: ± 1.

   ii. $\mathbb{Q}[x]$? $\mathbb{Q}^* = \{q \in \mathbb{Q} : q \neq 0\}$. (All non-zero rational numbers have multiplicative inverses.)

   iii. $\mathbb{R}[x]$? $\mathbb{R}^* = \{r \in \mathbb{R} : r \neq 0\}$.

   iv. $\mathbb{C}[x]$? $\mathbb{C}^* = \{z \in \mathbb{C} : z \neq 0\}$. (For any $z \neq 0$, $z \cdot \frac{\bar{z}}{|z|} = 1$.)

In what follows it will be helpful to recall that, thanks to unique factorization, any two integers have a *least common multiple*, defined (up to units) in a manner analogous to the greatest common divisor as follows:

Definition. The least common multiple of integers k and l, denoted by $LCM(k,l)$ is the integer m such that:

- m is a common multiple of k and l: $k \mid m$ and $l \mid m$
- m is least in the sense that if $k \mid n$ and $l \mid n$, then $m \mid n$.

It is clear that $LCM(k,l)$ (if it exists) is unique (justifying the anticipatory use of the word "the" above): if m' is another such, then $m \mid m'$ and $m' \mid m$; hence, $m = \pm m'$.

That $LCM(k,l)$ does exist is proven as follows: Using zero exponents as needed, we may write $k = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n}$ and $l = p_1^{f_1} p_2^{f_2} p_3^{f_3} \cdots p_n^{f_n}$, where $p_1, p_2, p_3, \ldots, p_n$ are distinct primes. Let $g_i = MAX(e_i, f_i)$ for $i = 1, 2, 3, \ldots, n$. Then one readily shows that $m = p_1^{g_1} p_2^{g_2} p_3^{g_3} \cdots p_n^{g_n}$ is the least common multiple of k and l.

3. Prove that $m = p_1^{g_1} p_2^{g_2} p_3^{g_3} \cdots p_n^{g_n}$, as defined above, is $LCM(k,l)$.

   Proof. Since $e_i \leq g_i$ for $i = 1, 2, 3, \ldots, n$, each prime in the factorization of k occurs to at least as high a power in the factorization of m. Thus, using commutativity and associativity, we can write $m = (p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_n^{e_n})(p_1^{h_1} p_2^{h_2} p_3^{h_3} \cdots p_n^{h_n}) = k(p_1^{h_1} p_2^{h_2} p_3^{h_3} \cdots p_n^{h_n})$, where $h_i = g_i - e_i \geq 0$ for all $i = 1, 2, 3, \ldots, n$, so $p_1^{h_1} p_2^{h_2} p_3^{h_3} \cdots p_n^{h_n}$ is an integer. Thus, $k \mid m$. The proof that $l \mid m$ is similar.

   If o is any other common multiple of k and l (I avoided using the letter "n", since it has already been used for the number of distinct primes), then by unique factorization all the primes $p_1, p_2, p_3, \ldots, p_n$ must occur in the factorization of o to a power at least as high as occurs in k or l; therefore, they must occur to a power at least as high as $g_i = MAX(e_i, f_i)$ for $i = 1, 2, 3, \ldots, n$. Using commutativity and associativity in a similar manner to that above, we see that $o = p_1^{g_1} p_2^{g_2} p_3^{g_3} \cdots p_n^{g_n} r$, where $r \in \mathbb{Z}$. (The factor r may be divisible by some powers of p_i for some i and also by other primes not in the factorization of k or l.) □

   Remark. An alternative method of proving the existence of the least common multiple is to show that $LCM(k,l) = \frac{kl}{GCD(k,l)}$. *Hint: This would be an excellent final exam question, so you might want to think about it! Other excellent exam questions you might think about would be generalization of the results about the greatest common divisor and least common multiple to finitely many numbers (more than two), using proof by induction.*

Lemma. *The product of primitive polynomials is primitive.*

5. Prove as a consequence of the preceding lemma that content is multiplicative: $c(PQ) = c(P)c(Q)$.

   Proof. Let $P(x)$ and $Q(x)$ be polynomials with integer coefficients. $P(x) = c(P)P'(x)$, where $P'(x)$ is primitive. (The coefficients of $P'(x)$ are relatively prime, since the greatest common divisor of the coefficients of $P(x)$ has already been factored out.) Similarly, $Q(x) = c(Q)Q'(x)$, where $Q'(x)$ is primitive. Since $\mathbb{Z}$ is a commutative ring, and the ring of polynomials over a commutative ring is commutative, we have $P(x)Q(x) = c(P)P'(x)c(Q)Q'(x) = c(P)c(Q)P'(x)Q'(x)$, and since the product of two primitive polynomials is primitive (as shown above), $P'(x)Q'(x)$ is primitive. Thus, the coefficients of $P'(x)Q'(x)$ are relatively prime and $c(P)c(Q)$ must be the greatest common divisor of the coefficients of $P(x)Q(x)$, from which it follows that $c(PQ) = c(P)c(Q)$. □

6. Let F be any field. The following steps prove that given any non-zero polynomial $D(x) \in F[x]$ and any polynomial $E(x) \in F[x]$, there exists polynomials $Q(x) \in F[x]$ and $R(x) \in F[x]$ such that $E(x) = Q(x)D(x) + R(x)$, and either $R(x) = 0$ or $\deg R(x) < \deg D(x)$.

   (a) Special cases: $E(x) = 0$ or $\deg E(x) < \deg D(x)$. In these cases $Q(x) = 0$ and $R(x) = E(x)$.

   (b) General case: $\deg E(x) \geq \deg D(x)$; hence, $E(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n$ and $D(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m$, with $m \leq n$.

Since we will proceed by strong induction, the initial case is unnecessary and we can go straight to the inductive claim:

Inductive claim: Assume the result holds if deg $E(x) < n$. Then it holds if deg $E(x) = n$.

Since $\frac{b_n}{a_m}x^{n-m}D(x)$ has the same highest degree term as $E(x)$, $E(x) - \frac{b_n}{a_m}x^{n-m}D(x)$ has degree strictly less than n. Thus, by inductive hypothesis, $E(x)-\frac{b_n}{a_m}x^{n-m}D(x) = Q'(x)D(x)+R(x)$, with $degR(x) < degD(x)$. It follows by adding $\frac{b_n}{a_m}x^{n-m}D(x)$ to both sides and using the distributive property that $E(x) = \left(\frac{b_n}{a_m}x^{n-m} + Q'(x)\right)D(x) + R(x)$. Setting $Q(x) = \frac{b_n}{a_m}x^{n-m} + Q'(x)$, we obtain the desired result. (Note that it is essential for the ring of coefficients to be a field, because whatever a_m is, we must be able to divide by it.)

7. A real or, more generally, complex number ρ is called *algebraic* if there is a polynomial with integer coefficients, $S(x) \in \mathbb{Z}[x]$, such that $S(\rho) = 0$. (Terminology: ρ is a *root* of S, ρ *satisfies* S.) For example, $\sqrt{2}$ and $i\sqrt{7}$ are algebraic numbers. A number that is not algebraic is called *transcendental*; it can be proven, for example, that e and π are transcendental. (In a sense that can be precisely defined, almost all real or complex numbers are transcendental; however, we only have names for a couple of them!)

   (a) Verify that $\sqrt{2}+i\sqrt{2}$ is algebraic by finding a polynomial in $\mathbb{Z}[x]$ that it satisfies. $\sqrt{2}+i\sqrt{2} = 2e^{\frac{i\pi}{4}}$. $\left(2e^{\frac{i\pi}{4}}\right)^4 = 16e^{i\pi} = -16$, so $(\sqrt{2}+i\sqrt{2})^4 + 16 = 0$.

   (b) Prove that ρ is algebraic if and only if there is a polynomial with rational coefficients, $T(x) \in \mathbb{Q}[x]$, such that $T(\rho) = 0$. (The *only if* direction is obvious, since integers are rational.)

   Proof. If $T(x) \in \mathbb{Q}[x]$, such that $T(\rho) = 0$, then multiplying by the least common denominator of the coefficients of T (or, for that matter, *any* common denominator) yields a polynomial with integer coefficients that clearly has the same roots. □

   (c) If $r \in \mathbb{C}$ is a root of $P(x)$, prove that $P(x) = (x - r)Q(x)$ for some $Q(x) \in \mathbb{C}[x]$.
   Many of you left unstated the important logical step in this proof.

   Proof. Using division with remainder (which works in any polynomial ring with coefficients in a field), we see that $P(x) = (x - r)Q(x) + R$, where R is a constant, since either $R = 0$ or $degR < deg(x - r) = 1$ (and hence $degR = 0$). Now, evaluating each side at $x = r$, we obtain $0 = P(r) = (r - r)Q(r) + R = 0 \cdot Q(r) + R = 0 + R = R$; hence, $R = 0$, so $P(x) = (x - r)Q(x)$. □

   (d) Let $P(x) \in \mathbb{Z}[x]$ be the primitive polynomial *of lowest degree* such that $P(r) = 0$. Let $S(x)$ be any primitive polynomial such that $S(r) = 0$. Prove that there is a primitive polynomial $Q(x) \in \mathbb{Z}[x]$ such that $S(x) = P(x)Q(x)$; in particular, $P(x) \mid S(x)$ in the ring $\mathbb{Z}[x]$.

   Proof. Using division with remainder in $\mathbb{Q}(x)$ (we cannot restrict ourselves to polynomials with integer coefficients, since we must be able to divide by any non-zero coefficient to guarantee that division with remainder works), we obtain $S(x) = P(x)Q'(x) + R(x)$, where $Q'(x)$ and $R(x)$ are polynomials with rational coefficients, and either $R(x) = 0$ or $degR(x) < degP(x)$. (Here is where it is crucial that $P(x)$ is a polynomial of *lowest degree* such that $P(r) = 0$. The fact that $P(x)$ is required to be primitive does not affect its degree: there is no non-primitive polynomial of lower degree such that $P(r) = 0$, since if there were, factoring out its content would yield a primitive polynomial of the same degree having the same roots. Nor does restricting to integer coefficients affect the lowest degree, since if there were a polynomial with rational coefficients with lower degree having r as a root, multiplying by a common denominator would yield a polynomial with integer coefficients having the same roots.) Evaluating each side of the equation at $x = r$ we obtain $0 = S(r) = P(r)Q'(r) + R(r) = 0 \cdot Q'(r) + R(r) = 0 + R(r) = R(r)$; hence, $R(r) = 0$. Since $P(x)$ is by hypothesis a polynomial of lowest degree having r as a root, it is not possible

that $degR(x) < degP(x)$; hence, $R(x) = 0$. Thus, $S(x) = P(x)Q'(x)$; however, we are not finished, because $Q'(x)$ might not have integer coefficients.

Let a be the lowest common denominator of the coefficients of $Q'(x)$. Multiplying both side by a we obtain $aS(x) = P(x)Q''(x)$, where $Q''(x) \in \mathbb{Z}[x]$; however, we are still not finished, because $Q''(x)$ need not be primitive (and, in fact, if $a \neq 1$, it isn't).

Since $S(x)$ is primitive by hypothesis, the content of aS, and hence of PQ'', is a. Since $P(x)$ is primitive, and $c(PQ'') = c(P)c(Q'') = 1 \cdot c(Q)$, $c(Q'') = a$ as well. Thus, $Q''(x) = aQ(x)$, where $Q(x)$ *is* (finally) primitive! We now have $aS(x) = aP(x)Q(x)$ in $\mathbb{Z}[x]$, and since $\mathbb{Z}[x]$ is an integral domain, we can cancel the factors of a to obtain $S(x) = P(x)Q(x)$, with $Q(x)$ primitive, as desired. □

This was admittedly a rather long and challenging problem, but I hope you can see that if you break it down logically into manageable steps you can handle it.

The significance of the results of the last few problems is that, in order to use the powerful tool division with remainder, we must consider polynomials with rational coefficients, rather than strictly integer coefficients. However, we have shown that all of the results about roots and factors in the rational context "descend" (that is, carry over when we go back "down" to having only integer coefficients) to polynomials with integer coefficients.

We have seen that the existence of division with remainder makes $F[x]$ into a *Euclidean* ring. (Here F is assumed to be a field, of course.) Recall that a ring R is *Euclidean* if there is a function $d : R-\{0\} \to \mathbb{N}_0$ such that:

- If $a, b \neq 0$, then $d(a) \leq d(ab)$
- If $a \in R$ and $b \neq 0$, then there are elements $q, r \in R$ such that $a = qb + r$ and $r = 0$ or $d(r) < d(b)$.

For polynomials, degree gives the function d. As we showed in class using a geometric argument, another example of a Euclidean ring is $\mathbb{Z}[i]$, where $d(z) = N(z) = z\bar{z}$. serves the purpose.

The reason for the name *Euclidean* is that for any such ring the greatest common divisor of any two elements exists and may be found by the Euclidean algorithm using repeated division with remainder. As a consequence, irreducible elements of Euclidean rings must be prime, and any element of a Euclidean ring factors uniquely (up to order of multiplication and multiplication by units) into prime elements.

I am not going to provide solutions here to the computational problems, since we thoroughly discussed the Euclidean algorithm in class, and it is also thoroughly discussed, with examples, in your text. Finding the greatest common divisor in a Euclidean ring other than the integers is simply a matter of applying the method of division with remainder that works in that ring. Synthetic division of polynomials should be familiar, and we carefully discussed the geometric approach to division with remainder in the Gaussian integers, $\mathbb{Z}[i]$, in class. *Make sure you can do these computations for the in-class final exam! Make sure you also understand how the proofs of results about greatest common divisors and least common multiples generalize from the ring of integers to any Euclidean domain.*