Over a GCD Domain – Part I

One of our big questions is to what extent the structure of R is reflected in the structure of $R[x]$; if R has more "technology" available, perhaps this can be used to say interesting things about the polynomials over R. In this section we will see that this is indeed the case if R is a GCD domain.

In fact, thanks to the polynomial long division algorithm, if R is a domain then $R[x]$ is already sitting inside a Euclidean domain – namely $F[x]$ where F is the field of fractions of R. So it doesn't take much to get extra technology in $R[x]$.

Definition 1 (Content of a polynomial)**.** *Let R be a GCD domain and let $p(x) \in R[x]$ be a polynomial with coefficients a_i. We define the* content *of $p(x)$ to be*

$$\mathsf{content}(p) = \begin{cases} 0 & \text{if } p(x) = 0 \\ \mathsf{gcd}\,(a_0, a_1, \ldots, a_d) & \text{if } p(x) \neq 0, \text{where } d = \deg p. \end{cases}$$

If $\mathsf{content}(p) = 1$, we say that $p(x)$ is primitive*.*

For example, $\mathbb{Z}$ is a GCD Domain, and $\mathsf{content}(2x^3 + 4x - 6) = 2$. Every field F is a GCD domain, and every nonzero polynomial over F is primitive.

Proposition 1. *Let R be a GCD domain.*

1. *Every polynomial $a(x) \in R[x]$ can be written as $a(x) = \mathsf{content}(a)\overline{a}(x)$, where $\overline{a}(x) \in R[x]$ is primitive.*

2. *Let $d \in R$ and $a(x) \in R[x]$. Then the constant polynomial d divides $a(x)$ in $R[x]$ if and only if d divides $\mathsf{content}(a)$ in R.*

3. *Let $d \in R$ and $a(x), b(x) \in R[x]$. If $d|\mathsf{content}(a+b)$ and $d|\mathsf{content}(a)$, then $d|\mathsf{content}(b)$.*

4. *If $d \in R$ and $a(x) \in R[x]$, then $\mathsf{content}(da) = d\mathsf{content}(a)$.*

5. *Let F be the field of fractions of R and let $q(x) \in F[x]$. Then there is a fraction $\frac{u}{v} \in F$ such that $p(x) = \frac{u}{v}q(x)$ is in $R[x]$ and is primitive there.*

6. *$\mathsf{content}(x^n a(x)) = \mathsf{content}(a(x))$.*

Proof.

1. If $a(x) = 0$, set $\overline{a}(x) = 1$. Suppose $a(x) \neq 0$. Now $\mathsf{content}(a) = \mathsf{gcd}\,(a_0, a_1, \ldots, a_n)$, and in particular for each i we have $a_i = \mathsf{content}(a)\overline{a}_i$ for some $\overline{a}_i$, and $\mathsf{gcd}\,(\overline{a}_0, \overline{a}_1, \ldots, \overline{a}_n) = 1$. Let $\overline{a}(x) = \sum_{i=0}^{n} \overline{a}_i x^i$.

2. (write these)

□

Proposition 2 (Gauss' Lemma – Part I)**.** *Let R be a GCD Domain with $a(x), b(x) \in R[x]$. Then we have the following.*

1. *If $a(x)$ and $b(x)$ are primitive, then $a(x)b(x)$ is primitive.*
2. $\mathsf{content}(ab) = \mathsf{content}(a)\mathsf{content}(b)$
3. *If $a(x)|b(x)$ in $R[x]$, then* $\mathsf{content}(a)|\mathsf{content}(b)$ *in R.*

Proof.

1. We proceed by induction on the number k of nonzero terms of a and b together.

   (a) **Base Case** ($k = 0$): If a and b together have no nonzero terms, then $a(x) = b(x) = 0$; neither is primitive.

   (b) **Base Case** ($k = 1$): If a and b together have exactly one nonzero term, then either $a(x) = 0$ or $b(x) = 0$; one is not primitive.

   (c) **Base Case** ($k = 2$): If $a(x)$ and $b(x)$ together have exactly two nonzero terms, then each must have exactly one. (Otherwise one is zero and thus not primitive.) Say $a(x) = a_n x^n$ and $b(x) = b_m x^m$. If both $a(x)$ and $b(x)$ are primitive, then $a_n = \mathsf{content}(a)$ and $b_m = \mathsf{content}(b)$ are units, so that $\mathsf{content}(ab) = a_n b_m$ is a unit; hence $a(x)b(x)$ is primitive.

   (d) **Inductive Step:** Suppose the result holds for all pairs of primitive polynomials having less than $n > 2$ nonzero terms together, and suppose that $a(x)$ and $b(x)$ are primitive with exactly n nonzero terms together. Say $\deg a = n$ and $\deg b = m$, so that the leading coefficients of a, b, and ab are a_n, b_m, and $a_n b_m$, respectively. Now let $c = \mathsf{content}(ab)$, and suppose BWOC that c is *not* a unit. Note that $c|a_n b_m$. Now $\mathsf{gcd}\,(c, a_n)$ and $\mathsf{gcd}\,(c, b_m)$ cannot both be units in R. (If $\mathsf{gcd}\,(c, a_n) = 1$, then by Euclid's lemma we have $c|\mathsf{gcd}\,(c, b_m)$.) So suppose WLOG that $\mathsf{gcd}\,(c, a_n) = d$ is not a unit.

   Now $d|\mathsf{content}(ab)$ in R, so that $d|a(x)b(x)$ in $R[x]$. Since $d|a_n$, we also have $d|a_n x^n$ in $R[x]$. Thus $d|b(x)(a(x) - a_n x^n)$ in $R[x]$, and thus

   $$d|\mathsf{content}(b(x)(a(x)-a_n x^n)) = \mathsf{content}(a(x)-a_n x^n)\mathsf{content}(b(x)p(x)),$$

   where $p(x) \in R[x]$ is primitive such that $a(x)-a_n x^n = \mathsf{content}(a(x)-a_n x^n)p(x)$. In particular, note that $p(x)$ and $a(x) - a_n x^n$ have the same number of nonzero terms which is one fewer than the number of nonzero terms of $a(x)$. Thus b and p have fewer than n nonzero terms. Since b and p are both primitive, by the inductive hypothesis, $\mathsf{content}(bp) = 1$. Thus we have $d|\mathsf{content}(a(x) - a_n x^n)$. Since $d|\mathsf{content}(a_n x^n)$, by the lemma we have $d|\mathsf{content}(a)$. But a is primitive, so that d is a unit, a contradiction. So $a(x)b(x)$ must be primitive.

2. We have

$$\begin{aligned}
\mathsf{content}(a(x)b(x)) &= \mathsf{content}(\mathsf{content}(a)\overline{a}\mathsf{content}(b)\overline{b}) \\
&= \mathsf{content}(a)\mathsf{content}(b)\mathsf{content}(\overline{a}\overline{b}) \\
&= \mathsf{content}(a)\mathsf{content}(b)
\end{aligned}$$

3. Say $a(x)c(x) = b(x)$; then $\mathsf{content}(a)\mathsf{content}(c) = \mathsf{content}(b)$. □

Lemma 3. *Let R be a GCD domain with field of fractions F.*

1. *If $p(x) \in R[x]$ is primitive, $r \in R$, and $a(x) \in R$ such that $p(x)|a(x)$ and $r|a(x)$ in $R[x]$, then $rp(x)|a(x)$ in $R[x]$.*

2. *If $q(x) \in F[x]$ and $p(x) \in R[x]$ such that $p(x)$ is primitive and $p(x)q(x) \in R[x]$, then in fact $q(x) \in R[x]$.*

Proof.

1. Write $a(x) = p(x)b(x)$ with $b(x) \in R[x]$. Since $r|a(x)$, we have $r|\mathsf{content}(a) = \mathsf{content}(p)\mathsf{content}(b) = \mathsf{content}(b)$, since p is primitive. So $r|b(x)$ in $R[x]$. Say $b(x) = rc(x)$; then $a(x) = rp(x)c(x)$ as needed.

2. We have $\frac{u}{v} \in F$ (in lowest terms) such that $\frac{u}{v}q(x) \in R[x]$ is primitive; say $\frac{u}{v}q(x) = s(x)$. Now $uq(x) = vs(x)$, and moreover $up(x)q(x) = vp(x)s(x) \in R[x]$. Now

$$\begin{aligned}
u \cdot \mathsf{content}(pq) &= \mathsf{content}(up(x)q(x)) \\
&= \mathsf{content}(vp(x)s(x)) \\
&= v \cdot \mathsf{content}(ps) = v,
\end{aligned}$$

since p and s are primitive in $R[x]$. In particular, $u|v$. Since $\frac{u}{v}$ is in lowest terms, without loss of generality, $u = 1$, so that $\frac{1}{v}q(x) = s(x)$. Thus $q(x) = vs(x) \in R[x]$ as needed. □

Proposition 4 (Gilmer-Parker)**.** *If R is a GCD Domain, then $R[x]$ is a GCD Domain.*

Proof. Let $a(x), b(x) \in R[x]$. Let $k = \mathsf{gcd}\left(\mathsf{content}(a), \mathsf{content}(b)\right)$ (remember that R is a GCD domain). Let F be the field of fractions of R. Now $F[x]$ is a Euclidean domain, in particular a GCD domain, so that $a(x)$ and $b(x)$ have a greatest common divisor in $F[x]$. By the lemma, we can take an associate (in $F[x]$) of this gcd which is in $R[x]$ and primitive; say $t(x)$. We claim that $kt(x)$ is a gcd of a and b in $R[x]$.

First note that $k|\mathsf{content}(a)$, so that $k|ax$. Now $t(x)|a(x)$ in $F[x]$, where t and a are in $R[x]$ and $t(x)$ is primitive. By the lemma, $t(x)|a(x)$ in $R[x]$, and again using the lemma, $kt(x)|a(x)$ in $R[x]$. Similarly, $kt(x)|b(x)$ in $R[x]$. So $kt(x)$ is a common divisor of $a(x)$ and $b(x)$ in $R[x]$.

Now suppose that $e(x) \in R[x]$ is a common divisor of $a(x)$ and $b(x)$ over R. If $e(x)$ is constant, then $e(x) = e_0|\mathsf{gcd}\left(\mathsf{content}(a), \mathsf{content}(b), =\right) k$. Suppose instead that $e(x)$ has positive degree. Now $e(x)$ divides $a(x)$ and $b(x)$ in $F[x]$, which is a GCD domain, and thus $e(x)$ divides $t(x)$ in $F[x]$. Say $e(x)f(x) = t(x)$ where $f(x) \in F[x]$. By the lemma, we may write $f(x) = \frac{u}{v}g(x)$ where $g(x) \in R[x]$ is primitive and $\mathsf{gcd}\,(u, v) = 1$. We have $ue(x)g(x) = vf(x) \in R[x]$. Now $\mathsf{content}(ue(x)g(x)) = \mathsf{content}(vt(x))$, and since g and t are primitive over R, $u\mathsf{content}(e) = v$. By Euclid's lemma, $v|\mathsf{content}(e)$, so that $v|\mathsf{content}(a)$ and $v|\mathsf{content}(b)$, and thus $v|k$. In particular, we have $kf(x) = k\frac{u}{v}g(x) \in R[x]$, and thus $e(x) \cdot kf(x) = kt(x)$, so that $e(x)|kt(x)$ in $R[x]$.

Thus $kt(x)$ is a greatest common divisor of $a(x)$ and $b(x)$ in $R[x]$. $\square$

Exercises

1. Let R be a GCD domain with $p(x), q(x) \in R[x]$ so that q is irreducible (hence prime), and let k be a natural number. Show that q^{k+1} divides p in $R[x]$ iff $q|p$ and $q^k|p'$ in $R[x]$. In particular, show that p is squarefree iff $\mathsf{gcd}\,(p, p') = 1$.

2. Let R be a GCD domain, with $p, q \in R[x]$ nonzero. Show that p and q have a common factor of positive degree in $R[x]$ if and only if there exist $a, b \in R[x]$, not zero, such that $\deg a < \deg q$, $\deg b < \deg p$, and $pa - qb = 0$. (Looking forward to univariate resultant.)