MATH 436 Notes: Applications of Unique Factorization.

Jonathan Pakianathan

December 13, 2005

1 Euclidean rings

We have previously discussed the basic concepts and fundamental theorems on unique factorization in PIDs. We will provide a few examples of how unique factorization is used in applications to number theory. One cannot stress how important the concept of unique factorization is in many mathematical applications and definately in algebraic number theory. We unfortunately will only have the time to get a taste of it but it should give the reader an idea.

Before we can do this, we need a useful simple method to show that a given integral domain is a PID. This is provided in the next concept:

Definition 1.1. *Let R be an integral ring and let R^* denote its nonzero elements. R is called a Euclidean ring if there is a degree map $D : R^* \to \mathbb{N}$ with the following properties:*
(1) $D(ab) \geq max(D(a), D(b))$ for all $a, b \in R^*$.
(2) For $a, b \in R^*$ we can write $a = qb + r$ where $q, r \in R$ and either $r = 0$ or $D(r) < D(b)$.
(3) For $a, b \in R^*$ we can write $a = bq' + r'$ where $q', r' \in R$ and either $r' = 0$ or $D(r') < D(b)$.

A commutative Euclidean ring is called a Euclidean domain. (The reader should note that (3) is redundant in the commutative case.)

Conditions (2) and (3) are sometimes refered to as the division algorithm for a Euclidean ring.

Property (1) of a Euclidean ring is not as important as the other properties and is only there for technical reasons illustrated below:

The important fact about Euclidean rings is the following:

Theorem 1.2. *Let R be a Euclidean ring, then R is a principal ring.*

Thus every Euclidean domain is a PID.

In fact if I is a nonzero left (right) ideal of R then $I = (\alpha)_L$ (resp. $I = (\alpha)_R$) for any nonzero element $\alpha \in I$ of minimal degree.

Proof. Let I be a left (right) ideal of R. Without loss of generality assume I is nonzero since the zero ideal is clearly principal.

Thus we may take $\alpha \in I$ with $D(\alpha) \in \mathbb{N}$ minimal.

Then the left (right) ideal generated by α lies inside of I. We wish to show that it is I. So assume $\beta \in I$ and apply the division algorithm condition of the Euclidean ring (we will do the case of left ideals, the case of right ideals uses property (3) instead of (2)):

$\beta = q\alpha + r$ where $r = 0$ or $D(r) < D(\alpha)$.

Since $\beta, \alpha \in I$, it follows that $r \in I$ and hence since $D(\alpha)$ is minimal we conclude $r = 0$, i.e., $\beta = q\alpha$.

Thus we see the left (right) ideal I is indeed generated by α. This completes the proof.

Notice in this proof we did not use property (1) of a Euclidean ring at all. □

Condition (1) of a Euclidean ring is only useful for the following refinement:

Corollary 1.3. *Let R be a Euclidean ring and I a nonzero left (right) ideal of R. Then a nonzero element $\alpha \in I$ is a generator of I as a left (right) ideal if and only if α has minimal degree in I.*

If $m = min\{D(r)|r \in R^*\}$ then u is a unit of R if and only if $D(u) = m$.

Proof. We will do the case of left ideals. The proof for right ideals is similar.

We have already seen that any element of minimal degree in I, generates I. Say $I = (\beta)_L$ where β is such an element of minimal degree.

It only remains to show that if α is some other generator of I, that it also shares this same minimal degree.

Since $\beta \in I = (\alpha)_L$ we have $\beta = q\alpha$. By property (1), it follows that $D(\beta) \geq max(D(q), D(\alpha)) \geq D(\alpha)$. Since $\alpha \in I$ and degree of β is minimal in I we conclude $D(\alpha) = D(\beta)$ is also minimal in I.

This proves the first part.

For the second part note that u has a left inverse if and only if $(u)_L = R$. This happens if and only if $D(u) = m$ by the first part.

Similarly u has a right inverse if and only if $(u)_R = R$ if and only if $D(u) = m$. Thus $(D(u) = m) \leftrightarrow$ (u is a unit of R).

□

2 Application I: Polynomial rings

Our first applications of unique factorization will be to polynomial rings in one variable with coefficients in a field (or division ring more generally).

Let k be a division ring and let $R = k[x]$ denote the polynomial ring with coefficients in k. We have seen that since k is in particular an integral ring, then $k[x]$ is also an integral ring and there is a degree map $D : R^* \to \mathbb{N}$ which satisfies $D(pq) = D(p) + D(q)$ for $p, q \in R^*$.

We say that this degree map is additive. Notice that any additive degree map satisfies condition (1) of a Euclidean ring as $D(pq) = D(p) + D(q) \leq min(D(p), D(q))$ as $D(p), D(q) \in \mathbb{N}$.

The next theorem shows that we may also perform the division algorithms in $k[x]$ and so indeed $k[x]$ is a Euclidean ring!

Theorem 2.1. *Let k be a division ring, then $k[x]$ is a Euclidean ring.*

Thus if k is a field, then $k[x]$ is a Euclidean domain and hence a PID.

Proof. It suffices to show property (2) of a Euclidean ring holds as the proof of property (3) is similar and (1) was proven in the preceding paragraph.

Let $R = k[x]$ and let $p(x), q(x) \in R^*$. We will prove condition (2) by induction on $D(p)$.

In any case notice that if $D(q) > D(p)$ then we have $p(x) = 0q(x) + p(x)$ gives condition (2). Thus we will only be concerned with the case $D(q) \leq D(p)$ in general.

To start the induction we consider the case $D(p) = 0$. By the above comment we may assume $D(q) \leq D(p)$ and so $D(q) = 0$ also. Thus p and q are both units of $R = k[x]$ and so we may write $p = (pq^{-1})q + 0$ and condition (2) holds. So the case where $D(p) = 0$ is done.

Now assume that condition (2) holds for all $p(x)$ with $D(p) \leq n$ for some $n \in \mathbb{N}$ and take $p(x) \in R^*$ with $D(p) = n + 1$. As usual assume $D(q) \leq D(p)$ and let $L(p)$ and $L(q)$ denote the leading coefficients of $p(x)$ and $q(x)$ respectively.

Since k is a division ring, $L(q)^{-1}$ exists in k.

Then $p(x) - L(p)L(q)^{-1}x^{D(p)-D(q)}q(x)$ is a polynomial of degree strictly less than the degree of p (since the leading terms in the difference cancel) and so by induction we may write:

$p(x) - L(p)L(q)^{-1}x^{D(p)-D(q)}q(x) = s(x)q(x) + r(x)$ where $r(x) = 0$ or $D(r) < D(q)$.

Thus $p(x) = (s(x) + L(p)L(q)^{-1}x^{D(p)-D(q)})q(x) + r(x)$ where $r(x) = 0$ or $D(r) < D(q)$.

Thus condition (2) holds for $p(x)$ and we are done by induction.

□

The division algorithms only hold in general when the coefficients are taken form a field or division ring as the next example illustrates:

Example 2.2. *Consider the ideal $I = (2, x) = \{2f(x) + xg(x) | f(x), g(x) \in \mathbb{Z}[x]\}$. If $h(x)$ were a generator for this ideal then $h(x)$ would have to divide 2 and hence be a constant. Since $h(x)$ also divides x it would have to be a unit, either ± 1 but this is a contradiction as I is not equal to $\mathbb{Z}[x]$ as $1 \notin I$.*

Thus I is not a principal ideal and so $\mathbb{Z}[x]$ is an integral domain which is not a PID and hence not a Euclidean domain.

The following corollary follows since $k[x]$ is a Euclidean domain and a PID:

Corollary 2.3. *Let k be a field.*

The units of $k[x]$ are exactly the nonzero constant polynomials.

The set of prime elements of $k[x]$ coincides with the set of irreducible elements of $k[x]$.

All nonzero prime ideals of $k[x]$ are maximal.

If $p(x)$ is a irreducible polynomial then $k[x]/(p(x))$ is a field.

The last statement in the above corollary follows as $p(x)$ is prime and so $(p(x))$ is a nonzero prime ideal and hence is a maximal ideal as $k[x]$ is a PID.

From now on let k be a field.

In $k[x]$ every nonzero polynomial is associate to a unique monic polynomial (i.e., one whose leading coefficient is 1) and we will take as our set of prime representatives the monic irreducible polynomials of $k[x]$.

Note since the degree zero polynomials are the units of $k[x]$, all irreducible polynomials have positive degree.

Since we know $k[x]$ is a PID and hence a UFD we then know that every nonzero polynomial in $k[x]$ factors **uniquely** as a unit (a constant) times a finite product of monic irreducible polynomials of $k[x]$.

We now discuss the concept of roots of a polynomial.

Definition 2.4. *Let R be a ring and E a bigger ring containing R as a subring. Let $\alpha \in E$, then we may consider the evaluation map*

$$ev_\alpha : R[x] \to E$$

given by $ev_\alpha(f(x)) = f(\alpha)$.

It is easy to see that ev_α is a ring homomorphism.

If $f(x) \in R[x]$ is in the kernel of ev_α i.e., $f(\alpha) = 0$ we say that α is a root of $f(x)$.

The following fact about roots is fundamental:

Theorem 2.5. *Let k be a field and let $\alpha \in k$.*

Then α is a root of $f(x)$ if and only if $f(x) = (x - \alpha)q(x)$.

Thus the kernel of ev_α is the ideal $(x - \alpha)$.

If $f(x)$ is a nonzero polynomial then $f(x)$ has at most $D(f)$ roots in k.

Proof. Let I denote the kernel of ev_α. It is clear that $x - \alpha \in I$. Let $f(x) \in I$ then we may perform the division algorithm:

$f(x) = q(x)(x - \alpha) + r(x)$ where $r(x) = 0$ or $D(r) < D(x - \alpha) = 1$. Thus if $r(x)$ is not zero, it is a nonzero constant.

Evalutating at α we find $0 = f(\alpha) = r(\alpha)$ and so we conclude that $r(x) = 0$. Thus $f(x) \in (x - \alpha)$ and we conclude $I = (x - \alpha)$. This proves the first parts of the theorem.

For the final part, we prove the result by induction on the degree of $f(x)$.

If the degree of $f(x)$ is zero, then f is a nonzero constant and has no roots in k so the theorem holds. So assume that the final part holds for all polynomials of degree $\leq n$ where $n \in \mathbb{N}$ and let $f(x)$ have degree $n+1$. If $f(x)$ has no roots in k we are done so assume α is a root. Then $f(x) = q(x)(x - \alpha)$ where $q(x)$ has degree n and hence has at most n roots in k by induction.

Since it is easy to see that $\{$ Roots of $f(x)\} = \{$ Roots of $q(x)\} \cup \{\alpha\}$ we conclude that $f(x)$ has at most $n+1$ roots in k as desired. Thus we are done.

□

We will see later that every integral domain embeds inside a field and so if R is an integral domain and $f(x) \in R[x]$ has degree n then $f(x)$ has at most n roots in R too. However the result does not hold if the ring R has zero divisors as the example below shows!

Example 2.6. *By Fermat's little theorem, for any prime p, all the p elements of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ are roots of $x^p - x$. So in $\mathbb{F}_p[x]$ we have*

$$x^p - x = \prod_{\alpha \in \mathbb{F}_p} (x - \alpha).$$

Now let R be the direct product ring $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. R is a commutative ring but has zero divisors. Consider $f(x) = (x^3 - x)(x^5 - x)$ a polynomial of degree 8 in $R[x]$. Let $(a,b) \in R$. Then $(a,b)^3 - (a,b)$ has zero first component while $(a,b)^5 - (a,b)$ has zero second component in R. Thus (a,b) is a root of $f(x)$. Since $(a,b) \in R$ was arbitrary, we have all 15 elements of R are roots of the degree 8 polynomial $f(x)$!

It is also certainly possible that a degree n polynomial does not have n roots in k:

Example 2.7. *Consider the quadratic polynomial $x^2 + 1 \in \mathbb{R}[x]$. This polynomial has no roots in $\mathbb{R}$ as is easily checked.*

Now we will use this "basic" fact about roots of polynomials in a field to prove a fundamental fact in elementary number theory:

Theorem 2.8. *Let k be a field then any finite subgroup of the multiplicative group of nonzero elements $(k^*, \cdot)$ is cyclic.*

Proof. Let A be a finite subgroup of $(k^*, \cdot)$. Thus A is a finite abelian group and so we may write $A \cong \times_{p \in S} A_p$ where S is a finite set of primes dividing $|A|$ and A_p are Abelian p-groups for each prime $p \in S$.

To show A is cyclic, by the classification of finte Abelian groups, it suffices to show that each A_p is cyclic. So without loss of generality we will consider the case when A is a p-group of order p^k say. If A has an element of order p^k

then it is cyclic so assume it does not. Then all elements of A have orders dividing p^{k-1} and so the elements of $A \subseteq k$ are all roots of $x^{p^{k-1}} - 1$. This is a contradiction as this polynomial has degree p^{k-1} and A has p^k elements!

□

Corollary 2.9. *Let $\mathbb{F}_p$ be the field of p elements. Then there exists a generator α for the multiplicative group $\mathbb{F}_p^*$. We call such an element a multiplicative generator of the integers modulo p.*

Since $\mathbb{F}_p^*$ has order $p-1$, the last corollary guarantees the existance of an element of order $p-1$. For example 2 is a multiplicative generator of $\mathbb{F}_5^*$ as $\bar{2}^2 = \bar{4}, \bar{2}^3 = \bar{3}$ and $\bar{2}^4 = \bar{1}$.

It is easy to check that $\bar{2}$ is not a multiplicative generator of $\mathbb{F}_7^*$ but $\bar{3}$ is.

In general, it can be difficult to explicitly find a multiplicative generator of a given $\mathbb{F}_p^*$ but the last corollary guarantees one exists!

3 Construction of fields from polynomial rings

Since we know $k[x]$ is a UFD, it would be nice to be able to determine the monic irreducible polynomials of $k[x]$. However this is a tricky problem in general.

The following proposition handles the question in some cases of low degree:

Proposition 3.1. *Let $p(x)$ be a nonzero polynomial of $k[x]$.*
(1) $D(p) = 0$ if and only if p is a unit of $k[x]$.
(2) If $D(p) = 1$ then $p(x)$ is always irreducible in $k[x]$.
(3) If $D(p) = 2$ or 3 then $p(x)$ is irreducible in $k[x]$ if and only if $p(x)$ has no root in k.

Proof. We have seen (1) previously.

For (2) and (3) suppose $p(x) = q(x)s(x)$ for $q(x), s(x) \in k[x]$. Then $D(p) = D(q) + D(s)$. If either $D(q)$ or $D(s)$ is zero then q or s is a unit in $k[x]$.

Thus if $D(p) = 1$ then one of q or s is a unit in $k[x]$ and so $p(x)$ is always irreducible. This proves (2)

Now suppose $D(p) = 2$ or 3 and $p(x) = q(x)s(x)$ is a proper reduction. This forces one (or both) of the degrees of $s(x)$ and $q(x)$ to be 1 and so $p(x)$

has a root in k. Taking the contrapositive, we conclude that if a quadratic or cubic polynomial has no roots in k, then it is irreducible in $k[x]$.

On the other hand, it is clear that if $p(x)$ has a root α in k then $p(x) = (x - \alpha)q(x)$ is reducible (as $D(p) > 1$) and so taking contrapositives again, we have that if $p(x)$ is irreducible, then $p(x)$ has no roots in k.

This completes the proof of the proposition. □

For degrees higher than 3, it is no longer sufficient that the polynomials have no roots as the next example shows:

Example 3.2. $x^2 + 1$ *is an irreducible quadratic polynomial in* $\mathbb{R}[x]$. *(as it has no roots in* $\mathbb{R}$*).*

However $f(x) = (x^2 + 1)(x^2 + 1) = x^4 + 2x^2 + 1$ *is a quartic polynomial in* $\mathbb{R}[x]$ *which also has no roots in* $\mathbb{R}$ *but it is clearly reducible in* $\mathbb{R}[x]$.

Since $k[x]$ is a PID, once we have an irreducible polynomial $f(x)$ then $k[x]/(f(x))$ is a field.

By the division algorithm, any $g(x) \in k[x]$ can be written as $g(x) = q(x)f(x) + r(x)$ where $r(x) = 0$ or $D(r) < D(f)$ and so in $k[x]/(f(x))$, $g(x)$ and $r(x)$ represent the same element.

From this it is not hard to show that in the field $k[x]/(f(x))$ any element can be uniquely represented by a polynomial of degree strictly less than the degree of $f(x)$.

We consider some examples below:

Example 3.3. *The polynomial* $x^2 + 1$ *is irreducible in* $\mathbb{R}[x]$ *and so* $\mathbb{F} = \mathbb{R}[x]/(x^2 + 1)$ *is a field. By the previous discussion, the elements of* $\mathbb{F}$ *can be represented uniquely as* $a + b\bar{x}$ *with* $a, b \in \mathbb{R}$.

However in $\mathbb{F}$ *note that* $\bar{x}^2 + 1 = 0$. *Using this it is not hard to show that the quotient ring* $\mathbb{R}[x]/(x^2 + 1)$ *is isomorphic to the field of complex numbers.*

Example 3.4. *The quadratic polynomial* $x^2 + x + 1$ *has no roots in* $\mathbb{F}_2$ *and is hence irreducible in* $\mathbb{F}_2[x]$. *Thus* $R = \mathbb{F}_2[x]/(x^2 + x + 1)$ *is a field where every element is represented uniquely as* $a + b\bar{x}$ *where* $a, b \in \mathbb{F}_2$.

Thus R *is a finite field of order* 4. *We may compute the multipication in* R *explicitly by using the relation* $\bar{x}^2 + \bar{x} + 1 = 0$.

It is important to note that R *is a field of order* 4 *and so is not the ring* $\mathbb{Z}/4\mathbb{Z}$ *since the latter is not even an integral domain!*

We will talk more about these exotic finite fields in the future.