18.704 Gary Sivek
2/09/05 gsivek@mit.edu

Adjoining Roots of Polynomials to Fields

We begin our discussion of roots of polynomials with a few useful definitions on rings.

Definition: A ring R is a *Euclidean domain* if there exists a function $N : R \to \{0, 1, 2, \ldots\}$ such that, given any $a, b \neq 0 \in R$ we may find $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $N(r) < N(b)$.

This is the standard division algorithm; when $R = \mathbb{Z}$, for example, we have the traditional norm $N(x) = |x|$. Note that q and r need not be uniquely determined.

Proposition 1: Let F be a field. Then $F[x]$ is a Euclidean domain.
Proof: We can define the norm of a polynomial to be its degree. Now suppose our polynomials are $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0$ and $g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_0$. If $m < n$, then $f(x) = 0 \cdot g(x) + f(x)$ and we are trivially done. Otherwise, we may iteratively lower the degree of f as follows: since F is a field, we know b_n is invertible, so write $G(x) = b_n^{-1} g(x) = x^n + c_{n-1} + \ldots + c_0$. Then we may subtract $a_m x^{m-n} G(x)$ from f to obtain a polynomial f' of degree not exceeding $m-1$, and we repeat on f' and G. After repeating the procedure sufficiently often, we have a polynomial f^* of degree not exceeding $n-1$, and it has the form $f^*(x) = f(x) - q(x) \cdot G(x) = f(x) - q(x) b_n^{-1} g(x)$; then $f(x) = (b_n^{-1} q(x))g(x) + f^*(x)$ satisfies the condition for a Euclidean domain.

Recall that a principle ideal is an ideal which can be generated by one element. A *principle ideal domain* (or PID) is a ring in which all ideals are principle.

Proposition 2: Any Euclidean domain is a principle ideal domain.
Proof: This statement is entirely analogous to the case of $\mathbb{Z}$, where it can easily be shown that the ideal generated by two elements is equal to the ideal generated by their greatest common divisor. For a general Euclidean domain R, suppose an ideal I has two arbitrary nonzero elements a, b. Then there exist $q, r \in R$ such that $a = qb + r$, and by the definition of an ideal it follows that $a - qb = r$ is also in I. If $r = 0$ then we may stop, since both a and b are in $(b) \subset I$. Otherwise, we note that $N(r) < N(b)$ and repeat on b and r, finding $s, t \in R$ such that $b = sr + t$. As before, $t \in I$, and we may repeat on r and t. Since the norm of these remainders is strictly decreasing, it must eventually be 0, and then the last nonzero remainder generates all remainders found; in particular it generates both a and b.

Among other important results, this means that $F[x]$ is a principle ideal domain. This will be quite useful later in proving results about roots of polynomials. Still, we need a few more standard definitions before we may discuss roots themselves. One of the most crucial concepts is that of a homomorphism:

Definition: A ring *homomorphism* is a map $\phi : R \to R'$ which satisfies the following three conditions for all $a, b \in R$:

1. $\phi(ab) = \phi(a)\phi(b)$
2. $\phi(a+b) = \phi(a) + \phi(b)$
3. $\phi(1_R) = 1_{R'}$

There are many important properties that arise from these definitions alone; for example, setting $a = b = 0_R$ in the second rule shows that $\phi(0_R) = 0_{R'}$. As with groups, we define the *kernel* and *image* of ϕ to be the sets $\{r \in R : \phi(r) = 0\}$ and $\{\phi(r) : r \in R\}$, respectively. The kernel in particular serves as a good motivation for ideals.

Proposition 3: The kernel of a homomorphism is an ideal.
Proof: We must simply verify that the properties of ideals hold for kernels. The first condition is that $\ker\phi$ is a subgroup of R^+. If $a, b \in \ker\phi$ then $\phi(a+b) = \phi(a)+\phi(b) = 0+0 = 0$, so the kernel has closure; as noted above, $0 = \phi(0) = \phi(a-a) = \phi(a)+\phi(-a) = \phi(-a)$, so elements of the kernel have inverses in the kernel; and, of course, $0 \in \ker(\phi)$, so this condition is satisfied. The second condition is that if $a \in \ker(\phi)$ and $r \in R$, then $ra \in \ker(\phi)$; this holds because $\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0 = 0$. Thus $\ker\phi$ is an ideal.

We now need one more result on polynomial rings: namely, the Substitution Principle.

Proposition 4: Given a ring homomorphism $\phi : R \to R'$ and an element $\alpha \in R$, there is a unique homomorphism $\Phi : R[x] \to R'$ which maps x to α and $r \in R$ to $\phi(r)$.
Proof: Given a polynomial $f(x) = \sum r_i x^i$, the above restrictions require that $\Phi(f(x)) = \sum \phi(r_i)\alpha^i$; this proves that Φ is unique. To show it is a homomorphism, it clearly satisfies the requirements on addition and the identity, so we only need to show that the multiplication law holds. Let $f(x) = \sum a_i x^i$ and $g(x) = \sum b_j x^j$ be functions in $R[x]$. Then:
$\Phi(fg) = \Phi((\sum a_i x^i)(\sum b_j x^j)) = \Phi(\sum a_i b_j x^{i+j}) = \sum \phi(a_i)\phi(b_j)\alpha^{i+j} = \sum \phi(a_i)\alpha^i \phi(b_j)\alpha^j$
$= (\sum \phi(a_i)\alpha^i)(\sum \phi(b_j)\alpha^j) = \Phi(f)\Phi(g)$.
So Φ is the desired unique homomorphism.

A number is *algebraic* over a ring R if it is the root of some polynomial in $R[x]$. To each such number α we may associate a polynomial of least positive degree which has α as a root; this is called the *irreducible polynomial* for α. It is unique up to scalar multiplication, since if there are two irreducible polynomials $f(x) = a_n x^n + \ldots + a_0$ and $g(x) = b_n x^n + \ldots + b_0$, then $b_n f(x) - a_n g(x)$ has α as a root but has degree less than n, so it is 0.

Proposition 5: Let $f(x) \in F[x]$ be the irreducible polynomial for α. If $g(\alpha) = 0$ and $g \in F[x]$ is nonzero, then f divides g.
Proof: By the Substitution Principle, the map $\Phi : F[x] \to F$ fixing F and sending x to α is a homomorphism. Its kernel is the set of polynomials for which α is a root, and by

Proposition 3 this kernel is an ideal. But Proposition 1 tells us that any ideal in $F[x]$ is a principle ideal, and so it is generated by a unique element of least degree. Thus $\ker\Phi = (f)$.

Now we will begin to adjoin roots of polynomials to fields. Given a field F and some value α, define $F(a)$ to be the smallest field that contains both F and a. One standard example is $\mathbb{R}(\sqrt{-1}) = \mathbb{C}$. The operation of adjoining an element to a field is a *field extension*, and a useful value is the *degree* of the field extension. In general, given two fields $F \subset K$, the degree of the extension, denoted $[K : F]$, is the dimension of K as an F-vector space. In the example of the complex numbers, any element in $\mathbb{C}$ can be written as a linear combination over $\mathbb{R}$ of 1 and i, so $[\mathbb{C} : \mathbb{R}] = 2$. If α has degree n over F, then $[f(\alpha) : f] = n$, since $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis and higher powers of α may be written in terms of lower powers.

Proposition 6: Let $F \subset K \subset L$ be fields. Then $[L : F] = [L : K][K : F]$.
Proof: Let $\{x_1, \ldots, x_m\}$ be a basis for L over K, and let $\{y_1, \ldots, y_m\}$ be a basis for K over F. An arbitrary element of L can be written as $l = a_1x_1 + \ldots a_mx_m$ for some $a_1, \ldots, a_m \in K$. Then each a_i can be written as $a_i = b_{1i}y_1 + \ldots + b_{nj}y_n$ for some $b_{1j}, \ldots, b_{nj} \in F$, so that $l = \sum c_{ij}x_iy_j$ for appropriate values of c_{ij}. Since each c_{ij} is uniquely determined by the a_j, which are in turn uniquely determined by l, we conclude that the set $\{x_iy_j\}$ is linearly independent, so it forms a basis for L over F.
Corollary: Let $F \subset K$ be fields with $[K : F] = n$, and pick $\alpha \in K - F$. Then α has degree dividing n in F.

This last proposition has many useful consequences. For example, it sometimes allows us to determine easily whether a number is in a field extension. Consider $\mathbb{Q}(\alpha)$, where $\alpha^3 + \alpha + 1 = 0$. Is $i \in \mathbb{Q}(\alpha)$? Any of a number of methods can show this polynomial is irreducible, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Assume i is in the extension; then $\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(\alpha)$, and so by the previous proposition, $3 = [\mathbb{Q}(\alpha) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2[\mathbb{Q}(\alpha) : \mathbb{Q}(i)]$. But this implies that $[\mathbb{Q}(\alpha) : \mathbb{Q}(i)] = 3/2$, which is impossible because it must be integral. Thus $i \notin \mathbb{Q}(\alpha)$.

We end with one last interesting result on these fields.

Proposition 7: Let F be a field. Then a and b are both algebraic over F if and only if $a + b$ and ab both are.
Proof: First suppose a and b are algebraic. Then $[F(a, b) : F]$ is finite because both $[F(a, b) : F(a)]$ and $[F(a) : F]$ are. Since we have the two chains $F \subset F(a+b) \subset F(a, b)$ and $F \subset F(ab) \subset F(a, b)$, it follows from Proposition 6 that both $[F(ab) : F]$ and $[F(a+b) : F]$ are finite as well. Second, suppose instead that $a + b$ and ab are algebraic. Then a and b are the roots of the quadratic equation $x^2 - (a + b)x + ab = 0$, so they both have degree at most 2 over $F(a + b, ab)$. Again using the previous proposition, we see that $[F(a, b) : F] = [F(a, b) : F(a + b, ab)][F(a + b, ab) : F]$; both terms on the right are finite, so $[F(a, b) : F]$ is and the two intermediate fields $F(a)$ and $F(b)$ then have finite degree as well.

These notes were based on: M. Artin, *Algebra*, Prentice Hall, New Jersey, 1991.