Notes on Algebra II

Nilay Kumar

Last updated: February 25, 2013

1 Reducibility

February 25, 2013

Let F be a field, and $F[x]$ be the ring of polynomials over F. Recall we have already shown that every ideal in $F[x]$ is principal, and that there exists a unique gcd of two non-zero polynomials. Additionally, we showed that if f and g are two relatively prime polynomials, then $f|gh \implies f|h$.

Definition 1. A polynomial $p(x) \in F[x]$ is **irreducible** if $\deg p(x) > 0$, i.e. p is not zero and not a unit, and if $p = fg$ implies that one of f, g is a unit and the other is a unit times p. In words, $p(x)$ is irreducible if it does not factor into a product of two polynomials with strictly smaller (non-zero) degree. A polynomial is said to be **reducible** if it is not irreducible.

Example 1. (Reducibility)

(i) Any linear polynomial $x + a$ is obviously irreducible.

(ii) Any quadratic polynomial is clearly reducible if and only if it has two linear factors. This is equivalent to the polynomial having a root, as long division will yield the second factor.

(iii) Similarly, a cubic polynomial is reducible if and only if it has a root.

(iv) For higher degrees, the existence of a root is not equivalent to reducibility, as we will see in the next example.

Example 2. (Simple examples)

- $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, as it has no roots in $\mathbb{Q}$. It is, however, reducible in $\mathbb{R}[x]$: $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.
- x^2+1 is irreducible in $\mathbb{R}[x]$ but reducible in $\mathbb{C}[x]$: $x^2+1 = (x-i)(x+i)$.

- $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$, but reducible in $\mathbb{R}[x]$, where we can write it as a product of $x - \sqrt[3]{2}$ and an irreducible quadratic.

- $x^4 - 4 = (x^2 - 2)(x^2 + 2)$ is reducible in $\mathbb{Q}[x]$ but has no roots!

In fact, it is generally a hard problem to determine whether an arbitrary polynomial $f(x) \in \mathbb{Q}[x]$ is irreducible. Note, however, that we can think of irreducibility in analogy to that for natural numbers, as the following dichotomy illustrates.

Remark. If $p(x) \in F[x]$ is irreducible, then for any polynomial $f \in F[x]$, either $p|f$ or p and f are relatively prime.

Proof. Let $d = \gcd(p, f)$. By definition, d divides p. However, as p is irreducible, d must either be a unit or d must be cp for c a unit. In the first case, since the gcd of p and f is a unit, p and f must be relatively prime. In the second case, since $d = cp$ by construction divides f, p must divide f. □

Corollary 1. *If $p \in F[x]$ is irreducible and $p|fg$, then either $p|f$ or $p|g$.*

Proof. By the above remark, either $p|f$ or p and f are relatively prime. If $p|f$, we are done. Otherwise, p is relatively prime to f, and by what we showed last class, $p|g$. □

Theorem 2 (Unique factorization of polynomials). *Let $f(x) \in F[x]$ with $\deg f(x) > 0$. Then there exist k irreducible polynomials in $F[x]$ such that*

$$f(x) = \prod_{i=1}^{k} p_i(x).$$

Additionally, if it is also true that $f(x) = \prod_{i=1}^{l} q_i$, then $k = l$, and after some reordering, there exist nonzero constants such that $q_i = c_i p_i$.

In other words, for any polynomial with degree greater than zero, there always exists a unique factorization into a product of irreducible polynomials.

Proof. Let us first show existence. We proceed by complete induction on the degree of f. If $\deg f = 1$, f is irreducible, and we are done. Otherwise, we assume that the theorem holds for all degrees less than n. Let $\deg f = n$. If f is irreducible, we are done. Otherwise, $f = g_1 g_2$ with $\deg g_1 < n$ and $\deg g_2 < n$. By the inductive hypothesis, g_1 and g_2 are products of irreducible polynomials, and thus f must be as well, and we are done.

The real muscle of this theorem comes in the form of uniqueness. Suppose $f = \prod_{i=1}^{k} p_i = \prod_{j=1}^{l} q_j$, with p_i, q_j reducible. We proceed by induction on k. If $k = 1$, $p_1 = q_1 \cdots q_l$. Clearly, then, $p_1 | q_1 \cdots q_l$, and thus (by induction over the statement at the beginning of lecture), p_1 must divide q_i for some i. But the q_i are irreducible and p_1 is not a constant, so $p_1 = cq_i$ for some unit c. If we now reorder terms, we can assume that $i = 1$ and we can cancel:

$$\begin{aligned} p_1 = cq_1 &= q_1 q_2 \cdots q_l \\ c &= q_2 \cdots q_l. \end{aligned}$$

But this is impossible, as the product of q's has degree greater than zero. Consequently, l must be 1, and thus $p_1 = q_1$ and we have shown that $k = l$. The general case is similar; we write $p_1 \cdots p_k = q_1 \cdots q_l$. Then $p_1 | q_1 \cdots q_l$, and so for some i, $p_1 = cq_i$. After reordering, we can write

$$\begin{aligned} cq_1 p_2 \cdots p_k &= q_1 \cdots q_l \\ cp_2 \cdots p_k &= q_2 \cdots q_l, \end{aligned}$$

and by induction, we know that $k - 1 = l - 1$. Reordering, we can write $p_= c_i q_i$ for $i = 2 \cdots k$, and we are done. □

Note that the irreducible factors need not be distinct.

Theorem 3. *Let F be a field. Let I be an ideal in $F[x]$. Then the following are equivalent:*

(i) I is a maximal ideal.

(ii) I is a prime ideal and $I \neq \{0\}$.

(iii) $I = (p)$, where p is a irreducible polynomial.

Proof. Let us first show that $(i) \implies (ii)$. Say I is maximal. Then, I must be prime. Additionally, I cannot be the zero ideal, as it is not maximal, and so we are done.

Showing $(ii) \implies (iii)$ is a little trickier. Suppose I is a prime ideal with $I \neq \{0\}$. We want to show that the ideal is generated by an irreducible element. Since every ideal in $F[x]$ is principal, $I = (p)$ for some $p \in F[x]$. Let us show that p is irreducible. First note that p cannot be a unit, because otherwise $1 \in (p)$ which implies that $(p) = F[x]$, which is not possible for prime ideals. Furthermore, $p \neq 0$, as I is assumed not to be the zero ideal.

To show that p is irreducible, we need to show that if $p = fg$ then one of f, g is a unit and the other is a unit times p. So take $p = fg$. Then, $fg \in (p) = I$. Since I is prime, either $f \in I$ or $g \in I$. Take the first case, $f \in (p)$. Then, $f = hp$ for some $h \in F[x]$, and so $p = hpg \implies 1 = hg$, i.e. h, g are units, and thus f is a unit times p. Thus, p is irreducible.

Finally, we show that $(iii) \implies (i)$. Let $I = (p)$, with p irreducible. We wish to show that I is maximal, i.e. $(p) \neq F[x]$ and if $(p) \subset J$ then either $J = (p)$ or $J = F[x]$. First note that $(p) \neq F[x]$ because $\deg p > 1$ and so it can't generate constants. Next, since J is necessarily a principal ideal, $J = (f)$, for some $f \in F[x]$. If $(p) \subset (f)$, then $p \in (f)$, so $p = fg$ for some $g \in F[x]$. But p is irreducible, so either f is a unit, in which case $J = (f) = F[x]$, or $f = cp$, for c a unit, in which case $J = (f) = (p)$. Hence, I is maximal. $\square$

This theorem is quite handy in constructing interesting fields, as the following corollary shows.

Corollary 4. *$F[x]/(f)$ is a field if and only if f is irreducible.*

Proof. This follows from above theorem and the fact that $F[x]/(f)$ is a field if and only if (f) is a maximal ideal. $\square$

This allows us to show that certain rings are, in fact, fields – something that may not have been obvious – or, in fact, to find wholly new fields.

Example 3.

- $\mathbb{Q}[x]/(x^2-2)$ is a field, as x^2-2 is irreducible in $\mathbb{Q}[x]$, and its elements, by what we know about long division, are of the form $c + d\alpha$, where $\alpha = x + (x^2 - 2)$. In addition, $\alpha^2 = 2$.

- $\mathbb{R}[x]/(x^2+1)$ is a field, as x^2+1 is irreducible in $\mathbb{R}[x]$, and its elements are of the form $c + d\alpha$ where $\alpha = x + (x^2 + 1)$ satisfies $\alpha^2 = -1$.

- $\mathbb{Q}[x]/(x^3-2)$ is a field, as x^3-2 is irreducible in $\mathbb{Q}[x]$, and its elements are of the form $c + d\alpha + e\alpha^2$, where $\alpha = x + (x^3 - 2)$ satisfies $\alpha^3 = 2$. We often rewrite the elements as $c + d\sqrt[3]{2} + e\sqrt[3]{2}^2$.

- Take the finite field $\mathbb{F}_2$ and the polynomial $x^2 + x + 1 \in \mathbb{F}_2$. Since the only members of $\mathbb{F}_2$ are 0 and 1, it should be clear that this polynomial has no roots, and thus is irreducible in $\mathbb{F}_2[x]$. Consequently, $E = \mathbb{F}_2[x]/(x^2+x+1)$ is a field. Its elements are of the form $c+d\alpha$, where of course $c, d \in \mathbb{F}_2$ and $\alpha = x+(x^2+x+1)$, which satisfies the property that $\alpha^2 = -\alpha - 1 = \alpha + 1$. E has four elements (since c and d can each take 2 values).