2.2 Divisibility and Irreducibility

RECALL: The division algorithm in $\mathbb{Z}$: if m is a positive integer and n is any integer, then there exist unique integers q and r (respectively called the quotient and remainder on dividing n by m) with $0 \leqslant r < m$ and

$$n = mq + r.$$

We will discuss in the seminar how the division algorithm for $\mathbb{Z}$ can be proved (although it is not very difficult to persuade yourself that it is true). In this section we will see that for a field F, the polynomial ring $F[x]$ has many properties in common with the ring $\mathbb{Z}$ of integers. The first of these is a version of the division algorithm.

Definition 2.2.1 *Let* $f(x)$, $g(x)$ *be polynomials in* $F[x]$. *We say that* $g(x)$ divides $f(x)$ *in* $F[x]$ *if* $f(x) = g(x)q(x)$ *for some* $q(x) \in F[x]$ *(i.e. if* $f(x)$ *is a multiple of* $g(x)$ *in* $F[x]$*).*

Theorem 2.2.2 (Division Algorithm in $F[x]$). *Let* F *be a field and let* $f(x)$ *and* $g(x)$ *be non-zero polynomials in* $F[x]$ *with* $g(x) \neq 0$. *respectively. Then there exist* unique *polynomials* $q(x)$ *and* $r(x)$ *in* $F[x]$ *with* $r(x) = 0$ *or* $\deg(r(x)) < \deg(g(x))$ *and*

$$f(x) = g(x)q(x) + r(x).$$

NOTES

1. In this situation $q(x)$ and $r(x)$ are called the quotient and remainder upon dividing $f(x)$ by $g(x)$.
2. There are two separate assertions to be proved - the existence of such a $q(x)$ and $r(x)$, and their uniqueness.

Proof: (Existence) Define S to be the set of all polynomials in $F[x]$ of the form $f(x) - g(x)h(x)$ where $s(x) \in F[x]$. So S is the set of all those polynomials in $F[x]$ *that differ from* $f(x)$ *by a multiple of* $g(x)$. Our goal for the existence part of the proof is show that either the zero polynomial belongs to S, or S contains some element whose degree is less than that of $g(x)$.

1. If $0 \in S$ then $f(x) - g(x)h(x) = 0$ for some $h(x) \in F[x]$, so $f(x) = g(x)h(x)$ and we can take $q(x) = h(x)$ and $r(x) = 0$.
2. If $0 \notin S$, let $r(x)$ be an element of minimal degree in S.

Let m denote the degree of $g(x)$ and write

$$g(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0, \ a_m \neq 0.$$

Let $t = \deg(r(x))$ and write

$$r(x) = b_t x^t + b_{t-1}x^{t-1} + \cdots + b_1 x + b_0,\ b_t \neq 0.$$

We claim that $t < m$. We know since $r(x) \in S$ that there exists a polynomial $h(x) \in F[x]$ for which

$$r(x) = f(x) - g(x)h(x).$$

Thus

$$b_t x^t + b_{t-1}x^{t-1} + \cdots + b_1 x + b_0 = f(x) - g(x)h(x).$$

If $t \geqslant m$ then $t - m \geqslant 0$. Also $a_m \neq 0$ in F, so a_m has an inverse $1/a_m$ in F and the element b_t/a_m belongs to F. Now subtract the polynomial $g(x)(b_t/a_m)x^{t-m}$ (which has leading term $b_t x^t$) from both sides of the above equation to get

$$b_t x^t + \cdots + b_1 x + b_0 - g(x)(b_t/a_m)x^{t-m} = f(x) - g(x)h(x) - g(x)(b_t/a_m)x^{t-m}.$$

The left side of the above equation is $r_1(x)$, a polynomial of degree less than t in $F[x]$. The right hand side is $f(x) - g(x)h_1(x)$ where $h_1(x) = h(x) + (b_t/a_m)x^{t-m}$. Thus $r_1(x)$ belongs to S, contrary to the choice of $r(x)$ as an element of minimal degree in S. We conclude that $t < m$ and

$$f(x) = g(x)h(x) + r(x)$$

is a description of $f(x)$ of the required type. This proves the existence.

QUESTIONS FOR THE SEMINAR:

1. How do we know that $r_1(x)$ above has degree less than t?
2. Why can we conclude that $t < m$ at the third last line above?
3. Where does the proof use the fact that F is a field?

Uniqueness: Suppose that

$$\begin{aligned} f(x) &= g(x)q_1(x) + r_1(x),\ \deg(r_1(x)) < m \\ \text{and } f(x) &= g(x)q_2(x) + r_2(x),\ \deg(r_2(x)) < m. \end{aligned}$$

Then

$$0 = g(x)(q_1(x) - q_2(x)) + (r_1(x) - r_2(x)) \Longrightarrow g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x).$$

Now $g(x)(q_1(x) - q_2(x))$ is either zero or a polynomial of degree at least m, and $r_2(x) - r_1(x)$ is either zero or a polynomial of degree less than m. Hence these two can be equal only if they are both zero, which means $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$. This completes the proof. □

QUESTION FOR THE SEMINAR: Why can we say that if $g(x)(q_1(x) - q_2(x)) = 0$ then it must follow that $q_1(x) = q_2(x)$?

Let $f(x) \in R[x]$ for some ring R; suppose

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

If $\alpha \in R$ then we let $f(\alpha)$ denote the element

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0$$

of R. Thus associated to the polynomial $f(x)$ we have a function from R to R sending α to $f(\alpha)$. Forming the element $f(\alpha)$ is called *evaluating* the polynomial $f(x)$ at α.

Definition 2.2.3 *In the above context,* $\alpha \in R$ *is a* root *of* $f(x)$ *if* $f(\alpha) = 0$.

Theorem 2.2.4 *(The Factor Theorem) Let* $f(x)$ *be a polynomial of degree* $n \geqslant 1$ *in* $F[x]$ *and let* $\alpha \in F$. *Then* α *is a root of* $f(x)$ *if and only if* $x - \alpha$ *divides* $f(x)$ *in* $F[x]$.

Proof: By the division algorithm (Theorem 2.2.2), we can write

$$f(x) = q(x)(x - \alpha) + r(x),$$

where $q(x) \in F[x]$ and either $r(x) = 0$ or $r(x)$ has degree zero and is thus a non-zero element of F. So $r(x) \in F$; we can write $r(x) = \beta$. Now

$$\begin{aligned} f(\alpha) &= q(\alpha)(\alpha - \alpha) + \beta \\ &= 0 + \beta \\ &= \beta. \end{aligned}$$

Thus $f(\alpha) = 0$ if and only if $\beta = 0$, i.e. if and only if $r(x) = 0$ and $f(x) = q(x)(x-\alpha)$ which means $x - \alpha$ divides $f(x)$. □

QUESTION FOR THE SEMINAR:
This actually proves more than the statement of the theorem - explain.

Now that we have some language for discussing divisibility in polynomial rings, we can also think about factorization. In $\mathbb{Z}$, we are used to calling an integer *prime* if it does not have any interesting factorizations. In polynomial rings, we call a polynomial *irreducible* if it does not have any interesting factorizations.

QUESTION FOR THE SEMINAR:
What does “interesting” mean in this context?

Definition 2.2.5 *Let* F *be a field and let* $f(x)$ *be a non-constant polynomial in* $F[x]$*. Then* $f(x)$ *is* irreducible *in* $F[x]$ *(or irreducible over* F*) if* $f(x)$ *cannot be expressed as the product of two factors both of degree at least 1 in* $F[x]$*. Otherwise* $f(x)$ *is* reducible *over* F*.*

NOTES:

1. Any polynomial $f(x) \in F[x]$ can be factorized (in an uninteresting way) by choosing $a \in F^{\times}$ and writing
$$f(x) = a(a^{-1}f(x).$$
This is not considered to be a proper factorization of $f(x)$.

2. Every polynomial of degree 1 is irreducible.

3. It is possible for a polynomial that is irreducible over a particular field to be reducible over a larger field. For example x^2-2 is irreducible in $\mathbb{Q}[x]$. However it is not irreducible in $\mathbb{R}[x]$, since here $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$. Therefore when discussing irreducibility, it is important to specify what field we are talking about (sometimes this is clear from the context).

4. The only irreducible polynomials in $\mathbb{C}[x]$ are the linear (i.e. degree 1) polynomials. This is basically the Fundamental Theorem of Algebra, which states that every non-constant polynomial with coefficients in $\mathbb{C}$ has a root in $\mathbb{C}$.

Let $f(x)$ be a polynomial of degree $\geqslant 2$ in $F[x]$. If $f(x)$ has a root α in F then $f(x)$ is not irreducible in $F[x]$ since it has $x-\alpha$ as a proper factor. This statement has a partial converse.

Theorem 2.2.6 *Let* $f(x)$ *be a quadratic or cubic polynomial in* $f(x)$*. Then* $f(x)$ *is irreducible in* $F[x]$ *if and only if* $f(x)$ *has no root in* F*.*

Proof: Since $f(x)$ is quadratic or cubic any proper factorization of $f(x)$ in $F[x]$ involves at least one linear (i.e. degree 1) factor. Suppose that $r(x) = ax + b$ is a linear factor of $f(x)$ in $F[x]$. Then we have $f(x) = r(x)g(x)$ for some $g(x)$ in $F[x]$. Since F is a field we can rewrite this as
$$f(x) = (x + b/a)(ag(x)).$$
Thus $x - (-b/a)$ divides $f(x)$ in $F[x]$ and by Theorem 2.2.4 $-b/a$ is a root of $f(x)$ in F. □

QUESTION FOR THE SEMINAR: Theorem 2.2.6 certainly does not hold for polynomials of degree 4 or higher. That is, for a polynomial of degree 4 or more, having no roots in a particular field does not mean being irreducible over that field. Give an example to demonstrate this.

In general, deciding whether a given polynomial is reducible over a field or not is a difficult problem. We will look at this problem in the case where the field of coefficients is $\mathbb{Q}$. The problem of deciding reducibility in $\mathbb{Q}[x]$ is basically the same as that of deciding reducibility in $\mathbb{Z}[x]$, as the following discussion will show.

Lemma 2.2.7 *For a field* F, *let* $a \in F^\times$ *and let* $f(x) \in F[x]$. *Then* $f(x)$ *is reducible in* $F[x]$ *if and only if* $af(x)$ *is reducible in* $F[x]$.

Proof: Exercise for the seminar.

Note that any polynomial in $\mathbb{Q}[x]$ can be multiplied by a non-zero integer to produce a polynomial in $\mathbb{Z}[x]$. Then by Lemma 2.2.7 the problem of deciding reducibility in $\mathbb{Q}[x]$ is the same as that of deciding reducibility over $\mathbb{Q}$ for polynomials in $\mathbb{Z}[x]$.
Suppose that $f(x)$ is a polynomial with coefficients in $\mathbb{Z}$. Surprisingly, $f(x)$ has a proper factorization with factors in $\mathbb{Q}[x]$ if and only if $f(x)$ has a proper factorization with factors (of the same degree) that belong to $\mathbb{Z}[x]$. This fact is a consequence of Gauss's lemma which is discussed below. It means that a polynomial with integer coefficients is irreducible over $\mathbb{Q}$ provided that it is irreducible over $\mathbb{Z}$. This is good news because irreducibility over $\mathbb{Z}$ is in principle easier to decide.

QUESTION FOR THE SEMINAR: Why is irreducibility over $\mathbb{Z}$ is in principle easier to decide than irreducibility over $\mathbb{Q}$, for a polynomial with integer coefficients?

Definition 2.2.8 *A polynomial in* $\mathbb{Z}[x]$ *is called* primitive *if the greatest common divisor of all its coefficients is 1.*

EXAMPLE
$3x^4 + 6x^2 - 2x - 2$ is primitive.
$3x^4 + 6x^2 = 18x$ is not primitive, since 3 divides each of the coefficients.

Theorem 2.2.9 *(Gauss's Lemma) : Let* $f(x)$ *and* $g(x)$ *be primitive polynomials in* $\mathbb{Z}[x]$. *Then their product is again primitive.*

Proof: We need to show that no prime divides all the coefficients of $f(x)g(x)$. We can write

$$\begin{aligned} f(x) &= a_s x^s + a_{s-1}x^{s-1} + \cdots + a_1 x + a_0,\ a_s \neq 0, \\ f(x) &= b_t x^t + b_{t-1}x^{t-1} + \cdots + b_1 x + b_0,\ b_t \neq 0. \end{aligned}$$

Let p be a prime. Since $f(x)$ and $g(x)$ are primitive we can choose k and m to be the least integers for which p does not divide a_k and p does not divide b_m. Now look at the coefficient of x^{k+m} in $f(x)g(x)$. This is

$$a_{k+m}b_0 + \cdots + a_{k+1}b_{m-1} + a_k b_m + a_{k-1}b_{m+1} + \cdots + a_0 b_{k+m}.$$

Since $p|b_i$ for $i < m$ and $p|a_i$ for $i < k$, every term in the above expression is a multiple of p except for $a_k b_m$ which is definitely not. Thus p does not divide the coefficient of x^{k+m} in $f(x)g(x)$, p does not divide all the coefficients in $f(x)g(x)$ and $f(x)g(x)$ is primitive. □

Corollary 2.2.10 *Suppose* $f(x)$ *is a polynomial of degree* $\geqslant 2$ *in* $\mathbb{Z}[x]$. *Then* $f(x)$ *has a proper factorization in* $\mathbb{Q}[x]$ *if and only if it has a proper factorization in* $\mathbb{Z}[x]$, *with factors of the same degrees.*

This means : if $f(x)$ can be properly factorized in $\mathbb{Q}[x]$ it can also be properly factorized in $\mathbb{Z}[x]$; if it can be written as the product of two polynomials of degree $\geqslant 1$ with rational coefficients, it can be written as the product of two such polynomials with *integer* coefficients.
Proof: $\Longleftarrow$: This direction is obvious, since any factorization in $\mathbb{Z}[x]$ is a factorization in $\mathbb{Q}[x]$.
$\Longrightarrow$: First assume that $f(x)$ is primitive in $\mathbb{Z}[x]$.
Suppose that $f(x) = g_1(x)h_1(x)$ where $g_1(x)$ and $h_1(x)$ are polynomials of degree $k \geqslant 1$ and $m \geqslant 1$ in $\mathbb{Q}[x]$. Then we can find integers a_1 and b_1 for which $a_1 g_1(x)$ and $b_1 h_1(x)$ are elements of $\mathbb{Z}[x]$, both of degree at least 1. Let d_1 and d_2 denote the greatest common divisors of the coefficients in $a_1 g_1(x)$ and $b_1 h_1(x)$ respectively. Then $(a_1/d_1)g_1(x)$ and $(b_1/d_2)h_1(x)$ are primitive polynomials in $\mathbb{Z}[x]$. Call these polynomials $g(x)$ and $h(x)$ respectively, and let a and b denote the rational numbers a_1/d_1 and b_1/d_2. Now

$$f(x) = g_1(x)h_1(x) \Longrightarrow abf(x) = ag_1(x)bh_1(x) = g(x)h(x).$$

Since $g(x)h(x) \in \mathbb{Z}[x]$ and $f(x)$ is primitive it follows that ab is an integer. Furthermore since $g(x)h(x)$ is primitive by Theorem 2.2.9, $abf(x)$ is primitive. This means $ab = 1$ or -1. Now either $ab = 1$ and $f(x) = g(x)h(x)$ or $ab = -1$ and $f(x) = (-g(x))h(x)$. Thus $f(x)$ factorizes in $\mathbb{Z}[x]$.
Finally, if $f(x)$ is not primitive we can write $f(x) = df_1(x)$ where d is the gcd of the coefficients in $f(x)$ and $f_1(x)$ is primitive. By Lemma 2.2.7 $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if $f_1(x)$ is. By the above, $f_1(x)$ factorizes in $\mathbb{Q}[x]$ if and only if it factorizes in $\mathbb{Z}[x]$. Finally, $f(x)$ clearly factorizes in $\mathbb{Z}[x]$ if $f_1[x]$ does. □

Theorem 2.2.9 and Corollary 2.2.10 make the reducibility question in $\mathbb{Q}[x]$ much easier.

Theorem 2.2.11 *Let* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *be a polynomial of degree* $n \geqslant 2$ *in* $\mathbb{Z}[x]$, *with* $a_0 \neq 0$. *If* $f(x)$ *has a root in* $\mathbb{Q}$ *this root has the form* b/a *where* a *and* b *are integers (positive or negative) for which* $b|a_0$ *and* $a|a_n$.

Proof: By Theorem 2.2.4, $f(x)$ has a root in $\mathbb{Q}$ only if $f(x)$ has a linear factor in $\mathbb{Q}[x]$. By Corollary 2.2.10 this happens only if

$$f(x) = (ax + b)(g(x))$$

where $a, b \in \mathbb{Z}$, $a \neq 0$ and $g(x) \in \mathbb{Z}[x]$. Then if

$$g(x) = c_{n-1}x^{n-1} + \cdots + c_1 x + c_0,$$

we have $ac_{n-1} = a_n$ and $b_0 c_0 = a_0$. Thus $a|a_n$, $b|a_0$ and $-b/a$ is a root of $f(x)$ in $\mathbb{Q}$. $\square$

Example: Let $f(x) = \frac{3}{5}x^3 + 2x - 1$ in $\mathbb{Q}[x]$. Determine if $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Solution: By Lemma 2.2.7 $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if $5f(x) = 3x^3 + 10x - 5$ is irreducible. By Theorem 2.2.6 this would mean having no root in $\mathbb{Q}$. By Theorem 2.2.11 possible roots of $5f(x)$ in $\mathbb{Q}$ are

$$1, -1, 5, -5, \frac{1}{3}, -\frac{1}{3}, \frac{5}{3}, -\frac{5}{3}.$$

It is easily checked that none of these is a root. Since $f(x)$ is cubic it follows that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

NOTE: A polynomial is called *monic* if its leading coefficient is 1. If $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$ then any rational roots of $f(x)$ are integer divisors of the constant term (provided that this is not zero).

EXAMPLE: Decide if the polynomial $f(x) = x^5 + 3x^4 - 3x^3 - 8x^2 + 3x - 2$ is irreducible in $\mathbb{Q}[x]$.

Solution : Possible rational roots of $f(x)$ are integer divisors of the constant term -2 - i.e. $1, -1, 2, -2$. Inspection of these possibilities reveals that -2 is a root. Thus $f(x)$ is reducible in $\mathbb{Q}[x]$.

NOTE: Since $f(x)$ has degree 5, a discovery that $f(x)$ had no rational roots would not have told us anything about the irreducibility or not of $f(x)$ over $\mathbb{Q}$.
There is one known criterion for irreducibility over $\mathbb{Q}$ that applies to polynomials of high degree, but it only applies to polynomials with a special property.

Theorem 2.2.12 *(The Eisenstein irreducibility Criterion) Let* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *be a polynomial in* $\mathbb{Z}[x]$ *where* $a_n \neq 0$*, and* $n \geqslant 2$*. Suppose that there exists a prime number* p *for which*

- p *divides all of* $a_0, a_1, \ldots, a_{n-1}$
- p *does not divide* a_n
- p^2 *does not divide* a_0.

Then $f(x)$ *is irreducible in* $\mathbb{Q}[x]$.

For example the Eisenstein test says that $2x^4 - 3x^3 + 6x^2 - 12x + 3$ is irreducible in $\mathbb{Q}[x]$ since the prime 3 divides all the coefficients except the leading one, and 9 does not divide the constant term.

Proof of Theorem 2.2.12: Assume (in the hope of contradiction) that $f(x)$ is reducible and write

$$f(x) = (\underbrace{b_s x^s + \cdots + b_1 x + b_0}_{g(x)})(\underbrace{c_t x^t + \cdots + c_1 x + c_0}_{h(x)})$$

where $g(x), h(x) \in \mathbb{Z}[x],\ b_s \neq 0,\ c_t \neq 0,\ s \geqslant 1,\ t \geqslant 1$ and $s + t = n$.
Now $b_0 c_0 = a_0$ which means p divides exactly one of b_0 and c_0, as p^2 does not divide a_0. Suppose $p|b_0$ and $p \not| c_0$. Now $a_1 = b_1 c_0 + b_0 c_1$, which means $p|b_1$ since p divides a_1 and b_0 but not c_0. Similarly looking at a_2 shows that p must divide b_2. However p does not divide all the b_i - it does not divide b_s, otherwise it would divide $a_n = b_s c_t$.
Now let k be the least for which $p \not| b_k$. Then $k \leqslant s \Longrightarrow k < n$ and

$$a_k = b_k c_0 + \underbrace{b_{k-1} c_1 + \cdots + b_0 c_k}_{\text{all multiplesof } p}$$

Now $p \not| b_k c_0$ since $p \not| b_k$ and $p \not| c_0$. Since the remaining terms in the above description of a_k are all multiples of p, it follows that $p \not| a_k$, contrary to hypothesis. We conclude that any polynomial in $\mathbb{Z}[x]$ satisfying the hypotheses of the theorem is irreducible in $\mathbb{Q}[x]$. □

NOTE: Theorem 2.2.12 says nothing at all about polynomials in $\mathbb{Z}[x]$ for which no prime satisfies the requirements in the statement.