9. Gauss Lemma

Obviously it would be nice to have some more general methods of proving that a given polynomial is irreducible. The first is rather beautiful and due to Gauss. The basic idea is as follows. Suppose we are given a polynomial with integer coefficients. Then it is natural to also consider this polynomial over the rationals. Note that it is much easier to prove that this polynomial is irreducible over the integers than it is to prove that it is irreducible over the rationals. For example it is clear that

$$x^2 - 2$$

is irreducible over the integers. In fact it is irreducible over the rationals as well, that is, $\sqrt{2}$ is not a rational number.

First some definitions.

Definition 9.1. *Let R be a commutative ring and let $a_1, a_2, \ldots, a_k$ be a sequence of elements of R. The **gcd** of $a_1, a_2, \ldots, a_k$ is an element $d \in R$ such that*

(1) $d|a_i$, for all $1 \leq i \leq k$.
(2) If $d'|a_i$, for all $1 \leq i \leq k$, then $d'|d$.

Lemma 9.2. *Let R be a UFD.*

Then the gcd of any sequence $a_1, a_2, \ldots, a_k$ of elements of R exists.

Proof. There are two obvious ways to proceed.

The first is to take a common factorisation of each a_i into a product of powers of primes, as in the case $k = 2$.

The second is to recursively construct the gcd, by setting d_i to be the gcd of d_{i-1} and a_i and taking $d_1 = a_1$. In this case $d = d_k$ will be a gcd for the whole sequence $a_1, a_2, \ldots, a_k$. □

Definition 9.3. *Let R be a UFD and let $f(x)$ be a polynomial with coefficients in R.*

*The **content** of $f(x)$, denoted $c(f)$, is the gcd of the coefficients of f.*

Example 9.4. *Let $f(x) = 24x^3 - 60x + 40$. Then the content of f is 4. Thus*

$$f(x) = 4(6x^3 - 15x + 10).$$

Lemma 9.5. *Let R be a UFD. Then every element of $R[x]$ has a factorisation of the form*

$$cf,$$

where $c \in R$ and the content of f is one.

Proof. Obvious. □

Here is the key result.

Proposition 9.6. *Let R be a UFD. Suppose that g and $h \in R[x]$ and let $f(x) = g(x)h(x)$.*

Then the content of f and the content of g times the content of h are associates.

Proof. It is clear that the content of g divides the content of f. Therefore we may assume that the content of g and h is one, and we only have to prove that the same is true for f.

As R is a UFD, we just have to show that no prime p divides the content of f. We may write

$$g(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0 \qquad \text{and} \qquad h(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0.$$

As the content of g is one, at least one coefficient of g is not divisible by p. Let i be the first such, so that p divides a_k, for $k < i$ whilst p does not divide a_i. Similarly pick j so that p divides b_k, for $k < j$, whilst p does not divide b_j.

Consider the coefficient of x^{i+j} in f. This is equal to

$$a_0 b_{i+j} + a_1 b_{i+j-1} + \cdots + a_{i-1}b_{j+1} + a_i b_j + a_{i+1}b_{j+1} + \cdots + a_{i+j}b_0.$$

Note that p divides every term of this sum, except the middle one $a_i b_j$. Thus p does not divide the coefficient of x^{i+j}. □

Theorem 9.7 (Gauss' Lemma)**.** *Let R be a UFD and let $f(x) \in R[x]$. Let F be the field of fractions of R. Suppose that the content of f is one and that we may write $f(x) = u_1(x)v_1(x)$, where $u_1(x)$ and $v_1(x)$ are in $F[x]$.*

Then we may find $u(x)$ and $v(x)$ in $R[x]$ such that

$$f(x) = u(x)v(x)$$

where $u(x)$ and $v(x)$ are multiples of $u_1(x)$ and $v_1(x)$.

In particular if f is irreducible in $R[x]$ then it is irreducible in $F[x]$.

Proof. We have

$$f(x) = u_1(x)v_1(x).$$

Now clear denominators. That is, multiply through by the product c of all the denominators in $u_1(x)$ and $v_1(x)$. In this way we get an expression of the form

$$cf(x) = u_2(x)v_2(x),$$

where now u_2 and v_2 belong to $R[x]$. Now write

$$u_2(x) = au(x) \qquad \text{and} \qquad v_2(x) = bv(x),$$

where u and $v \in R[x]$ have content one. We get

$$cf(x) = abu(x)v(x).$$

By (9.6) we ab and c are associates. Thus, possibly multiplying u by an invertible element, we have

$$f(x) = u(x)v(x). \qquad \square$$

Corollary 9.8. *Let R be a UFD.*
Then $R[x]$ is a UFD.

Proof. It is clear that the Factorisation algorithm terminates (or what comes to the same thing, the set of principal ideals satisfies the ACC), by induction on the degree.

Therefore it suffices to prove that irreducible implies prime.

Suppose that $f(x) \in R[x]$ is irreducible. If f has degree zero, then it is an irreducible element of R and hence a prime element of R and there is nothing to prove.

Otherwise we may assume that the content of f is one. By Gauss' Lemma, f is not only irreducible in $R[x]$ but also in $F[x]$. But then f is a prime element of $F[x]$ as $F[x]$ is a UFD.

Now suppose that f divides gh. As $f(x)$ is a prime in $F[x]$, f divides g or h in $F[x]$. Suppose it divides g. Then we may write

$$g = fk,$$

some $k \in F[x]$. As in the proof of Gauss' Lemma, this means we may write

$$g = fk',$$

some $k' \in R[x]$. But then $f(x)$ divides g in $R[x]$. $\square$

Corollary 9.9. *$\mathbb{Z}[x]$ is a UFD.*

Definition 9.10. *Let R be a commutative ring and let $x_1, x_2, \ldots, x_n$ be indeterminates.*

*A **monomial** in $x_1, x_2, \ldots, x_n$ is a product of powers. If $I = (d_1, d_2, \ldots, d_n)$, then let*

$$x^I = \prod x_i^{d_i}.$$

*The **degree** d of a monomial is the sum of the degrees of the individual terms, $\sum d_i$.*

*The **polynomial ring** $R[x_1, x_2, \ldots, x_n]$ is equal to the set of all finite formal sums*

$$\sum_I a_I x^I,$$

with the obvious addition and multiplication. The ***degree of a polynomial*** *is the maximum degree of a monomial term that appears with non-zero coefficient.*

Example 9.11. *Let x and y be indeterminates. A typical element of $\mathbb{Q}[x, y]$ might be*

$$x^2 + y^2 - 1.$$

This has degree 2. Note that xy also has degree two. A more complicated example might be

$$\frac{2}{3}x^3 - 7xy + y^5,$$

a polynomial of degree 5.

Lemma 9.12. *Let R be a commutative ring and let $x_1, x_2, \ldots, x_n$ be indeterminates. Let $S = R[x_1, x_2, \ldots, x_{n-1}]$. Then there is a natural isomorphism*

$$R[x_1, x_2, \ldots, x_n] \simeq S[x_n].$$

Proof. Both sides statisfy a universal property; given any ring homomorphism $\phi\colon R \longrightarrow T$ and any elements $a_1, a_2, \ldots, a_n \in T$ there is a unique ring homomorphism from the polynomial ring in $x_1, x_2, \ldots, x_n$ extending ϕ and sending x_i to a_i. Thus there is a natural isomorphism. □

To illustrate why (9.12) is true, it will probably help to give an example. Consider the polynomial

$$\frac{2}{3}x^3 - 7xy + y^5.$$

Consider this as a polynomial in y, whose coefficients lie in the ring $R[x]$. That is

$$y^5 + (-7x)y + 2/3x^3 \in R[x][y].$$

Corollary 9.13. *Let R be a UFD. Then $R[x_1, x_2, \ldots, x_n]$ is a UFD.*

Proof. By induction on n. The case $n = 1$ is (9.8).

Set $S = R[x_1, x_2, \ldots, x_{n-1}]$. By induction S is a UFD. But then $S[x] \simeq R[x_1, x_2, \ldots, x_n]$ is a UFD. □

Now we give a way to prove that polynomials with integer coefficients are irreducible.

Lemma 9.14. *Let*

$$\phi\colon R \longrightarrow S$$

be a ring homomorphism.

Then there is a unique ring homomorphism

$$\psi\colon R[x] \longrightarrow S[x]$$

which makes the following diagram commute

$$\begin{array}{ccc} R & \xrightarrow{\phi} & S \\ \downarrow & & \downarrow \\ R[x] & \xrightarrow{\psi} & S[x] \end{array}$$

and which sends x to x.

Proof. Let

$$f\colon R \longrightarrow S[x]$$

be the composition of ϕ with the natural inclusion of S into $S[x]$. By the universal property of $R[x]$, there is a unique ring homomorphism

$$\psi\colon R[x] \longrightarrow S[x].$$

The rest is clear. □

Theorem 9.15 (Eisenstein's Criteria)**.** *Let*

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

be a polynomial with integer coefficients. Suppose that there is a prime p such that p divides a_i, $i \leq n-1$, p does not divide a_n and p^2 does not divide a_0.

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

Proof. Note that the content of f is not divisible by p. Pulling out the content from f we may assume that the content is one. By Gauss' Lemma, it suffices to prove that f is irreducible over $\mathbb{Z}$.

Suppose not. Then we may find two polynomials $g(x)$ and $h(x)$, of positive degree, with integral coefficients, such that

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

Suppose that

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \\ g(x) &= b_d x^d + b_{d-1}x^{d-1} + \cdots + b_0 \\ h(x) &= c_e x^e + c_{e-1}x^{e-1} + \cdots + c_0. \end{aligned}$$

for some n, d and $e > 1$. As $a_n = b_d c_e$ and a_n is not divisible by p, then neither is b_d nor c_e.

Consider the natural ring homomorphism

$$\mathbb{Z} \longrightarrow \mathbb{F}_p.$$

This induces a ring homomorphism

$$\mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x].$$

It is convenient to denote the image of a polynomial $g(x)$ as $\bar{g}(x)$. As we have a ring homomorphism,

$$\bar{f}(x) = \bar{g}(x)\bar{h}(x).$$

Since the leading coefficient of f is not divisible by p, $\bar{f}(x)$ has the same degree as $f(x)$, and the same holds for $g(x)$ and $h(x)$. On the other hand, every other coefficient of $f(x)$ is divisible by p, and so

$$\bar{f}(x) = \bar{a}_n x^n.$$

Since $\mathbb{F}_p$ is a field, $\mathbb{F}_p[x]$ is a UFD and so $\bar{g}(x) = \bar{b}_d x^d$ and $\bar{h}(x) = \bar{c}_e x^e$. It follows that every other coefficient of $g(x)$ and $h(x)$ is divisible by p. In particular b_0 and c_0 are both divisible by p, and so, as $a_0 = b_0 c_0$, a_0 must be divisible by p^2, a contradiction. □

Example 9.16. *Let*

$$f(x) = 2x^7 - 15x^6 + 60x^5 - 18x^4 - 9x^3 + 45x^2 - 3x + 6.$$

Then $f(x)$ is irreducible over $\mathbb{Q}$. We apply Eisenstein with $p = 3$. Then the top coefficient is not divisible by 3, the others are, and the smallest coefficient is not divisible by $9 = 3^2$.

Lemma 9.17. *Let p be a prime. Then*

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

is irreducible over $\mathbb{Q}$.

Proof. By Gauss' Lemma, it suffices to prove that $f(x)$ is irreducible over $\mathbb{Z}$.

First note that

$$f(x) = \frac{x^p - 1}{x - 1},$$

as can be easily checked. Consider the change of variable

$$y = x - 1.$$

As this induces an automorphism

$$\mathbb{Z}[x] \longrightarrow \mathbb{Z}[x]$$

by sending x to $x-1$, this will not alter whether or not f is irreducible. In this case

$$\begin{aligned} g(y) &= \frac{(y+1)^p - 1}{y} \\ &= y^{p-1} + \binom{p}{1} y^{p-2} + \binom{p}{2} y^{p-3} + \cdots + \binom{p}{p-1} \\ &= y^{p-1} + py^{p-2} + \cdots + p. \end{aligned}$$

Note that $\binom{p}{i}$ is divisible by p, for all $1 \leq i < p$, and the constant coefficient is not divisible by p^2, so that we can apply Eisenstein to $f(y)$, using the prime p. $\square$