21MAB143 Rings and Polynomials: Week 8

1 Irreducible polynomials in one variable

The basic question we want to explore in this week's lectures is how to tell whehter a polynomial in one variable can be "factored". Let's start by making precise what that means.

Definition 1.1. *Let* R *be a commutative ring. An element* $r \in R$ *is a* **unit** *if it has a multiplicative inverse* r^{-1}*. A nonzero element* $a \in R$ *is said to be* **irreducible** *if it is not a unit, and whenever* $a = bc$ *for some elements* $b, c \in R$*, either* b *or* c *is a unit.*

What is this definition saying? Notice that if r is a unit in the ring R, then for any other element $a \in R$ we can write $a = r \cdot (r^{-1} \cdot a)$, so r divides a. But this should not count as a "true" factorisation of a. Our definition says that irreducible elements are those which can only be factored in this "fake" way using units: they have no "true" factorisations.

Example This week we will focus on the case of a polynomial ring $K[x]$ over a field K. In Problem Sheet 2 Question 1 we showed that the units in the ring $K[x]$ are exactly the nonzero constant polynomials, or equivalently the polymomials p with $\deg(p) = 0$.

So according to the above definition, a nonconstant polynomial $f \in K[x]$ is irreducible if, whenever we have $f = gh$ for polynomials $g, h \in K[x]$, then either g or h is a constant polynomial. An equivalent way to say this is:

f *is irreducible in* $K[x]$ *if we cannot write* $f = gh$ *where both* g *and* h *are polynomials in* $K[x]$ *with smaller degree than that of* f*.*

Important remark: For a given polynomial, the question of irreducibility depends crucially on which ring we are talking about. For example, given a polynomial $f \in \mathbf{Q}[x]$ we can also view it as an element of $\mathbf{R}[x]$ or $\mathbf{C}[x]$. However, it may well be the case that f is irreducible in $\mathbf{Q}[x]$ whereas it is reducible (meaning not irreducible) in $\mathbf{R}[x]$ or $\mathbf{C}[x]$. This is not too surprising: f might not have factors with coefficients in $\mathbf{Q}$, yet have factors with coefficients in $\mathbf{R}$ or in $\mathbf{C}$. Similarly, a polynomial with real coefficients may be irreducible in $\mathbf{R}[x]$ but reducible in $\mathbf{C}[x]$. We will see examples of both kinds shortly.

1.1 Irreducibility in $C[x]$

The question of which polynomials in $\mathbf{C}[x]$ are irreducible has a very simple answer.

Theorem 1.2 (Fundamental Theorem of Algebra)**.** *Every nonconstant polynomial* $f \in \mathbf{C}[x]$ *factors into a product of linear factors in* $\mathbf{C}[x]$*:*

$$f = a(x - z_1) \cdots (x - z_n)$$

where $a \in \mathbf{C}$ *is the leading coefficient of* f*,* n *is the degree* $\deg(f)$*, and* $z_1, \ldots, z_n$ *are the complex roots of* f *(counted with multiplicity).*

In particular, f *is irreducible if and only if* $\deg(f) = 1$*.*

In spite of its name, this is really more a theorem of analysis, using some completeness properties of the complex numbers in its proof. We will not say anything more than this!

1.2 Irreducibility in $\mathbf{R}[x]$

The question of irreducibility is a bit (but not a lot) more interesting in the ring $\mathbf{R}[x]$. Here the main general statement is the following:

Theorem 1.3. *If* $f \in \mathbf{R}[x]$ *is an irreducible polynomial, then* f *has degree 1 or 2.*

Proof. Let $f \in \mathbf{R}[x]$ be a nonconstant polynomial. By Theorem 1.2 we know that f factors into linear factors in $\mathbf{C}[x]$:

$$f = a(x - z_1) \cdots (x - z_n)$$

where the z_i are the complex roots of f. If any of the roots z_i is real, then $x - z_i \in \mathbf{R}[x]$ is a nonconstant factor of f in $\mathbf{R}[x]$, so in this case if $\deg(f) \geq 2$ then f is reducible in $\mathbf{R}[x]$.

So we may assume each root z_i is non-real. The non-real roots of a real polynomial occur in complex conjugate pairs, so we have $\overline{z_i} = z_j$ for some $j \neq i$. Consider the product

$$\begin{aligned} q &= (x - z_i)(x - z_j) \\ &= (x - z_i)(x - \overline{z_i}) \\ &= x^2 - 2rx + |z_i|^2 \end{aligned}$$

where r is the real part of z_i. Then q is a polynomial in $\mathbf{R}[x]$ which divides f.

Now suppose $\deg(f) \geq 3$. We therefore have

$$f = pq$$

with $\deg(p) \geq 1$. Since both p and q have degree at least 1, they are not units in $\mathbf{R}[x]$, and therefore f is reducible in $\mathbf{R}[x]$. □

Remark: What about the converse? Any polynomial of degree 1 in $\mathbf{R}[x]$ (or any polynomial ring) is certainly irreducible.

Polynomials of degree 2 in $\mathbf{R}[x]$ can be irreducible or reducible in $\mathbf{R}[x]$, depending on the sign of the discriminant b^2-4ac: a polynomial ax^2+bx+c of degree 2 in $\mathbf{R}[x]$ is irreducible in $\mathbf{R}[x]$ if and only if it has no linear factor, which by the Factor Theorem is true if and only if it has no real root. By the quadratic formula, this is equivalent to $b^2-4ac<0$.

To emphasise the point we made earlier, on the other hand by Theorem 1.2 **any** polynomial of degree at least 2 in $\mathbf{R}[x]$ is reducible in $\mathbf{C}[x]$. As a concrete example, $x^2+1 \in \mathbf{R}[x]$ is irreducible in $\mathbf{R}[x]$ but reducible in $\mathbf{C}[x]$.

1.3 Irreducibility in $\mathbf{Q}[x]$: the Gauss Lemma

Much more interesting than either of the previous discussions is the question of irreducibility in $\mathbf{Q}[x]$. It can be highly nontrivial to decide whether a given polynomial $f \in \mathbf{Q}[x]$ is irreducible in $\mathbf{Q}[x]$. For the remainder of this week we will look at some methods to answer this question.

We will start with the following simple but very useful result.

Proposition 1.4 (Gauss Lemma)**.** *Let $f \in \mathbf{Z}[x]$ be a polynomial with integer coefficients. If f does not factor into nonconstant polynomials in $\mathbf{Z}[x]$, then it is irreducible in $\mathbf{Q}[x]$.*

Remark: The hypothesis "does not factor into nonconstant polynomials in $\mathbf{Z}[x]$" is slightly weaker than "irreducible in $\mathbf{Z}[x]$". For example, the polynomial $2x$ is **not** irreducible in $\mathbf{Z}[x]$ because $2x = 2 \cdot x$ and neither 2 nor x is a unit in $\mathbf{Z}[x]$. But our version of the Gauss Lemma nevertheless tells us that $2x$ is irreducible in $\mathbf{Q}[x]$.

We are not going to prove the Gauss Lemma, but let's say something about what it means. When looking for factors in $\mathbf{Q}[x]$, it allows us to focus our attention on factors with **integer** coefficients. This is extremely usful in practice, since then we can use divisibility properties of the coefficients to show that no factors (other than constants) exist.

Example Let's look at some examples to see how the Gauss Lemma helps us to prove irreducibility in $\mathbf{Q}[x]$ of polynomials with integer coefficients.

We start with the polynomial

$$f = x^3 + 2x^2 + x + 6$$

By the Gauss Lemma, to prove that f is irreducible in $\mathbf{Q}[x]$ it is enough to prove it cannot be factored into nonconstant factors in $\mathbf{Z}[x]$. So suppose that

$$f = gh$$

where g and h are polynomials in $\mathbf{Z}[x]$ and neither is a constant. We want to show this leads to a contradiction. Let us assume, by swapping g and h if necessary, that $\deg(g) \leq \deg(h)$. Since $\deg(f) = 3$, this means $\deg(g) = 1$. So we have

$$x^3 + 2x^2 + x + 6 = (ax+b)(cx^2+dx+e) \quad \text{where } a, b, c, d, e \in \mathbf{Z}$$

Comparing coefficients of x^3 on both sides, we see that $ac = 1$. Since both a and c are integers, this implies $a = c = \pm 1$. If $a = c = -1$ we can replace g by $-g$ and h by $-h$, so we can assume that $a = c = 1$. So we get

$$x^3 + 2x^2 + x + 6 = (x + b)(x^2 + dx + e) \quad \text{where } b, d, e \in \mathbf{Z}$$

Now we can compare coefficients on both sides to get the following equations for b, d, e:

$$\begin{aligned} b + d &= 2 \\ bd + e &= 1 \\ be &= 6 \end{aligned}$$

The first equation gives $d = 2 - b$, and then the second gives $2b - b^2 + e = 1$.

On the other hand, the last equation implies that on of the following is true:

$$\begin{aligned} b = \pm 1, e = \pm 6 \\ b = \pm 2, e = \pm 3 \\ b = \pm 3, e = \pm 2 \\ b = \pm 6, e = \pm 1 \end{aligned}$$

where the signs of b and e are the same in each case. It's not hard to check that none of these possibilities satisfy the equation $2b - b^2 + e = 1$.

Example Let's show that the polynomial

$$f = x^4 + 3x^2 + 7$$

is irreducible in $\mathbf{Q}[x]$.

Again by the Gauss Lemma, it is enough to show that f can't be factored as $f = gh$ where $g, h \in \mathbf{Z}[x]$ and neither g nor h is constant.

Let's prove this by contradiction: we suppose on the contrary that $f = gh$ with $g, h \in \mathbf{Z}[x]$ and both g and h are nonconstant, and derive a contradiction. Without loss of generality we may assume $\deg(g) \leq \deg(h)$.

Case 1: $\deg(g) = 1$, $\deg(h) = 3$.

As before we can assume both g and h have leading coefficient 1, so our factorisation looks like

$$x^4 + 3x^2 + 7 = (x + a)(x^3 + bx^2 + cx + d)$$

with $a, b, c, d \in \mathbf{Z}$.

Comparing coefficients on the two sides gives equations

$$\begin{aligned} a + b &= 0 \\ ab + c &= 3 \\ ac + d &= 0 \\ ad &= 7. \end{aligned}$$

These can be manipulated to give the equations

$$\begin{aligned} b &= -a \\ -a^2 + c &= 3 \\ d &= -ac \\ -a^2 c &= 7. \end{aligned}$$

Now the last equation implies that $c < 0$, and since $a^2 \neq 7$ for any $a \in \mathbf{Z}$ we must have $c = -7$ and $a = \pm 1$. But these values do not satisfy $-a^2 + c = 3$, so we get a contradiction.

Case 2: $\deg(g) = \deg(h) = 2$.

Here our factorisation looks like

$$x^4 + 3x^2 + 7 = (x^2 + ax + b)(x^3 + cx + d)$$

leading to equations

$$\begin{aligned} a + c &= 0 \\ ac + b + d &= 3 \\ ad + bc &= 0 \\ bd &= 7 \end{aligned}$$

The first equation gives $c = -a$, and then the third equation gives $a(d - b) = 0$. There are two possibilities to consider: $a = 0$ or $d - b = 0$.

If $a = 0$ then the second equation gives $b + d = 3$. The last equation says that $b = \pm 1$ or ± 7 and $d = \pm 7$ or ± 1, but none of these possibilities gives a solution of $b + d = 3$.

If $d - b = 0$ then $d = b$, so the last equation gives $b^2 = 7$, which has no integer solution.

2 Irreducibility in $\mathbf{Q}[x]$ continued: reduction mod p

Using the Gauss Lemma was successful in our examples in the previous section, but it took a lot of work. Here's another tool that we can combine with the Gauss Lemma in some cases to show more efficiently that a polynomial is irreducible $\mathbf{Q}[x]$.

Fix a prime number p. In Week 1 we discussed the field

$$\mathbf{Z}_p = \{0, 1, \ldots, p-1\}$$

in which the operations were addition and multiplication mod p. We also introduced the ring homomorphism called "reduction mod p" defined by

$$\begin{aligned} \rho_p \colon \mathbf{Z} &\to \mathbf{Z}_p \\ k &\mapsto k \mod p \end{aligned}$$

We can soup this up into a homomorphism between the corresponding polynomial rings, as follows:

Definition 2.1. *Let p be a prime. Define* polynomial reduction mod p *to be the map*

$$\rho_p \colon \mathbf{Z}[x] \to \mathbf{Z}_p[x]$$

obtained by applying reduction mod p to all the coefficients of a polynomial.

For example, the map $\rho_3 : \mathbf{Z}[x] \to \mathbf{Z}_3[x]$ takes the polynomial $-4x^2 - 2x + 3$ in $\mathbf{Z}[x]$ to the polynomial $2x^2 + x$ in $\mathbf{Z}_3[x]$.

Theorem 2.2. *For any prime p, the map $\rho_p : \mathbf{Z}[x] \to \mathbf{Z}_p[x]$ is a ring homomorphism.*

Sketch of proof. We have to prove that for any polynomials f and g in $\mathbf{Z}[x]$, we have

$$\begin{aligned} \rho_p(f+g) &= \rho_p(f) + \rho_p(g) \\ \rho_p(fg) &= \rho_p(f)\rho_p(g) \end{aligned}$$

For example to prove the second equality, if we have

$$\begin{aligned} f &= \sum_i a_i x^i \\ g &= \sum_i b_i x^i \end{aligned}$$

then the coefficient of x^k in fg is

$$\sum_{i+j=k} a_i b_j.$$

So the coefficient of x^k in $\rho_p(fg)$ is

$$\rho_p\left(\sum_{i+j=k} a_i b_j\right) = \sum_{i+j=k} \rho_p(a_i)\rho_p(b_j)$$

which is exactly the coefficient of x^k in $\rho_p(f)\rho_p(g)$. □

As a consequence, we see:

$$\begin{aligned} &\text{if } f = gh \quad \text{ in } \mathbf{Z}[x] \\ &\text{then } \rho_p(f) = \rho_p(g)\ \rho_p(h) \quad \text{ in } \mathbf{Z}_p[x]. \end{aligned}$$

If $\rho_p(f)$ has the same degree as f, then $\rho_p(g)$ and $\rho_p(h)$ have the same degrees as g and h respectively. So if g and h are nonconstant, then $\rho_p(g)$ and $\rho_p(h)$ are nonconstant, and so $\rho_p(f)$ is reducible.

Turning this conclusion around, we get our criterion:

Corollary 2.3 (Reduction Test for irreducibility)**.** *Let $f \in \mathbf{Z}[x]$ be a polynomial with integer coefficients, and p a prime number. If $\rho_p(f)$ is irreducible and the same degree as f, then f does not factor into nonconstant polynomials in $\mathbf{Z}[x]$, hence is irreducible in $\mathbf{Q}[x]$.*

Warning: If the leading coefficient of f is divisible by p then $\rho_p(f)$ will have lower degree than f. In this case we need to choose a different p and try again.

Reduction mod p sometimes allows us to prove irreducibility very efficiently.

Example 2.4. *Let's prove that the polynomial*

$$f = 25x^3 + 60x^2 - 99x + 11$$

does not factor into nonconstant factors in $\mathbf{Z}[x]$, and so by the Gauss Lemma, is irreducible in $\mathbf{Q}[x]$.

Consider the map $\rho_2 : \mathbf{Z}[x] \to \mathbf{Z}_2[x]$. Under this map, f goes the polynomial

$$\varphi = \rho_2(f) = x^3 + x + 1.$$

By the Reduction Test, it's enough to show that φ is irreducible in $Z_2[x]$.

The polynomial φ is cubic, so as before, if it were reducible, it would have to have a linear factor $(x - a)$ for some $a \in \mathbf{Z}_2$. But the field $\mathbf{Z}_2$ has just two elements, 0 and 1. Plugging these into φ, we get

$$\begin{aligned} \varphi(0) &= 0 + 0 + 1 = 1 \\ \varphi(1) &= 1 + 1 + 1 = 1. \end{aligned}$$

So by the Factor Theorem, neither $(x - 0)$ nor $(x - 1)$ is a factor of φ. So φ is irreducible, hence f is irreducible in $\mathbf{Q}[x]$.

Warning: When it works quickly, as above, this method is very slick. But there are complications:

- Firstly, if f is reducible, but has degree at least 4, there is no reason that it should have a *linear* factor. So we can't simply use the Factor Theorem like we did in the example: we also have to look for factors of $\rho_p(f)$ with degree greater than 1.

- Secondly, even if the method works for some p, you don't know ahead of time which p will work. It's conceivable (although I don't know an example) that $\rho_p(f)$ is irreducible for some very large prime p, but reducible for all smaller primes p. In such a case, the method would take a long time to apply.
- Finally, and worst of all, there exist irreducible polynomials $f \in \mathbf{Z}[x]$ such that $\rho_p(f)$ is reducible for *every* prime p! For these polynomials, the method is doomed to fail, and we need other tools.

Example Let's use the reduction method to show that the polynomial

$$f = x^4 + 10x^3 + x^2 - 4x + 6$$

is irreducible in $\mathbf{Q}[x]$.

We start with a couple of observations:

- Since the constant term of f equals 6, which is divisible by the primes 2 and 3, both $\rho_2(f)$ and $\rho_3(f)$ will have constant term equal to 0. So they will be reducible, and we get no information. Therefore we start with $p = 5$.
- Suppose $\rho_5(f) = gh$, so it is divisible by g. Then we also have $\rho_5(f) = \widehat{g}(ah)$ where a is the leading coefficient of g. This shows that $\rho_5(f)$ is also divisible by the **monic** polynomial $\widehat{g}$. This means that when we are looking for factors, we can restrict our attention to monic factors.
- If q is a quadratic factor of $\rho_5(f)$ which is itself a product of linear factors, say $q = gh$, then both g and h are factors of $\rho_5(f)$. So if we know that $\rho_5(f)$ has no linear factors, any quadratic factor must be irreudicible. So it is enough to check for **irreducible** quadratic factors.

Now let's check for factors of $\varphi = \rho_5(f)$.

Step 1: First we check for monic linear factors. We have

$$\varphi = x^4 + x^2 + x + 1 \in \mathbf{Z}_5[x].$$

As before the Factor Theorem says that $(x - a)$ is a factor of φ if and only if $\varphi(a) = 0$. We compute

$$\begin{aligned}
\varphi(0) &= 1 \\
\varphi(1) &= 4 \\
\varphi(2) &= 2^4 + 2^2 + 2 + 1 \\
&= 3 \\
\varphi(3) &= 3^4 + 3^2 + 3 + 1 \\
&= 4 \\
\varphi(4) &= (-1)^4 + (-1)^2 + (-1) + 1 \\
&= 2.
\end{aligned}$$

So φ has no roots in $\mathbf{Z}_5$, hence no linear factors in $\mathbf{Z}_5[x]$.

Step 2: Now we check for quadratic factors of φ in $\mathbf{Z}_5[x]$. As explained above, we only need to check for irreducible monic quadratic factors.

Monic quadratic polynomials in $\mathbf{Z}_5[x]$ have the form

$$x^2 + ax + b$$

with $a, b \in \mathbf{Z}_5$. There are 25 of these. The reducible ones have the form

$$(x - c)(x - d)$$

with $c, d \in \mathbf{Z}_5$, so there are $\binom{5}{2} + 5 = 15$ such reducible polynomials. That leaves 10 irreducible quadratics to check as possible factors of φ.

We won't check this in full, but we will show what is involved. For example, let's take the irreducible quadratic $x^2 + x + 1 \in \mathbf{Z}_5[x]$. Dividing we find

$$\begin{aligned} \varphi &= x^4 + x^2 + x + 1 \\ &= (x^2 + x + 1)(x^2 + 4x + 1) + x \end{aligned}$$

Since there is a nonzero remainder x when we divide, this shows that $x^2 + x + 1$ is not a factor of φ.

In fact the same calculation also shows that the irreducible quadratic $x^2 + 4x + 1$ is not a factor of φ.

You can do the same thing for all irreducible quadratics in $\mathbf{Z}_5[x]$, to show that φ has no irreducible quadratic factor. (See Problem Sheet 8.)

Steps 1 and 2 together show that φ is irreducible in $\mathbf{Z}_5[x]$, so by the Reduction Test, our original polynomial

$$f = x^4 + 10x^3 + x^2 - 4x + 6$$

is irreducible in $\mathbf{Q}[x]$.