Galois Theory - Week 3 - Polynomials

Antonio León Villares

January 2023

Contents

Based on the notes by Tom Leinster, Chapter 3

1 Polynomials as Rings

1.1 Definition: Polynomials Over Rings

*Let R be a **ring**. A **polynomial over** R is an **infinite sequence**:*

$$(a_0, a_1, \ldots)$$

*of elements of R, such that $\{i \mid a_i \neq 0\}$ is **finite**.*

---

*The set of **polynomials** over R forms a **ring** $R[t]$, defined by:*

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_1, a_1 + b_1, \ldots)$$

$$(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) = (c_0, c_1, \ldots), \qquad c_k = \sum_{i,j \,:\, i+j=k} a_i b_j$$

*with **additive identity**:*

$$(0_R, 0_R, \ldots)$$

*and **multiplicative identity**:*

$$(1_R, 0_R, \ldots)$$

Of course, we typically define elements in $R[t]$ as:

$$a_0 + a_1 t + a_2 t^2 + \ldots$$

(Definition 3.1.1)

- **How can polynomials over multiple variables be defined?**
  - since $R[t]$ is a **ring**, we can define some polynomial over $R[t]$ itself
  - for example, if $S = R[t]$, the polynomial ring $S[u]$ is nothing but:

$$S[u] = (R[t])[u] = R[t, u]$$

- **How do polynomials over R lead to endomorphisms?**
  - let $f = (a_0, a_1, \ldots) \in R[t]$

- then, f gives rise to an **endomorphism**:

$$R \to R$$
$$r \mapsto a_0 + a_1 r + a_2 r^2 + \dots$$

- this sum of elements in R is defined, since it involves finitely many elements

- **Are these endomorphisms unique to a polynomial?**
  - this depends on the ring over which we operate
  - for example, in $\mathbb{Z}_2$, we have that:
$$0^2 = 0 \qquad 1^2 = 1$$
  - hence, the polynomials $f(t) = t, g(t) = t^2 \in \mathbb{Z}_2$, whilst different, induce the same endomorphism:

- **How are polynomials related to free groups?**
  - recall, a **free group** is a group for which we are only given some elements, and the structure of the group arises naturally from using these elements (i.e its the group containing all these elements, their inverses, and any possible logical combination of these)
  - turns out, **free rings** are nothing but **polynomial rings**: if we have some elements s, u, t, a free ring will include any possible combination of these elements:
    * $s + ut^3 s^{-}4 - u^2 s^8$
    * $ut + t^3 + su^{-1}$
    * ...

1.1.1 Exercises

1. *[Exercise 3.1.4]* **Show that whenever R is a finite non-trivial ring, it is possible to find distinct polynomials over R that induce the same function $R \to R$.**

   Notice, if R is finite, the number of functions of the form $R \to R$ will be finite. However, the poossible polynomials will be infinite (we can always add as many finite terms as we want). Thus, by the pigeonhole principle, we must have that at least 2 polynomials correspond to the same function.

1.2 Proposition: The Universal Property of the Polynomial Ring

*Let R, B be **rings**. Consider **any** homomorphism:*

$$\varphi : R \to B$$

*and **any** $b \in B$.*
*Then, there exists a **unique** homomorphism:*

$$\theta : R[t] \to B$$

such that:

$$\forall a \in R, \theta(a) = \varphi(a)$$
$$\theta(t) = b$$

(Proposition 3.1.6)

One way to think about this is the following: I can pick out any homomorphism φ I want, and pick any $b \in B$ I want. Once I have these, they will define a unique homomorphism. This uniqueness arises by the fact that:

- *θ uniquely maps the polynomial coefficients (since this is defined by our choice φ)*
- *θ uniquely maps the indeterminate t (since this is defined by our choice b)*

Proof. We first show that there is **at most one** such θ. Indeed, let θ be any homomorphism $\theta : R[t] \to B$, such that:

$$\forall a \in R,\ \theta(a) = \varphi(a) \qquad \theta(t) = b$$

Then, for any polynomial over R:

$$\begin{aligned} \theta\left(\sum_i a_i t^i\right) &= \sum_i \theta(a_i)\theta(t)^i \\ &= \sum_i \varphi(a_i) b^i \end{aligned}$$

This θ is uniquely determined (by the values of $\varphi(a_i)b^i$), so there is at most one such θ.

Now we show that there is **at least one** such θ. Consider a function $\theta : R[t] \to B$, defined by:

$$\theta\left(\sum_i a_i t^i\right) = \sum_i \varphi(a_i) b^i$$

Clearly:

$$\theta(a) = \varphi(a) \qquad \theta(t) = b$$

It remains to show that this is a homomorphism (which is tedious, and we already did a lot in Honours Algebra)

□

The Universal Property allows us to find many interesting homomomorphisms for polynomials.

2 Polynomials and Homomorphisms

2.1 Definition: The Induced Homomorphism

Let:

$$\varphi : R \to S$$

be a ***ring homomorphism****. The* ***induced homomorphism*** *is the* ***unique homomorphism****:*

$$\varphi_* : R[t] \to S[t]$$

such that:

$$\forall a \in R,\ \varphi_*(a) = \varphi(a) \qquad \varphi_*(t) = t$$

By the ***universal property****, it follows immediately that this is unique; it is also intuitively defined:*

$$\varphi_* \left(\sum_i a_t^i \right) = \sum_i \varphi(a_i) t^i$$

(Definition 3.1.7)

2.2 Definition: The Evaluation Homomorphism

*Let R be a **ring**, and let $r \in R$. We can **evaluate** polynomials $R[t]$ at r through a **unique homomorphism**:*

$$ev_r : R[t] \to R$$

such that:

$$\forall a \in R,\ ev_r(a) = a \qquad ev_r(t) = r$$

---

*By the **universal property**, it follows immediately that this is unique; it is also intuitively defined:*

$$ev_r\left(\sum_i a_t^i\right) = \sum_i a_i r^i$$

2.3 Definition: The Substitution Isomorphism

Let R be a ***ring****, and let $c \in R$. There is a* ***unique homomorphism***

$$\theta : R[t] \to R[u]$$

, such that:

$$\forall a \in R,\ \theta(a) = a \qquad \theta(t) = u + c$$

By the ***universal property****, it follows immediately that this is unique; it is also intuitively defined:*

$$\theta\left(\sum_i a_t^i\right) = \sum_i a_i (u + c)^i$$

Notice, this ***homomorphism*** *is nothing but a* ***change of variables****. In particular, it is an* ***isomorphism****, since it is* ***invertible****:*

$$\theta^{-1} : R[u] \to R[t]$$

such that:

$$\forall a \in R,\ \theta^{-1}(a) = a \qquad \theta^{-1}(u) = t - c$$

In particular, these isomorphisms preserve ***structure****: what is true for polynomials $f(t)$ will be true for polynomials $g(u) = f(t-c)$; in particular:*

$$f(t) \text{ is irreducible} \iff f(t - c) \text{ is irreducible}$$

2.3.1 Exercises

1. *[Exercise 3.1.8]* **What happens to this if instead we substitute $t = u^2 + c$?**

   We would no longer have a bijective mapping, since we'd only map to polynomials with even powers in $R[u]$.

3 Polynomial Properties

3.1 Definition: Degree of a Polynomial

Consider some ***non-zero polynomial****:*

$$f(t) = \sum_i a_i t^i$$

The ***degree*** *of f, $deg(f)$, is the* ***largest*** *$n \geq 0$, such that $a_n \neq 0$.*
By convention:

$$deg(0) = -\infty$$

where $-\infty$ is a formal symbol defined by the following properties $\forall n \in \mathbb{Z}$:

$$-\infty < n \qquad (-\infty) + n = -\infty \qquad (-\infty) + (-\infty) = -\infty$$

(Definition 3.1.9)

3.2 Lemma: Polynomials Over Integral Domains

Let R be an ***integral domain****. Then:*

1. $$\forall f, g \in R[t], \quad deg(fg) = deg(f) + deg(g)$$

2. *$R[t]$ is an* ***integral domain***

(Lemma 3.1.11)

In fact, applying induction it can be seen that the ring $R[t_1, \ldots, t_n]$ of polynomials over R with n variables will also be an integral domain.

Proof.

(1)

For the first claim, since R is an integral domain, it has no zero-divisors (2 non-zero elements whose product is zero), then the leading coefficient of PQ is the product of the leading coefficients of P and Q. From this it is easy to see that we will indeed have $deg(PQ) = deg(P) + deg(Q)$. Moreover, it is clear that $PQ \neq 0$ if and only if $P \neq 0 \wedge Q \neq 0$ (since no possible multiplication of coefficients can be 0).

(2)

For the second claim, we note that if R has no zero-divisors, $R[t]$ doesn't either. An integral domain is a ring with no zero-divisors, so if R is an integral domain, so is $R[t]$.

□

3.2.1 Exercises

1. *[Exercise 3.1.13]* **Let p be a prime, and consider the field $\mathbb{Z}_p(t)$ of rational expression of $Z_p[t]$. Show that t has no pth root in $\mathbb{Z}_p(t)$.**

   Assume that t has a pth root in $\mathbb{Z}_p(t)$. In particular, this means that there exist $f, g \in \mathbb{Z}_p[t]$ such that:

   $$\left(\frac{f}{g}\right)^p = t \implies f^p = tg^p$$

   Considering degree:

   $$\deg(f^p) = \deg(tg^p) \implies p\deg(f) = 1 + p\deg(g)$$

   But this is impossible: p divides the LHS, but won't divide the RHS. Hence, t can't have a root in $\mathbb{Z}_p(t)$.

3.3 Lemma: Polynomials Over Fields and Irreducibility

> *Let K be a **field**. Then:*
>
> 1. *the **units** in $K[t]$ are the **non-zero constants** (namely, the non-zero elements of K/polynomials of degree 0)*
> 2. *$f \in K[t]$ is **irreducible if and only if**:*
>   - *f is **non-constant***
>   - *f can't be expressed as a **product** of 2 **non-constant** polynomials*
>
> *(Lemma 3.1.14)*

Proof.

(1)

It is clear that if $a \in K$, then the polynomial of degree 0 $f(t) = a$ is a unit (since K is a field). Now, assume that f is a unit in $K[t]$, such that $deg(f) \geq 1$. Let g be the inverse. Since K is a field, it is an integral domain, and so:

$$deg(fg) = deg(1_K) = 0 \implies deg(f) + deg(g) = 0$$

Since the degree is a non-negative integer, this can only be the case if $deg(f) = deg(g) = 0$. Hence, all the units of $K[t]$ are the non-zero constants.

(2)

Recall the definition of an irreducible ring element:

> *Let R be a **ring**. $r \in R$ is **irreducible** if:*
>
> - $r \neq 0_R$
> - *r is not a **unit***
> - $$\forall a, b \in R \ : \ ab = r \implies a \text{ or } b \text{ is a unit}$$

Translated to polynomial parlance, a polynomial $f \in K[t]$ is **irreducible** if and only if:

- $f \neq 0_K$
- f is **not** a non-zero, constant polynomial
- $$\forall g, h \in K[t] \ : \ gh = f \implies g \text{ or } h \text{ are non-zero, constant polynomials}$$

Hence, the result follows from the definition of irreducibility.

□

3.4 Polynomial Factorisation

3.4.1 Proposition: Polynomial Remainders

> *Let K be a **field**, and $f, g \in K[t]$, with $g \neq 0_K$.*
> *Then, there is a **unique** pair of polynomials $q, r \in K[t]$, such that:*
>
> $$f = qg + r \qquad deg(r) < deg(g)$$
>
> *(Proposition 3.2.1)*

Proof. Pick q to minimise $deg(f - gq)$. This is always possible, since the degree of any polynomial is always non-negative.

Assume that after this:

$$deg(f - gq) \geq deg(g)$$

That is, we have:

$$f - gq = \sum_{i=0}^{r} a_i t^i$$

and $r \geq d = deg(g)$.

Now consider:

$$f - (q + a_r t^{r-d})g = f - gq - a_r t^r + \ldots$$

As we can see $deg(f-(q+a_r t^{r-d})g) = deg(f-gq)-1$. This contradicts the fact that our choice of q leads to $deg(f-gq) \geq deg(g)$, meaning that we must have $deg(f-gq) < deg(g)$.

Thus, we have found q and $r = f - gq$, with $deg(r) < deg(g)$ such that:

$$r = f - gq \implies f = gq + r$$

as required.

We now show that these choices are indeed unique. Suppose that q', r' also satisfy the conclusions (so $f = q'g + r'$ and $deg(r') < deg(g)$. Then:

$$0 = f - f = (q - q')g + (r - r')$$

Notice:

- $(q-q')g$ will have degree greater than (or equal to) g
- $r - r'$ has degree less than Q

But the polynomial should have degree 0. This is only possible if $q - q' = 0 \implies q = q'$ (since r could have degree 0).

But then notice that:

$$r = f - gq = f - q'g = r'$$

Thus, the choice of q, r is unique.

□

3.4.2 Proposition: Polynomials Over Fields are Principal Ideal Domains

> *Let K be a **field**. Then $K[t]$ is a **principal ideal domain**. (Proposition 3.2.2)*

Proof. Since K is a field, it is an integral domain, so $K[t]$ is an integral domain.

Now, let I be an ideal of $K[t]$. If $I = \{0_K\}$, then clearly $I = \langle 0_K \rangle$.

Otherwise, define d to be the smallest degree of all polynomials in I:

$$d = \min\{deg(f) \mid 0_K \neq f \in I\}$$

and let $g \in I$, such that $deg(g) = d$.

We claim that $I = \langle g \rangle$. To do this, it is sufficient to show that:

$$\forall f \in I,\ g \mid f$$

To this end, we know that $\exists! q, r \in K[t]$ such that:

$$f = gq + r$$

and $deg(r) < deg(g) = d$. Notice, since $q \in K[t]$, by properties of ideal $gq \in I$. Again, by properties of ideal:

$$r = f - gq \in I$$

But then, since g was chosen to have minimal degree, and $deg(r) < d$, it must be the case that $r = 0$ (otherwise, we would've picked r as our element of minmal degree). Hence, as required:

$$f = qg \implies g \mid f$$

□

- **Since $K[t]$ is a principal ideal domain when K is a field, and $K[t_1, \ldots, t_n]$ is an integral domain, is it also a principal ideal domain?**
  - no, for $n > 1$ polynomials in n variables over a field need not be principal ideal domains
  - for example, the ideal:

    $$\langle t_1, t_2 \rangle = \{t_1 f(t_1, t_2) + t_2 g(t_1, t_2) \mid f(t_1, t_2), g(t_1, t_2) \in \mathbb{Q}[t_1, t_2]\}$$

    is not principal
  - this can be seen by contradiction. Assume $\exists h(t_1, t_2) \in \mathbb{Q}[t_1, t_2]$, such that:

    $$\langle t_1, t_2 \rangle = \langle h \rangle$$

    In particular, this implies that:

    $$h \mid t_1 \implies \exists a(t_1, t_2) \ : \ ha = t_1$$

    so either $deg(h) = 0 \implies h = c \in \mathbb{Q}$ or $deg(h) = 1 \implies h = ct_1$. But then, by similar logic:

    $$h \mid t_2 \implies h = d \text{ or } h = dt_2$$

    Both of these together imply that h must be a non-zero constant polynomial. But then, h would be a unit, and in particular, $\langle h \rangle = \mathbb{Q}[t_1, t_2]$, which is a contradiction, as $\langle t_1, t_2 \rangle$ is an ideal containing polynomials with a constant term of 0.
- **If K is a principal ideal domain, is $K[t]$ a principal ideal domain?**
  - no, we require K to be a field
  - for example, $\mathbb{Z}$ is a principal ideal domain (not a field), but the ideal:

    $$\langle 2, t \rangle = \{2f(t) + tg(t) \mid f(t), g(t) \in \mathbb{Z}[t]\}$$

    is not a principal ideal (we can see this using a similar procedure to the one above)

At the end of last week's work, we saw that irreducible ring elements allowed us to create fields. We revisit this now, so that we can use polynomials to generate fields! To do this, we'll need to develop theory, which:

1. *allows us to factorise polynomials into irreducible factors*
2. *llows us to determine when some polynomial is irreducible*

4 Generating Fields from Polynomials

4.1 Corollary: Fields from Irreducible Polynomials

*Let K be a **field**, and let:*

$$0_K \neq f \in K[t]$$

Then:

$$f \text{ is } \textbf{irreducible} \iff K[t]/\langle f \rangle \text{ is a } \textbf{field}$$

(Corollary 3.2.5)

Proof. This follows from last week's conclusion:

*Let R be a **principal ideal domain**, and $r \in R, r \neq 0_R$. Then:*

$$r \text{ is } \textbf{irreducible} \iff R/\langle r \rangle \text{ is a } \textbf{field}$$

alongside the fact that since K is a field, $K[t]$ is a principal ideal domain. □

4.2 Factorising Polynomials with Irreducibles

4.2.1 Lemma: Non-Constant Polynomials are Divisible by Irreducible Polynomials

*Let K be a **field**, and let $f(t) \in K[t]$ be a **non-constant polynomial**. Then, $f(t)$ is divisible by some **irreducible** in $K[t]$.*
(Lemma 3.2.6)

Proof. Let $f \in K[t]$, and pick g to be some non-constant polynomial, such that g is the polynomial of smallest degree satisfying $g \mid f$. g must be irreducible. To this end, let $g_1, g_2 \in K[t]$ be such that $g = g_1 g_2$. Then:

$$g \mid f \implies g_1 \mid f \quad g_2 \mid f$$

Since we operate over an integral domain:

$$deg(g) = deg(g_1) + deg(g_2)$$

Thus, the fact that g had minimal degree implies that:

$$deg(g_i) = 0 \text{ or } deg(g_i) = deg(g)$$

Thus, at least one of the g_i must have degree 0; in other words, it must be a unit. Hence, since g is not a unit (since it is non-constant) or zero, it must be that g is irreducible, as required.

□

4.2.2 Lemma: Irreducibility and Division of a Product

> *Let K be a **field**, and let $f, g, h \in K[t]$. Suppose that f is **irreducible**, and $f \mid gh$. Then:*
>
> $$f \mid g \text{ or } f \mid h$$
>
> *(Lemma 3.2.7)*

Proof. Assume that $f \nmid g$. f is irreducible, so it is only divisible by units; hence, f, g must be coprime (the only common divisor they have is a unit). Since $K[t]$ is a principal ideal domain, Bezout's Lemma applies:

$$\exists p, q \in K[t] \ : \ pf + qg = 1_K$$

Multiplying both sides by h:

$$pfh + qgh = h$$

Notice:

- $f \mid pfh$
- $f \mid gh \implies f \mid qgh$

Thus, the RHS is divisible by f, so we must have that $f \mid h$, as required.

□

4.2.3 Theorem: Polynomials Over Fields Factorise Uniquely

We now show a really important results: that we can uniquely factorise polynomials over a field. This isn't always true for rings, so this is rather neat!

Recall, a polynomial is ***monic*** *if its* ***leading coefficient*** *is* 1_K.

Let K *be a* ***field****, and:*

$$0_K \neq f \in K[t]$$

Then:

$$f = af_1f_2 \dots f_n$$

where:

- $n \geq 0$
- $a \in K$
- $f_1, \dots, f_n \in K[t]$ *are* ***monic irreducible*** *polynomials*

Moreover, n, a *are* ***uniquely determined*** *by* f*, and the factors* $f_1, \dots, f_n$ *are unique up to reordering.*
If $n = 0$*, the product* $f_1 \dots f_n$ *should be interpreted as* 1_K.
(Theorem 3.2.8)

Proof. We prove this in 2 steps: firstly, we show that such a factorisation exists; then, we prove that it is unique.

We induct on $deg(f)$.

(1) **Base Case:** $deg(f) = 0$

If $deg(f) = 0$, then f is a constant polynomial $f = a \in K$, which is as in the theorem (with $n = 0$)

(2) **Inductive Hypothesis:** $deg(f) \in [0, k]$

Now, assume that for all polynomials with $deg(f) \in [0, k]$ the claim holds.

(3) **Inductive Step:** $deg(f) = k + 1$

Now, consider a polynomial $f \in K[t]$ with $deg(f) = k + 1$. By the Lemma above, we can find an irreducible polynomial g, such that $g \mid f$ (WLOG we may assume that g is monic, and otherwise we just divide by a constant). In particular, f/g will be a non-zero polynomial, with $deg(f/g) \in [0, k]$, so by the inductive hypothesis:

$$f/g = ah_1 \dots h_m$$

where $a \in K$ and $h_1, \dots, h_m$ are irreducible. Hence:

$$f = ah_1 \dots h_m g$$

as required.

Now, we prove uniqueness, again by induction on $deg(f)$.

(1) **Base Case:** $deg(f) = 0$

If $deg(f) = 0$, then f is a constant polynomial $f = a \in K$, which is the only possible factorisation.

(2) **Inductive Hypothesis:** $deg(f) \in [0, k]$

Now, assume that for all polynomials with $deg(f) \in [0, k]$ the claim holds.

(3) **Inductive Step:** $deg(f) = k + 1$

Now, consider a polynomial $f \in K[t]$ with $deg(f) = k + 1$. Suppose it has 2 factorisations:

$$af_1 \dots f_n = f = bg_1 \dots g_m$$

such that $a, b \in K$ and f_i, g_j are monic irreducibles. Since $deg(f) > 0$, it is a non-constant polynomial, and $n, m \geq 1$. Now:

$$f_n \mid bg_1 \dots g_m \implies \exists j \ : \ f_n \mid g_j$$

WLOG we may assume that $f_n \mid g_m$. But since f_n, g_m are both irreducible, we must have that:

$$f_n = cg_m$$

where $c \neq 0_K$. Furthermore, f_n, g_m are monic, so $c = 1_K$, and so, $f_n = g_m$. Now, since $K[t]$ is an integral domain, by the cancellation law:

$$af_1 \dots f_{n-1} = bg_1 \dots g_{m-1}$$

By the inductive hypothesis, the resulting products correspond to a polynomial with degree lower than $k+1$, so it thus follows that:

- $n - 1 = m - 1$
- $a = b$
- $f_1, \dots, f_{n-1}$ and $g_1, \dots, g_{n-1}$ are the same up to reordering

as required.

□

4.2.4 Lemma: Linear Factors of Polynomials

Roots of polynomials allow us to find irreducible factors easily.

> *Let K be a **field** $f(t) \in K[t]$, and $a \in K$. Then:*
>
> $$f(a) = 0_K \iff (t - a) \mid f(t)$$
>
> *(Lemma 3.2.9)*

Proof.

- ($\implies$): Assume that $f(a) = 0_K$. We can write:

$$f(t) = (t-a)q(t) + r(t), \quad q, r \in K[t]$$

where $deg(r) < deg(t-a) = 1$. Thus, $r(t)$ is a constant polynomial, and:

$$f(a) = 0_K = (a-a)q(a) + r(a) \implies r(t) = r(a) = 0_K$$

In other words:

$$f(t) = (t-a)q(t) \implies (t-a) \mid f(t)$$

- ($\impliedby$): Suppose that $(t-a) \mid f(t)$. Then:

$$f(t) = (t-a)q(t) \implies f(a) = 0$$

□

4.2.5 Lemma: Linear Factorisation for Algebraically Closed Fields

*Recall, a **field** is **algebraically closed** if every **non-constant** polynomial has **at least** one root in the field. By the **Fundamental Theorem of Algebra**, $\mathbb{C}$ is **algebraically closed**.*

---

*Let K be an **algebraically closed field**, and:*

$$0_K \neq f \in K[t]$$

Then:

$$f(t) = c(t-a_1)^{m_1} \dots (t-a_k)^{m_k}$$

where:

- *$a_1, \dots, a_k$ are the **distinct roots** of f in K*
- *$m_1, \dots, m_k \geq 1$*

4.3 Finding Irreducible Polynomials

4.3.1 Lemma: Irreducibility from Degree and Roots

*Let K be a **field** and $f \in K[t]$. Then:*

1. $$deg(f) \leq 0 \implies f \text{ is } \textbf{not irreducible}$$
2. $$deg(f) = 1 \implies f \text{ is } \textbf{irreducible}$$
3. $$deg(f) \geq 2 \text{ and } f \text{ has a } \textbf{root} \implies f \text{ is } \textbf{reducible}$$
4. $$deg(f) \in \{2, 3\} \text{ and } f \text{ has } \textbf{no root} \implies f \text{ is } \textbf{irreducible}$$

(Lemma 3.3.1)

Proof.

(1)

If $deg(f) = 0$, then f is a non-zero constant, and so, is a unit, so it's not irreducible. If $f = 0_K$, then again f can't be irreducible.

(2)

Linear polynomials are non-zero and not units. If f factorises $f = gh$, then $deg(f) = 1 = deg(g) + deg(h)$, which forces one of g, h to have degree 0. Hence, one of g, h will be a unit, so f is irreducible.

(3)

Since f has a root, by Lemma 3.2.9, f has a linear factor. In particular, and since $deg(f) \geq 2$, f can be factorised as a product of non-constant polynomials, so f is reducible.

(4)

By contradiction, assume that $f = gh$ and:

$$deg(g), deg(h) \geq 1$$

(so that f is not irreducible). We must have:

$$deg(f) \in \{2, 3\} \implies deg(g) + deg(h) \in \{2, 3\}$$

WLOG, we may assume that $deg(g) = 1$, and also that g is monic (otherwise just divide by a constant factor). In other words, we can write:

$$g(t) = t + a$$

But this is a contradiction, as it would imply that $f(-a) = 0$. Hence, f must be irreducible if it doesn't have a root and $deg(f) \in \{2, 3\}$.

□

- **If a polynomial doesn't have a root, can we immediately assume that it is irreducible?**
  - this is the converse of (3) above
  - this isn't true in general: for example, $(t^2 + 1)^2 \in \mathbb{Q}[t]$ has no root, but it is certainly reducible

4.3.2 Definition: Primitive Polynomials

> *A **polynomial** over $\mathbb{Z}$ is **primitive**, if its coefficients have **no common divisor**, except for ± 1.*
> *(Definition 3.3.6)*

For example:

- $15 + 6t + 10t^2$ *is primitive*
- $15 + 6t + 30t^2$ *isn't primitive (the coefficients share a factor of 3)*

4.3.3 Lemma: Rational Polynomials from Primitive Integer Polynomials

> *Let $f(t) \in \mathbb{Q}[t]$. Then:*
>
> $$\exists F(t) \in \mathbb{Z}[t], \alpha \in \mathbb{Q} \ : \ f = \alpha F$$
>
> *where F is **primitive**.*
> *(Lemma 3.3.7)*

Proof. Since f is a polynomial over $\mathbb{Q}$, we can write:

$$f(t) = \sum_i \frac{a_i}{b_i} t^i, \quad a_i \in \mathbb{Z}, b_i \neq 0, b_i \in \mathbb{Z}$$

Now, let b be some common multiple of all the b_is. Define:

$$c_i = \frac{a_i b}{b_i} \in \mathbb{Z}$$

such that:

$$f(t) = \sum_i \frac{a_i}{b_i} t^i = \frac{1}{b} \sum_i c_i t^i$$

Now, let c be the greatest common divisor of the c_is. Define:

$$d_i = \frac{c_i}{c} \in \mathbb{Z}$$

Then, we can define a primitive polynomial:

$$F(t) = \sum_i d_i t^i$$

and:

$$f(t) = \frac{1}{b} \sum_i c_i t^i = \frac{c}{b} \sum_i d_i t^i = \frac{c}{b} F(t)$$

□

4.3.4 Lemma: Gauss's Lemma

> 1. *The product of 2* ***primitive polynomials*** *over* $\mathbb{Z}$ *is* ***primitive***
> 2. *If a non-constant* ***polynomial*** *over* $\mathbb{Z}$ *is* ***irreducible*** *over* $\mathbb{Z}$*, it is* ***irreducible*** *over* $\mathbb{Q}$*.*
>
> *(Lemma 3.3.8)*

Proof.

(1)

Let f, g be primitive polynomials over $\mathbb{Z}$, and let p be prime. We will show that no p divides all the coefficients of fg, which will show that it is indeed primitive. Define a canonical mapping:

$$\pi : \mathbb{Z} \to \mathbb{Z}_p$$

which induces a homomorphism:

$$\pi_* : \mathbb{Z}[t] \to \mathbb{Z}_p[t]$$

f, g are primitive, so p won't divide all the coefficients of f, g. In other words:

$$\pi_*(f) \neq 0 \qquad \pi_*(g) \neq 0$$

(if p divided the coefficients, then the coefficients would be 0 over $\mathbb{Z}_p$)

But then, since $\mathbb{Z}_p$ is an integral domain, so is $\mathbb{Z}_p[t]$, so:

$$\pi_*(fg) = \pi_*(f)\pi_*(g) \neq 0$$

Thus, p won't divide all coefficients of fg, and this holds for all primes p, so fg will be primitive.

---

(2)

Now, let $f \in \mathbb{Z}[t]$ be a non-constant irreducible polynomial over $\mathbb{Z}$. We seek to show it is also irreducible over $\mathbb{Q}$. To this end, consider:

$$g, h \in \mathbb{Q}[t] \ : \ f = gh$$

We can write g, h using primitive polynomials:

$$\exists \alpha, \beta \in \mathbb{Q} \ : \ g = \alpha G \quad h = \beta H$$

where $G, H \in \mathbb{Z}[t]$ are primitive. Since $\alpha, \beta \in \mathbb{Q}$, then there are coprime integers m, n such that:

$$\alpha\beta = \frac{m}{n}$$

so that:

$$f = gh \implies nf = mGH$$

n divides every coefficient of nf, so it must divide every coefficient of mGH. Since m, n are coprime, n must then divide every coefficient of GH. But since GH is primitive (it is a product of primitives) we must have $n = \pm 1$, and $f = \pm mGH$. f is irreducible over $\mathbb{Z}$, so either G or H must be constant. But then, either g or h must be constant, which implies that f is irreducible over $\mathbb{Q}$.

□

4.3.5 Proposition: Irreducibility from Mod p Method

Let:

$$f(t) = a_0 + a_1 t + \ldots + a_n t^n \in \mathbb{Z}[t]$$

Let $\pi : \mathbb{Z} \to \mathbb{Z}_p$ be the canonical homomorphism, and $\pi_* : \mathbb{Z}[t] \to \mathbb{Z}_p[t]$ the resulting induced homomorphism. Define notation:

$$\pi(a) = \bar{a} \qquad \pi_*(f) = \bar{f}$$

If there exists a prime p such that:

- $p \nmid a_n$
- $\bar{f} \in \mathbb{Z}_p[t]$ *is* ***irreducible***

then f is ***irreducible*** *over $\mathbb{Q}$.*
(Proposition 3.3.9)

Proof. Let p be a prime satisfying:

- $p \nmid a_n$

- $\bar{f} \in \mathbb{Z}_p[t]$ is **irreducible**

We first assume that f is primitive. To show that f is irreducible over $\mathbb{Q}$, it is sufficient to show that it is irreducible over $\mathbb{Z}$, by Gauss's Lemma.

By assumption, $\bar{f}$ is irreducible, so:

$$deg(\bar{f}) > 0 \implies deg(f) > 0$$

Now, let $f = gh \in \mathbb{Z}[t]$. By properties of homomorphisms, we also have $\bar{f} = \bar{g}\bar{h}$; but since $\bar{f}$ is irreducible, WLOG we have that $\bar{g}$ is a unit, and so, a constant polynomial.

Now, the leading coefficient a_n of f is the product of the leading coefficients of g and h, and by assumption, $p \nmid a_n$. In particular, this also implies that p won't divide the leading coefficient of g, and so:

$$deg(g) = deg(\bar{g}) = 0$$

In other words, g must be a constant polynomial, and thus, a unit $g = b \in \mathbb{Z}$. Hence, $f = gh = bh$. Now, $f \in \mathbb{Z}[t]$ and since $b \in \mathbb{Z}$, $h \in \mathbb{Z}[t]$. In particular, the coefficients of f must be divisible by b. But f is primitive, so they can't have a common divisor; this forces $b = \pm 1$, which are units in $\mathbb{Z}[t]$, so f must be irreducible.

Now, consider an arbitrary polynomial $f \in \mathbb{Z}[t]$. We can write $f = cF$, where $F \in \mathbb{Z}[t]$ is primitive, and c is the greatest common factor of the coefficients of f. Then, $\bar{f} = \bar{c}\bar{F}$. Moreover, $\mathbb{Z}_p$ is a field, and since $p \nmid c$ (since p doesn't divide a_n by assumption), $\bar{c}$ must be a unit in $\mathbb{Z}_p$. Moreover, $\bar{f}$ being irreducible implies that $\bar{F}$ is also irreducible. But by (1), then F is irreducible over $\mathbb{Q}$. Since $c \neq 0$, c is a unit in $\mathbb{Q}$, so $f = cF$ must also be irreducible over $\mathbb{Q}$. □

4.3.6 Proposition: Eisenstein's Criterion

Let:

$$f(t) = a_0 + \ldots + a_n t^n \in \mathbb{Z}[t]$$

where $n \geq 1$.
Suppose there exists a prime p*, such that:*

- $p \nmid a_n$
- $\forall i \in [0, n-1],\ p \mid a_i$
- $p^2 \nmid a_0$

Then. f *is* ***irreducible*** *over* $\mathbb{Q}$.
(Proposition 3.3.12)

Proof. To prove this, we define the **codegree** of a polynomial:

Consider a polynomial:

$$f(t) = \sum_i a_i t^i$$

The ***codegree*** *of f, $codeg(f)$, is the least i, such that $a_i \neq 0$. If $f = 0$, then $codeg(f) = \infty$.*

The ***codegree*** *has the following properties:*

- *if f, g are polynomials over an integral domain:*

$$codeg(fg) = codeg(f) + codeg(g)$$

- *if $f \neq 0$, then:*

$$codeg(f) \leq deg(f)$$

By Gauss's Lemma, to show that f is irreducible over $\mathbb{Q}$ it is sufficient that this is the case over $\mathbb{Z}$.

Let $g, h \in \mathbb{Z}[t]$, such that:

$$f = gh$$

Let $\bar{f}(t) \in \mathbb{Z}_p[t]$, such that $\bar{f} = \bar{g}\bar{h}$, where p is a prime satisfying the conditions:

- $p \nmid a_n$
- $\forall i \in [0, n-1],\ p \mid a_i$
- $p^2 \nmid a_0$

The last condition implies:

$$p^2 \nmid a_0 \implies p^2 \nmid f(0) = g(0)h(0)$$

In particular, this means that p won't divide both of them, so WLOG, assume that:

$$p \nmid g(0)$$

In other words, $codeg(\bar{g}) = 0$ (since $\bar{g}$ must have a constant term, as the constant term doesn't have p as a factor). Moreover, since $p \nmid a_n$ but $\forall i \in [0, n-1],\ p \mid a_i$, we will have that:

$$codeg(\bar{f}) = n$$

But then:

$$n = codeg(\bar{f}) = codeg(\bar{g}) + codeg(\bar{h}) = codeg(\bar{h}) \leq deg(\bar{h}) \leq deg(h)$$

The last inequality follows because if a_n has p as a factor, it will disappear as a coefficient from $\bar{h}$, so the degree of $\bar{h}$ could be smaller than that of h.

However, this means that $n \leq deg(h)$, and we know that:

$$deg(f) = n = deg(g) + deg(h) \geq n + deg(g)$$

This forces $deg(g) = 0$, and so, $f = gh$ implies that f is irreducible, since g is a unit.

□

4.3.7 Exercises

1. *[Exercise 3.3.15]* **Use Eisenstein's criterion to show that for every $n \geq 1$ there is an irreducible polynomial over $\mathbb{Q}$ of degree n.**

   If we use Gauss's Lemma, we can restrict ourselves to polynomials over $\mathbb{Z}$. We can, for any $n \geq 1$, define:

   $$f(t) = p + t^n$$

   By Eisenstein's Criterion with p, this polynomial will be irreducible, and this holds for any n.

4.4 Examples: Verifying Irreducibility in Polynomials

4.4.1 Using Degree and Roots

*Let K be a **field** and $f \in K[t]$. Then:*

1. $$deg(f) \leq 0 \implies f \text{ is } \textbf{not irreducible}$$
2. $$deg(f) = 1 \implies f \text{ is } \textbf{irreducible}$$
3. $$deg(f) \geq 2 \text{ and } f \text{ has a } \textbf{root} \implies f \text{ is } \textbf{reducible}$$
4. $$deg(f) \in \{2, 3\} \text{ and } f \text{ has } \textbf{no root} \implies f \text{ is } \textbf{irreducible}$$

- if p is prime, then:
  $$f(t) = 1 + t + \ldots + t^{p-1} \in \mathbb{Z}_p[t]$$
  is **reducible**, since $f(1) = 0$ (this is (2))

- let $f(t) = t^3 - 10 \in \mathbb{Q}[t]$. Then, $deg(f) = 3$, and f has no root in $\mathbb{Q}$, so by (4), f is **irreducible**

- over $\mathbb{C}$ (or any other algebraically closed field), the **irreducibles** are exactly the polynomials of degree 1

4.4.2 Using the Mod p Method

Let:

$$f(t) = a_0 + a_1 t + \ldots + a_n t^n \in \mathbb{Z}[t]$$

Let $\pi : \mathbb{Z} \to \mathbb{Z}_p$ be the canonical homomorphism, and $\pi_* : \mathbb{Z}[t] \to \mathbb{Z}_p[t]$ the resulting induced homomorphism. Define notation:

$$\pi(a) = \bar{a} \qquad \pi_*(f) = \bar{f}$$

If there exists a prime p such that:

- $p \nmid a_n$
- $\bar{f} \in \mathbb{Z}_p[t]$ *is* ***irreducible***

then f is ***irreducible*** *over $\mathbb{Q}$.*
(Proposition 3.3.9)

- consider:

  $$f(t) = 9 + 14t - 8t^3$$

  and let $p = 7$. Clearly, $7 \nmid -8$. Moreover, over $\mathbb{Z}_7$, the polynomial becomes:

  $$\bar{f} = 2 - t^3$$

  Recall, by the above test for irreducibility, since $\bar{f}$ has degree 3, it is sufficient to show that $2 - t^3$ has no roots in $\mathbb{Z}_7$. Indeed:

  - $\bar{0}^3 = \bar{0}$
  - $\bar{1}^3 = \bar{1}$
  - $\bar{2}^3 = \bar{1}$
  - $\bar{3}^3 = \bar{1}$
  - $\bar{4}^3 = \bar{-3}^3 = \bar{-6} = \bar{1}$
  - $\bar{5}^3 = \bar{-2}^3 = \bar{-1} = \bar{6}$
  - $\bar{6}^3 = \bar{-1}^3 = \bar{-1} = \bar{6}$

  so no $t \in \mathbb{Z}_7$ satisfyies $t^3 - 2$. Hence, by the mod p method, $f(t) = 9 + 14t - 8t^3$ is irreducible

- if instead we'd used $p = 3$, we'd get that:

  $$\bar{f} = -t + t^3 = t(t^2 - 1)$$

  so $\bar{f}$ is reducible over $\mathbb{Z}_3$; however, clearly this doesn't mean that f is reducible. The mod p method is only useful when determining whether something is *irreducible*

- if we take $f(t) = 6t^2 + t$, this is clearly reducible. If we ignore the condition $p \nmid a_n$, we'd get that $\bar{f} = t$, which is irreducible. Hence, it's a necessary condition!

4.4.3 Using Eisenstein's Criterion

Let:

$$f(t) = a_0 + \ldots + a_n t^n \in \mathbb{Z}[t]$$

where $n \geq 1$.
Suppose there exists a prime p*, such that:*

- $p \nmid a_n$
- $\forall i \in [0, n-1],\ p \mid a_i$
- $p^2 \nmid a_0$

Then. f *is* ***irreducible*** *over* $\mathbb{Q}$.
(Proposition 3.3.12)

- consider:

$$g(t) = \frac{2}{9}t^5 - \frac{5}{3}t^4 + t^3 + \frac{1}{3} \in \mathbb{Q}[t]$$

By Gauss's Lemma, we know that g is irreducible over $\mathbb{Q}$ if and only if:

$$9g(t) = 2t^5 - 15t^4 + 9t^3 + 3$$

is irreducible over $\mathbb{Q}$; by Eisenstein's criterion with $p = 3$, it is clear that this is the case:

  - $3 \nmid 2$
  - $3 \mid -15$
  - $3 \mid 9$
  - $3^2 \nmid 3$

- let p be prime. The pth **cyclotomic polynomial** is:

$$\Phi_p(t) = 1 + t + \ldots + t^{p-1} = \frac{t^p - 1}{t - 1}$$

We can't immediately apply Eisenstein's Criterion: no prime can divide any of the coefficients. Instead, we use the substitution homomorphism, which tells us that $\Phi_p(t)$ is irreducible if and only if $\Phi_p(t-c)$ is irreducible, for any $c \in \mathbb{Q}$. If we take $c = -1$:

$$\begin{aligned}
\Phi_p(t+1) &= \frac{(t+1)^p - 1}{(t+1) - 1} \\
&= \frac{1}{t}((t+1)^p - 1) \\
&= \frac{1}{t}\sum_{i=1}^{p} \binom{p}{i} t^i \\
&= p + \binom{p}{2} t + \ldots + \binom{p}{p-1} t^{p-2} + t^{p-1}
\end{aligned}$$

As we showed last week, each $\binom{p}{j}$ is divisible by p when $j \in [1, p-1]$. Moreover, clearly t^{p-1} isn't, and p isn't divisible by p^2. Thus, by Eisenstein's criterion, $\Phi_p(t)$ is irreducible.

If we don't restrict ourselves to p prime, the nth cyclotomic polynomial is defined by:

$$\Phi_n(t) = \prod_{\omega}(t - \omega)$$

where each ω is an nth root of unity. Whilst not obvious:

- *the coefficients of Φ_n are* ***real***
- *not only that, they are* ***rational***
- *not even that, they are* ***integers***
- *the* ***degree*** *of Φ_n is $\varphi(n)$. the* ***Euler totient function*** *(the number of integers between 1 and n which are coprime to n)*
- Φ_n *is* ***irreducible*** *for* ***all*** $n \geq 1$