

MA40037
Galois Theory
Lectures by Geoff Smith

(Notes by Graeme Taylor)

Lecture course ran Semester 1, 04/05 academic year

Contents

1	Ring Theory	3
1.1	Rings	3
1.1.1	New rings from old	3
1.2	Motivation	3
1.3	Integral Domains	4
1.4	Fields of fractions	5
1.5	Units	6
1.5.1	Discussion of \mathbb{G}	7
1.6	Ideals	7
1.7	Homomorphisms	8
1.8	The first isomorphism theorem for rings	9
1.8.1	Quotient structures	9
1.8.2	First Isomorphism Theorem for Rings	10
1.9	The Chinese Remainder Theorem	11
1.10	More on Ideals	12
1.11	Irreducibles	14
1.11.1	Irreducibles of $\mathbb{F}[x]$	15
1.12	Field Extensions	16
1.13	Characteristic of a field	17
1.14	More on Irreducibles	18
1.15	Minimal Polynomials	19
1.15.1	Algebraic Integers	21
1.16	A few more prosaic details	21
2	Galois Theory	25
2.1	Preliminaries	25
2.2	Most celebrated application	27
2.3	Technicalities	27
2.4	Fundamental Theorem of Galois Theory	29

1 Ring Theory

1.1 Rings

Definition. A *commutative ring with 1* (“ring”) is a set R equipped with two binary operations $+, \cdot$ (the latter is often abbreviated to \cdot) such that

- $\exists 0 \in R$ st $R, +, 0$ is an abelian group
- Multiplication is closed, associative, commutative, distributes over $+$, and 1 is a multiplicative identity

Example. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all rings.

For $n \in \mathbb{N}$, \mathbb{Z}_n is a ring. Note that in \mathbb{Z}_4 , $2 \cdot 2 = 0$.

1.1.1 New rings from old

Suppose that R_1, \dots, R_n are rings, then you can form

$$\bigoplus_{i=1}^n R_i = R_1 \oplus \dots \oplus R_n = \{(a_1, \dots, a_n) \mid a_i \in R_i \forall i \in 1 \dots n\}$$

With $+$ and \cdot defined ”co-ordinate wise”. The zero is $(0, 0, \dots, 0)$ and the multiplicative identity is $(1, 1, \dots, 1)$.

Another possibility, given a ring R , is to form the collection $R[x]$ of “Polynomials in x ” with coefficients in R . A polynomial is a formal expression $a_0 + a_1x + \dots + a_nx^n$ where $n \in \mathbb{N} \cup \{0\}$ and addition and multiplication are defined as usual.

You can even form $R[[x]]$, the ring of formal power series, where elements are expressions $a_0 + a_1x + a_2x^2 + \dots$. Addition and multiplication are defined in the obvious way- for $f, h \in R[[x]]$ with

$$f = \sum_{i=0}^{\infty} a_i x^i, h = \sum_{j=0}^{\infty} b_j x^j,$$

$$f + h = \sum_{k=0}^{\infty} c_k x^k, \text{ where } c_k = a_k + b_k \forall k \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$$

$$fh = \sum_{l=0}^{\infty} d_l x^l, \text{ where } d_l = \sum_{s=0}^l a_s b_{l-s}$$

It is easy to verify that $R[x]$ and $R[[x]]$ are rings.

1.2 Motivation

Galois Theory, invented by Evariste Galois in the early 19th century, is the investigation, via group theory, of the roots of polynomials.

1.3 Integral Domains

Definition. A ring R is an *integral domain* (i.e., it is like the integers) if whenever $a, b \in R$ and $a \neq 0 \neq b$ then $ab \neq 0$; moreover we also insist that $1 \neq 0$.

Example. $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$ (for p prime) are all integral domains. \mathbb{Z}_n (for n composite) is not, nor is $\mathbb{Z} \oplus \mathbb{Z}$.

Justification p a prime $[x] \in \mathbb{Z}_p$ $x \in \mathbb{Z}$, $[x] \neq [0]$

So $p \nmid x$, Therefore $\gcd(x, p) = 1$

By Euclid's algorithm, $\exists \lambda, \mu \in \mathbb{Z}$ st $\lambda x + \mu p = 1$

Therefore $[\lambda][x] = [1]$ in \mathbb{Z}_p .

Now suppose $[x][y] = [0]$. Then $([\lambda][x])[y] = [\lambda][0] \therefore [y] = [0]$ and of course $[1] \neq [0]$ in \mathbb{Z}_p (incidentally, we have shown that non-zero elements of \mathbb{Z}_p have multiplicative inverses, so \mathbb{Z}_p is actually a *field*.)

If $n = rs$, $1 < r, s < n$ then $[r] \neq [0] \neq [s]$ but $[r][s] = [0]$.

In $\mathbb{Z} \oplus \mathbb{Z}$, $(1, 0) \cdot (0, 1) = (0, 0) = 0$ yet $(1, 0) \neq (0, 0) \neq (0, 1)$.

Proposition 1.1. *If R is a finite integral domain, then it is a field.*

Proof. Suppose that $r \in R \setminus \{0\}$. It suffices to show that r has a multiplicative inverse. Define a map

$$\begin{aligned} \mu_R : R &\rightarrow R \\ x &\mapsto xr \quad \forall x \in R \end{aligned}$$

Suppose that $(x)\mu_R = (y)\mu_R$ for some $x, y \in R$

Then $xr = yr$, so $(x - y)r = 0$

Now $r \neq 0$ and R is an ID so $x - y = 0$ i.e., $x = y$.

Therefore μ_R is an injective map, but R is finite, so μ_R is also surjective. Choose $z \in R$ such that $(z)\mu_R = 1$, uniquely by bijectivity. Thus $zr = 1$ i.e., z is the inverse of r . ■

Definition. R any ring, $S = R[x]$. If $f = \sum_{i=0}^n a_i x^i$ and $a_n \neq 0$ we define the *degree* of f to be n ,

and write it $\deg f$ or $\deg(f)$.

We define the degree of the zero polynomial to be $-\infty$, where this symbol has the properties:

- $-\infty < z \forall z \in \mathbb{Z}$
- $(-\infty) + (-\infty) = (-\infty) + x = x + (-\infty) = -\infty \quad \forall x \in \mathbb{Z}$

Proposition 1.2. *In this notation, if $f, h \in S$ then, provided R is an ID,*

$$\deg(f \pm h) \leq \max\{\deg f, \deg h\}$$

$$\deg(fh) = \deg(f) + \deg(h)$$

NB: This result forces the definition of $\deg 0 = -\infty$.

If R is an ID, so is $S = R[x]$, and therefore so is $S[y] = R[x, y]$: polynomials in two commuting variables with coefficients in R . Indeed by induction $R[x_1, \dots, x_n]$ is an ID.

Definition. R a ring, $S \subseteq R$ is called a *subring* of R if $1_R \in S$ and S is a ring in its own right using $+$, \cdot borrowed from R .

Example. \mathbb{Z} is a subring of \mathbb{C} .

R is a subring of $R[x]$ where R is a ring (via the constants)

Non-example. $R = \mathbb{Z} \oplus \mathbb{Z}$, $S = \{(x, 0) \mid x \in \mathbb{Z}\}$

S is a ring and a subset of R , but it is not a subring since $1_R = (1, 1) \notin S$.

1.4 Fields of fractions

A construction

Suppose that R is an ID. Let $\Omega = R \times (R \setminus \{0\}) = \{(r, s) \mid r, s \in R, s \neq 0\}$. Define a relation \sim on Ω via

$$(r, s) \sim (r', s') \text{ iff } rs' = r's$$

It is routine to verify that \sim is an equivalence relation; we write the equivalence class of (r, s) as $\frac{r}{s}$.

We try to define $+$ and \cdot on Ω / \sim (the set of equivalence classes) thus-

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{s_2 r_1 + s_1 r_2}{s_1 s_2}$$

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

It is vital to verify that these operations are well-defined. Suppose that $\frac{r_1}{s_1} = \frac{u_1}{v_1}$ and $\frac{r_2}{s_2} = \frac{u_2}{v_2}$. For addition, we want to show that

$$\frac{s_2 r_1 + s_1 r_2}{s_1 s_2} = \frac{v_2 u_1 + v_1 u_2}{v_1 v_2}$$

i.e., that $v_1 v_2 (s_2 r_1 + s_1 r_2) = (v_2 u_1 + v_1 u_2) s_1 s_2$. But we know $r_1 v_1 = s_1 u_1$ and $r_2 v_2 = s_2 u_2$ so

$$\begin{aligned} LHS &= v_1 v_2 (s_2 r_1 + s_1 r_2) \\ &= s_1 u_1 s_2 v_2 + v_1 v_2 s_1 r_2 \\ &= s_1 u_1 s_2 v_2 + v_1 s_1 s_2 u_2 = RHS \end{aligned}$$

Further, for multiplication¹ we require that

$$\frac{r_1 r_2}{s_1 s_2} = \frac{u_1 u_2}{v_1} v_2$$

¹originally an exercise

i.e., that $v_1v_2r_1r_2 = u_1u_2s_1s_2$.

$$\begin{aligned}
 LHS &= v_1v_2r_1r_2 \\
 &= v_1r_1v_2r_2 \\
 &= s_1u_1s_2u_2 \\
 &= u_1u_2s_1s_2 = RHS
 \end{aligned}$$

It is now a routine matter to verify that $\Omega/\sim = F_R$ forms a field. We can regard R as a subring of F_R via $r \mapsto r/1$.

Recall that if R is an ID then the polynomial rings $R[x]$ and $R[x_1, \dots, x_n]$ are IDs. In these cases the fields of fractions have special names- for $R[x]$ we use $R(x)$ and for $R[x_1, \dots, x_n]$ we use $R(x_1, \dots, x_n)$. These are often called *fields of rational functions*.

Example. $\mathbb{Q}(x) = \{f/g \mid f, g \in \mathbb{Q}[x], g \neq 0\}$.

1.5 Units

Let R be a ring. An element $u \in R$ is a *unit* if $u|1$ i.e., $\exists v \in R$ st $uv = 1$. Observe that 1 is a unit. The set of units of R is variously denoted $U(R) = U_R = R^0 = R^*$; we will use U_R . Notice that U_R is a group under multiplication, specifically, an abelian group.

- $U_{\mathbb{Z}} = \{-1, 1\}$
- $U_{\mathbb{Q}} = \mathbb{Q} \setminus \{0\}$
- $U_{\mathbb{F}} = \mathbb{F} \setminus \{0\}$ for any field \mathbb{F} .
- $U_{\mathbb{Q}[x]} = \mathbb{Q} \setminus \{0\}$
- $U_{\mathbb{G}} = \{1, -1, i, -i\}$ where \mathbb{G} are the Gaussian integers.

Definition. For R a ring, $r, s \in R$, we say r and s are *associates* (denoted $r \sim s$) if $\exists u \in U_R$ st $ru = s$. Check reflexivity, symmetry and transitivity to see this is an equivalence relation.

Gauss' Fundamental Theorem of Arithmetic asserts (loosely) that factorisation in $\mathbb{Z} \setminus \{0\}$ into unfactorable elements is more or less unique. For instance, $6 = 2 \times 3 = 3 \times 2 = 1 \times 3 \times 2 = (-3) \times (-2) \dots$

Definition. $x \notin U_{\mathbb{Z}}$ a non-zero integer is *irreducible* if whenever $x = yz$ for $y, z \in \mathbb{Z}$ then $y \in U_{\mathbb{Z}}$ or $z \in U_{\mathbb{Z}}$

Thus Gauss' FTA formally asserts: If $x \in \mathbb{Z} \setminus \{-1, 0, 1\}$ then there exist irreducible $a_1, \dots, a_n \in \mathbb{Z}$ such that $x = a_1 \cdots a_n$ and if $b_1 \cdots b_m = x$ is a rival factorisation then $m = n$ and there is a permutation π of $1, \dots, n$ st for each i , $a_{\pi(i)} \sim b_i$.

This notion of irreducible makes sense in an arbitrary ring R : see section 1.11. An integral domain R in which the FTA holds is called a *UFD* (unique factorisation domain). Examples include \mathbb{G} , $\mathbb{Q}[x]$, $\mathbb{F}[x]$ for \mathbb{F} a field, $\mathbb{F}[x_1, \dots, x_n]$.

1.5.1 Discussion of \mathbb{G}

$U_{\mathbb{G}} = \{1, -1, i, -i\}$. We call the irreducibles *Gaussian Primes*, for instance 7 (and $-7, 7i, -7i$) but not 2 (which has a factorisation $2 = (1+i)(1-i)$).

$1+i$ is a Gaussian prime, since if $(1+i) = g_1 \cdot g_2$ then $(1+i)(1-i) = g_1 \overline{g_1} \cdot g_2 \overline{g_2}$ so $2 = |g_1|^2 |g_2|^2$ which forces $\{g_1, g_2\} = \{1, 2\}$. Wlog $|g_1| = 1, |g_2| = \sqrt{2}$. $\therefore g_1 \overline{g_1} = 1$ so $g_1 |_{\mathbb{G}} 1$ i.e., $g_1 \in U_{\mathbb{G}}$ and hence $1+i$ is a Gaussian prime.

For $p \in \mathbb{Z}$ a prime, there are 3 possibilities:

- $p = 2 = (1+i)(1-i)$ gives rise to two Gaussian primes as demonstrated above.
- $p \equiv 3 \pmod{4}$ ($3 \pmod{4}$); then p is a Gaussian prime.
- $p \equiv 1 \pmod{4} \Rightarrow p = a^2 + b^2$ for some integers a, b (this is *Fermat's 2 squares theorem*. Thus $p = (a+ib)(a-ib)$, a unique factorisation into two Gaussian primes (hence, a and b are themselves unique).

All Gaussian primes are these and their associates.

1.6 Ideals

Definition. Suppose that R is a ring. A subset $I \subseteq R$ is an *ideal* if both

- I is an additive subgroup of $(R, +, 0)$.
- $a \in I$ and $r \in R \Rightarrow ra \in I$.

Example. For $R = \mathbb{Z}$

$$I = \{42k \mid k \in \mathbb{Z}\} \tag{1}$$

gives an ideal of R .

Example. For $S = R[[x]]$ (formal power series with integer coefficients)

$$J = \{f \mid f \in S, f = \sum_{i=0}^{\infty} a_i x^i, a_0 \text{ even}\} \tag{2}$$

gives an ideal of S .

Notation “ I is an ideal of R ” is written $I \trianglelefteq R$.

Let $r \in R$ any ring, then $(r) = \{rt \mid t \in R\} \trianglelefteq R$ (an ideal with the property that $\exists a \in R$ st the ideal is (a) is called a *principal ideal*). More generally, if $\Omega \subseteq R$ then

$$(\Omega) = \left\{ \sum'_{w \in \Omega} \lambda_w w \mid \lambda_w \in R \forall w \in \Omega \right\}$$

is an ideal of R , where Σ' denotes that all but finitely many summands are zero. If $\Omega = \{w_1, w_2, \dots, w_n\}$ is finite we can write $(\Omega) = (w_1, w_2, \dots, w_n)$; an ideal of this shape is called a *finitely generated ideal*.

For example (1), $I = (42)$ is a principal ideal; whereas in example (2) $J = (2, x)$ is (verify) a finitely generated ideal but is not a principal ideal².

An example of an ideal which is not finitely generated is

$$T = \mathbb{Q}[x_1, x_2, x_3, \dots] \text{ Polynomials in infinitely many commuting variables}$$

$$I = (x_1, x_2, x_3, \dots)$$

Note I is the set of polynomials with constant term zero.

Ideals play a similar role in ring theory to that of normal subgroups in group theory.

1.7 Homomorphisms

Definition. R and S rings, a map $\theta : R \rightarrow S$ is a *homomorphism (of rings)* if the following hold:

- $(r + s)\theta = (r)\theta + (s)\theta \forall r, s \in R$ (so $(0_R)\theta = 0_S$)
- $(rs)\theta = (r)\theta \cdot (s)\theta \forall r, s \in R$
- $(1_r)\theta = 1_S$

Example.

$$\epsilon_{42} : \mathbb{Q}[x] \rightarrow \mathbb{Q}$$

$$f \mapsto f(42) \forall f \in \mathbb{Q}[x]$$

Equivalently, $(f)\epsilon_{42} = f(42)$.

Example.

$$\pi : \mathbb{Z} \rightarrow \mathbb{Z}_{42}$$

$$x \mapsto [x]_{42} \text{ "x mod 42"}$$

²Exercise: why?

Proposition 1.3. Let R, S be rings and $\theta : R \rightarrow S$ be a ring homomorphism. Let

$$K = \text{Ker}(\theta) := \{r \mid r \in R \text{ } (r)\theta = 0\}$$

Then $K \trianglelefteq R$.

Proof. Suppose $k_1, k_2 \in K$. Then $(k_1)\theta = (k_2)\theta = 0$.

$\therefore (k_1 + k_2)\theta = (k_1)\theta + (k_2)\theta = 0 + 0 = 0$ so $k_1 + k_2 \in K$.

Also $(0)\theta = (0)\theta + (0)\theta$ since $0 = 0 + 0$, so $0 = (0)\theta$. Hence $0 = (0)\theta = (k_1 + -k_1)\theta$ i.e., $0 + (-k_1)\theta = 0$ so $-k_1 \in K$. Further $0 \in K \neq \emptyset$. Thus K is an additive subgroup of $(R, +, 0)$.

Now if $r \in R$ and $k \in K$, $(rk)\theta = (r)\theta \cdot (k)\theta = (r)\theta \cdot 0 = 0$ ■

Note that θ is injective (a *monomorphism*) iff $\text{ker } \theta = 0$ (from theory of abelian groups).

1.8 The first isomorphism theorem for rings

1.8.1 Quotient structures

Suppose that R is a ring and $I \trianglelefteq R$. Let

$$R/I = \{a + I \mid a \in R\}$$

Example. $R = \mathbb{Z}, I = (3)$

$$R/I = \{0 + I, 1 + I, 2 + I\}$$

The cosets of I in R form a partition of R (The reason for this is group theoretic):

If $r \in R$ then $r \neq 0 \in (r + I)$ so $R \subseteq \bigcup_{r \in R} (r + I)$.

Now suppose $x \in [r + I] \cap [s + I]$ so $x = r + \lambda$ for some $\lambda \in I$ and

$r = x - \lambda \therefore x + I = r + \lambda + I = r + I$ as $\lambda + I = I$. By same argument for s in place of r , $x + I = s + I$.

Hence $r + I = s + I$ i.e. the cosets are disjoint.

We render R/I into a ring as follows

$$\begin{aligned} [a + I] + [b + I] &:= \{a + \lambda_1 + b + \lambda_2 \mid \lambda_1, \lambda_2 \in I\} \\ &= \{a + b + \lambda \mid \lambda \in I\} \\ &= [a + b] + I \end{aligned}$$

This makes R/I an abelian group with identity $0 + I = I$. We can similarly define

$$[a + I] \times [b + I] = [ab + I]$$

to obtain an associative multiplication with identity $1 + I$, and so the ring axioms hold³

³you should verify these details; there are some technicalities to ensure $\exists! x + I$ st $(a+I)(b+I) \subseteq x + I = ab + I$.

We have a natural (in the sense of categories) map

$$\pi : R \rightarrow R/I$$

$$r \mapsto r + I \forall r \in R$$

We can (and you should!) easily check π is an *epimorphism* (surjective ring homomorphism). Notice

$$\ker \pi = \{r \mid r \in R, r + I = 0 + I\} = I$$

1.8.2 First Isomorphism Theorem for Rings

Theorem 1.4 (First Isomorphism Theorem). *Suppose that R, S are rings and $\theta : R \rightarrow S$ is a ring homomorphism. Then let $\pi : R \rightarrow R/\ker \theta$ be the natural epimorphism. Then there is a unique ring isomorphism (mono- and epimorphism)*

$$\hat{\theta} : R/\ker \theta \rightarrow \text{Im } \theta$$

such that, shrinking the image of θ , $\theta = \pi \circ \hat{\theta}$, i.e., the following diagram commutes⁴:

$$\begin{array}{ccc} R & \xrightarrow{\theta} & S \\ \downarrow \pi & \nearrow \hat{\theta} & \\ R/\ker \theta & & \end{array}$$

Proof. Define $\hat{\theta}$, as you must, by

$$(r + I)\hat{\theta} := (r)\theta \quad \forall r \in R \text{ where } I = \ker \theta$$

Well-defined: If $r_1 + I = r_2 + I$ then $r_1 - r_2 \in I$

$$\therefore (r_1 - r_2)\theta = 0 \text{ as } I = \ker \theta$$

$$\therefore (r_1)\theta - (r_2)\theta = 0 \therefore (r_1)\theta = (r_2)\theta$$

Donkey work: $\hat{\theta}$ is a homomorphism of rings $R/I \rightarrow \text{Im } \theta$ (exercise!)

Surjectivity: $\hat{\theta}$ is visibly surjective since if $(r)\theta \in \text{Im } \theta$ then $(r + I)\hat{\theta} = (r)\theta$.

Injectivity: Let $K = \ker \hat{\theta}$. If $(r + I) \in K$ then

$$(r)\theta = 0 \therefore r \in \ker \theta = I \therefore r + I = I = 0_{R/I}$$

so $\hat{\theta}$ is injective.

Thus we have an isomorphism of rings.

⁴either route to S yields the same result

Uniqueness: Suppose that $\bar{\theta}$ is a rival to $\hat{\theta}$, then if $r \in R$

$$((r)\pi)\bar{\theta} = (r)\theta$$

Thus

$$(r + I)\bar{\theta} = (r)\theta = (r + I)\hat{\theta}$$

Since $\hat{\theta}, \bar{\theta}$ have the same domain and codomain, $\hat{\theta} = \bar{\theta}$. ■

1.9 The Chinese Remainder Theorem

Notation For a ring R with ideals I, J , we define

$$I + J = \{a + b \mid a \in I, b \in J\}$$

$$IJ = \left\{ \sum_{i=1}^n a_i b_i \mid (a_i, b_i) \in I \times J, 1 \leq i \leq n \right\}$$

It is routine to check that these are also ideals of R .

Lemma 1.5. For R a ring and I_1, I_2, \dots, I_n ideals of R with the co-primality / co-maximality property $I_i + I_j = (1)$ whenever $i \neq j$,

$$I_1 + I_2 I_3 \cdots I_n = (1)$$

Proof. For $i = 2, \dots, n$ choose $a_i \in I_1, b_i \in I_i$ such that $a_i + b_i = 1$. Multiplying these gives a large number of terms on the LHS, all of which other than $b_2 b_3 \cdots b_n$ is in I_1 . Thus $1 \in I_1 + I_2 I_3 \cdots I_n$ as required. ■

Lemma 1.6. For R a ring and I_1, I_2, \dots, I_n ideals of R with the co-primality / co-maximality property $I_i + I_j = (1)$ whenever $i \neq j$,

$$I_1 I_2 \cdots I_n = \bigcap_{i=1}^n I_i$$

Proof. $I_1 I_2 \subseteq I_1 \cap I_2$. Note that $1 = a + b$ for some $a \in I_1, b \in I_2$ so for any $x \in I_1 \cap I_2$, $x = x(a + b) = xa + xb \in I_1 I_2$ so additionally $I_1 \cap I_2 \subseteq I_1 I_2$. Hence $I_1 I_2 = I_1 \cap I_2$. Induction and Lemma 1.5 ensure the result then holds for general n . ■

Theorem 1.7 (Chinese Remainder Theorem). Let R be a ring and I_1, I_2, \dots, I_n ideals of R with the co-primality / co-maximality property $I_i + I_j = (1)$ whenever $i \neq j$.

For each i let $\theta_i : R \rightarrow S_i$ be a ring epimorphism with kernel I_i , and define

$$\theta : R \rightarrow S_1 \oplus S_2 \oplus \cdots \oplus S_n$$

$$(r)\theta = ((r)\theta_1, (r)\theta_2, \dots, (r)\theta_n)$$

for each $r \in R$. Then

$$R/I_1 I_2 \cdots I_n \simeq S_1 \oplus S_2 \oplus \cdots \oplus S_n \text{ (Isomorphic)}$$

Proof. The kernel of θ is evidently the intersection of the ideals I_i , but by Lemma 1.6 this is also their product. Thus we have

$$\text{Ker } \theta = I_1 I_2 \cdots I_n$$

Further, θ surjects. For instance, $e_1 = (1, 0, 0, \dots, 0) \in \text{Im } \theta$ since by Lemma 1.5 there are $a \in I_1, b \in I_2 I_3 \cdots I_n$ with $a + b = 1$ ensuring $(b)\theta = (1 - a)\theta = (1, 0, 0, \dots, 0)$. This generalises for each such e_i consisting of all entries zero except for an entry of 1 in position i . This suffices to ensure that θ is surjective by the surjectivity of each θ_i . So

$$\text{Im } \theta = S_1 \oplus S_2 \oplus \cdots \oplus S_n$$

The first isomorphism theorem therefore applies to give the desired result. ■

Example. $\mathbb{Z}_{2004} \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{167}$

Proof. 3,4,167 are pairwise coprime, so Euclid's algorithm gives

$$(4) + (3) = (4) + (167) = (3) + (167) = (1)$$

Therefore the Chinese Remainder Theorem gives

$$\mathbb{Z}/(2004) \simeq \mathbb{Z}/(4) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(167)$$

with the natural isomorphism

$$[z]_{2004} \mapsto ([z]_4, [z]_3, [z]_{167})$$

■

Example. There are 8 elements in the range $0 \leq x \leq 2003$ such that $x^2 \equiv 1 \pmod{2004}$.

Proof. We can exploit the isomorphism above to work in $S = \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{167}$. To equal 1 in \mathbb{Z}_{2004} , a number must equal $(1, 1, 1)$ in S . Since \mathbb{Z}_3 and \mathbb{Z}_{167} are fields and thus integral domains, $a^2 = 1 \Rightarrow a = \pm 1$. \mathbb{Z}_4 is not an ID, but inspection reveals that again the only elements that square to 1 are ± 1 . So choosing 1 such element for each coordinate gives $2^3 = 8$ choices of x .

The keen student may wish to find these elements! ■

1.10 More on Ideals

Definition. R a ring, $I \trianglelefteq R$.

I is a *prime ideal* if both

- $I \neq R = (1)$
- If $a, b \in R$ st $a, b \notin I$ then $ab \notin I$

Definition. R a ring, $I \trianglelefteq R$.

I is a *maximal ideal* if both

- $I \neq R = (1)$
- Whenever $J \trianglelefteq R$ and $I \subseteq J \subseteq R$ then $I = J$ or $R = J$

Proposition 1.8. R a ring, $I \trianglelefteq R$ then

(a) I is a prime ideal iff R/I is an integral domain.

(b) I is a maximal ideal iff R/I is a field.

Proof (a). I a prime ideal $\Rightarrow I \neq R$ by definition $\Rightarrow R/I$ has more than one element. So $1+I \neq 0+I$ else $1 \in I$ and $I = R$. $\therefore 1_{R/I} \neq 0_{R/I}$.

Also if $a+I, b+I \in R/I$ are not $0_{R/I}$ then $a+I, b+I \neq I$ i.e., $a, b \notin I$. I is a prime ideal so $ab \notin I$. Therefore $ab+I \neq I = 0_{R/I}$ so R/I is an integral domain.

Conversely, if R/I is an ID then $1_{R/I} \neq 0_{R/I}$ so $1+I \neq 0+I$ so $1 \notin I$ and $I \neq R$.

Suppose $x, y \in R - I$ then $x+I, y+I \neq I = 0_{R/I}$. R/I is an ID so $xy+I \neq 0 = I \therefore xy \notin I$. ■

Proof (b). Suppose I is maximal. We need to show that if $x+I \neq I$ then $\exists y \in R$ with $xy+I = 1+I$, as then $y+I$ is a multiplicative inverse for $x+I$.

Well, $x \notin I \therefore (I \cup \{x\}) = R$ since $I \subsetneq (I \cup \{x\}) \trianglelefteq R$ and I is maximal. $\therefore 1 \in (I \cup \{x\})$. So

$$1 = r_1\lambda_1 + r_2\lambda_2 + \dots + r_k\lambda_k + sx \text{ for some } r_1, \dots, r_k, s \in R \text{ and } \lambda_1, \dots, \lambda_k \in I$$

Therefore $1 = \lambda + sx$ for some $\lambda \in I$. Hence $1+I = \lambda + sx + I = sx + I = xs + I$. Let $y = s$.

Conversely, suppose R/I is a field, so $1+I \neq 0+I \therefore 1 \notin I$ and $I \subsetneq R$. Suppose that $J \trianglelefteq R$ and $I \subsetneq J \subset R$. We need to show $J = R$.

$\exists j \in J - I$. Now $j+I \neq 0+I$ else $j \in I$. R/I is a field thus $\exists k \in R$ st $(j+I)(k+I) = jk+I = 1+I$. $\therefore 1 - jk \in I$ i.e., $1 = jk + \lambda$ for some $\lambda \in I$. Since $jk \in J, \lambda \in I \subset J, jk + \lambda \in J$ so $1 \in J$.

So $R = (1) \subseteq J \subseteq R$ i.e., $J = R$ ■

Note A field is an ID so a maximal ideal must be a prime ideal.

Example. $R = \mathbb{Z}$

The prime ideals are (p) where p is a common or garden prime number. Then $\mathbb{Z}/(p) = \mathbb{Z}_p$ the integers mod p .

(0) is an ideal and is the only other prime ideal (*Exercise- why?*). $\mathbb{Z}/(0)$ is morally equivalent to \mathbb{Z} since $x \mapsto x+0$.

The maximal ideals are (p) for p prime since \mathbb{Z}_p are fields; (0) is not maximal since $(0) \subset (p)$ yet $(0) \neq (p) \neq \mathbb{Z}$. Worse, consider $(42) = (2) \cap (3) \cap (7)$ neither maximal nor prime, yet also contains (0) .

If $(x) \neq 0 \neq (y)$ in \mathbb{Z} with $(x) \subseteq (y)$ then $y|x$.

Definition. A *principal ideal ring* (PIR) R is a ring where if $I \trianglelefteq R$ then $\exists r \in R$ st $I = (r)$.

Example. \mathbb{Z}_n for $n \in \mathbb{N}$.

Definition. A *principal ideal domain* (PID) R is an integral domain which is a PIR.

Example. \mathbb{Z}, \mathbb{Z}_p for p a prime, $\mathbb{F}[x]$ for \mathbb{F} a field.

1.11 Irreducibles

Definition. $r \in R$ a ring, $r \neq 0$, $r \notin U_R$

We say r is *irreducible* if whenever $r = st$ for $s, t \in R$, then $s \in U_R$ or $t \in U_R$.

Example. In \mathbb{Z} , the irreducible elements are $\pm p$ for p prime.

Proposition 1.9. Let R be a PID which is not a field, and $I = (r)$ an ideal of R . Then the following are equivalent:

1. I is a maximal ideal of R .
2. I is a non-zero prime ideal of R .
3. r is irreducible.

Proof. $1 \Rightarrow 2$

From earlier, I maximal $\Rightarrow I$ prime. If $I = (0)$ then maximality of I and the fact that $1 \neq 0$ as we are working in an integral domain ensures that R has precisely two ideals, $(0), (1)$. This in turn ensures that R is a field⁵. But R is assumed to not be a field, so it cannot be that $I = (0)$. Hence, I is non-zero and prime.

$2 \Rightarrow 3$

$I = (r) \neq (0)$. Suppose $r = st$ with $s, t \in R$. Then $st \in I$ so by primality of I , one of s, t is in I . Wlog, let $s \in I$. Hence $s = rw$ for some $w \in R$. $\therefore r = st = rwt$ so $r(1 - wt) = 0$. As $r \neq 0$ and R is an integral domain, it follows that $1 - wt = 0$ i.e., $wt = 1 \Rightarrow t \in U_R \Rightarrow r$ irreducible.

$3 \Rightarrow 1$

Suppose that r is irreducible and $(r) = I \subsetneq J \trianglelefteq R$. As R a PID, $J = (j)$ for some $j \in J$. Further $j \notin I$ else $J \subset I$ which would force $I = J$, which is false by construction. Since $r \in I, r \in J = (j)$. So $\exists k \in R$ st $r = kj$. The irreducibility of r forces $j \in U_R$ or $k \in U_R$. Were $k \in U_R$ then $\exists k'$ with $kk' = 1$, then $j = jkk' = rk' \in (r) = I$ which would give a contradiction, namely $J \subset I$ as before. Thus $j \in U_R$ so $\exists j' \in R$ with $1 = jj' \in (j) = J$. So $J = R$ and I is maximal. ■

Proposition 1.10. \mathbb{Z} is a PID.

Proof. \mathbb{Z} is an integral domain. Suppose $I \trianglelefteq \mathbb{Z}$ with $I \neq (0)$. Choose $x \in I$ st $x \neq 0$ and $|x|$ is minimal. Replacing x by $-x$ if necessary, wma $x > 0$.

Now if $y \in I, y = qx + r (q, r \in \mathbb{Z}) 0 \leq r < x$. Then $r = y - qx \in I$. Since x is the smallest non-zero positive element of I , r is necessarily 0 else $0 < r < x$. So $y = qx \in (x) \therefore I \subseteq (x)$.

But since $x \in I, (x) \subseteq I$ hence $I = (x)$ a principal ideal. ■

⁵This was a problem sheet exercise.

Proposition 1.11. *If \mathbb{F} is a field, then $\mathbb{F}[x]$ is a PID.*

Proof. Exercise⁶ ■

1.11.1 Irreducibles of $\mathbb{F}[x]$

What are the irreducible elements of $\mathbb{F}[x]$? This depends on \mathbb{F} .

$\mathbb{C}[x]$ Here the irreducible polynomials are the linear polynomials. This follows from Gauss' *Fundamental Theorem of Algebra*.

$\mathbb{R}[x]$ Here the irreducible polynomials are

- the linear polynomials
- the quadratic polynomials of negative discriminant

Note that α a root of $f \in \mathbb{R}[x]$ in \mathbb{C} then $\bar{\alpha}$ is also a root with $g = (x - \alpha)(x - \bar{\alpha}) \in \mathbb{R}[x]$ so either α is real and f has $(x - \alpha)$ as a factor; or $\alpha \notin \mathbb{R}$ and g is irreducible in the context of $\mathbb{R}[x]$, with $g|f$.

$\mathbb{Q}[x]$ Here “most” polynomials are irreducible (a vague but “true” statement!)

Proposition 1.12 (Factor/Remainder Theorem). *\mathbb{F} a field, $\alpha \in \mathbb{F}[x]$, $f(\alpha) = 0$
Then $\exists g \in \mathbb{F}[x]$ st $f = qg$ with $q = [x - \alpha]$*

Proof. $\exists q, r \in \mathbb{F}[x]$ st $f = q[x - \alpha] + r$ and $\deg r < \deg(x - \alpha) = 1$. Therefore r is a constant. So $0 = f(\alpha) = g(\alpha)[\alpha - \alpha] + r = 0 + r$ i.e., $r = 0$ and so $f = g[x - \alpha]$. ■

Proposition 1.13. *\mathbb{F} a field, $f \in \mathbb{F}[x]$ an irreducible polynomial.*

Then $\exists K$ a field with $F \leq K$ (subfield) such that there is $\alpha \in K$ with $f(\alpha) = 0$.

Moreover, we can arrange that $\dim_{\mathbb{F}} K = n$ where n is the degree of f (finite). For instance, \mathbb{C} is a 2D vector space over \mathbb{R} .

Proof. Forget x , and change the name of the variable to y . Let $\hat{f} = \sum_{i=0}^n a_i y^i$ where $f = \sum_{i=0}^n a_i x^i$.

\hat{f} is irreducible in $\mathbb{F}[y]$ so (\hat{f}) is a maximal ideal of $\mathbb{F}[y]$.

Let $K = \mathbb{F}[y]/(\hat{f})$ so K a field. The elements of K are of the form $h + (\hat{f})$ where $h \in \mathbb{F}[y]$.

Note that $h = q\hat{f} + r$ for $q, r \in \mathbb{F}[y]$ and $\deg r < \deg \hat{f} = n$ so $h + (\hat{f}) = r + q\hat{f} + (\hat{f}) = r + (\hat{f})$.

Thus any element of K is of the form $h + (\hat{f})$ where $h \in \mathbb{F}[y]$ with $\deg h < n$. Suppose that $h_1, h_2 \in \mathbb{F}[y]$ and $\deg h_1, \deg h_2 < n$ with $h_1 + (\hat{f}) = h_2 + (\hat{f})$. Then $h_1 - h_2 \in (\hat{f})$ but $\deg(h_1 - h_2) < n = \deg \hat{f}$ so $h_1 - h_2 = 0$ i.e., $h_1 = h_2$.

Thus our representation is unique, and elements of K can be uniquely described as $h + (\hat{f})$ where $\deg h < n$.

⁶It is helpful to observe that if $f, g \in \mathbb{F}[x]$ with $g \neq 0$ then (by induction) $\exists q, r \in \mathbb{F}[x]$ st $f = qg + r$ with $\deg r < \deg g$.

Note that $\{c + (\hat{f}) \mid \deg c \leq 0\}$ is a copy of \mathbb{F} (with decoration). Identifying the “old \mathbb{F} ” with this “new \mathbb{F} ” we can think of K as an overfield of \mathbb{F} .

Let $\alpha = y + (\hat{f}) \in K$. $f = \sum_{i=0}^n a_i x^i$. So

$$\begin{aligned} f(\alpha) &= \sum_{i=0}^n a_i [y + (\hat{f})]^i = \sum_{i=0}^n “a_i” [y^i + (\hat{f})] \\ &= \sum_{i=0}^n [a_i + (\hat{f})][y^i + (\hat{f})] = \sum_{i=0}^n a_i y^i + (\hat{f}) \\ &= \hat{f} + (\hat{f}) = (\hat{f}) = 0 + (\hat{f}) \\ &= 0_K \end{aligned}$$

Now $1 + (\hat{f}), y + (\hat{f}), y^2 + (\hat{f}), \dots, y^{n-1} + (\hat{f})$ is a basis for K viewed as a vector space over \mathbb{F} . These clearly span K as an \mathbb{F} -vector space, and linear independence follows from uniqueness of expression. Therefore, $\dim_{\mathbb{F}} K = n$. ■

1.12 Field Extensions

Suppose $K \leq L$ (subfield) for K, L fields. Then L is naturally a vector space over K . Let $|L : K| = \dim_K L$ the *degree* of the extension. Observe that $|L : K| = 1$ iff $K = L$.

Proposition 1.14. *Suppose that K, L, M are fields with $K \leq L \leq M$. Then*

$$|M : K| = |M : L| \cdot |L : K|$$

Proof. Let $a_i, i \in I$ be a K -basis of L , and $b_j, j \in J$ an L -basis of M . It is claimed that

$$a_i b_j, (i, j) \in I \times J$$

is a K -basis of M :

Suppose $m \in M, m = \sum'_{j \in J} \lambda_j b_j$ for suitable $\lambda_j \in L$.

Then $\lambda_j = \sum'_{i \in I} k_{ji} a_i$ for suitable $k_{ji} \in K$.

Thus $m = \sum_{(i,j) \in I \times J} k_{ji} a_i b_j$ which establishes spanning.

Next we address linear independence.

Suppose that

$$\exists \theta_{ij} \in K \text{ st } \sum_{(i,j) \in I \times J} \theta_{ij} a_i b_j = 0$$

Then

$$\sum'_{j \in J} \left(\sum'_{i \in I} \theta_{ij} a_i \right) b_j = 0$$

But the b_j are LI over L so $\sum'_{i \in I} \theta_{ij} a_i = 0 \forall j$. As the a_i are in turn LI over K , $\theta_{ij} = 0 \forall i \forall j$. ■

Corollary 1.15. *If K is a subfield of L and $|L : K| = p$ a prime number and M is an intermediate field $K \leq M \leq L$ then $M = K$ or $M = L$.*

1.13 Characteristic of a field

If K is any field, define a map $\theta : \mathbb{Z} \rightarrow K$ by

$$\begin{aligned} 0 &\mapsto 0_K \\ n &\mapsto \sum_{i=1}^n 1_K \text{ for } n \in \mathbb{N} \\ n &\mapsto (-n)\theta = \sum_{i=1}^{|n|} (-1_K) \text{ for } -n \in \mathbb{N} \end{aligned}$$

This is a ring homomorphism. $\text{Im } \theta$ is a subring of K and so is an integral domain. Hence $\text{Ker } \theta$ is a prime ideal of \mathbb{Z} , i.e., (0) or (p) for p a prime.

If $\text{Ker } \theta = (0)$ then $\text{Im } \theta \simeq \mathbb{Z}$ (isomorphic) and we describe K as having *characteristic 0*. Examples include $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Else $\text{Ker } \theta = (p)$ and $\text{Im } \theta \simeq \mathbb{Z}/(p) = \mathbb{Z}_p$ from the first isomorphism theorem. K is said to have *characteristic p* .

Observation If $|K|$ is finite, then K cannot contain a copy of \mathbb{Z} , so $\text{char } K$ is p for some prime number p . Let $T = \text{Im } \theta$, so $T \leq K$ and $|T| = p$. Further, let $|K : T| = n < \infty$. By choosing a basis v_1, \dots, v_n of K as a vector space over T , every element of K is uniquely expressible as $\sum_{i=1}^n t_i v_i$ for $t_i \in T$. Therefore we have proved:

Proposition 1.16. *If K is a finite field, then $\exists p$ a prime and $n \in \mathbb{N}$ such that $|K| = p^n$*

Fact: (asserted without proof) $\forall n \forall p, \exists$ a field of size p^n and any such two are isomorphic.

Example. $L = \mathbb{Z}_2, f = x^2 + x + 1 \in L[x]$
 f has no roots in L so does not factor in $L[x]$ except trivially; so f is irreducible. As (f) is then a maximal ideal, $K = L[x]/(f)$ is a field. The elements are

$$0 + (f) := \text{“0”}, 1 + (f) := \text{“1”}, x + (f) := \text{“}\alpha\text{”}, 1 + x + (f) := \text{“}1 + \alpha\text{”}$$

Multiplication in K: Consider

$$\begin{aligned}\alpha^2 &= x^2 + (f) \\ &= \underbrace{x^2 + x + 1}_{\text{in } (f)} + x + 1 + (f) \text{ since } x + x = 0 = 1 + 1. \\ &= x + 1 + (f)\end{aligned}$$

Thus $\alpha^2 = \alpha + 1$. The full multiplication table is

\times	0	1	α	$\alpha + 1$
0	0	0	0	0
1	0	1	α	$\alpha + 1$
α	0	α	$\alpha + 1$	1
$\alpha + 1$	0	$\alpha + 1$	1	α

So we have a finite group of size $2^2 = 4$.

1.14 More on Irreducibles

Proposition 1.17. *If R is a PID then every $r \in R$ which is not in U_R and is not zero can be factorised into irreducibles*

$$r = \pi_1 \cdot \pi_2 \cdots \pi_n$$

and if $\pi_1' \cdot \pi_2' \cdots \pi_k'$ is a rival factorisation into irreducibles then $k = n$ and $\exists \sigma \in \text{Sym}(n)$ such that π_i and $\pi_{i\sigma}'$ are associates i.e., $(\pi_i) = (\pi_{i\sigma}')$.

Observation: This ensures a PID is a UFD.

Proof. (Existence) Suppose for contradiction that such an r exists which cannot be factored into irreducibles. So $r = r_0 = ab$ where $a, b \notin U_R$ since r not irreducible (else it factors to itself). At least one, wlog a , of these elements cannot be factored into irreducibles. Let $r_1 = a$. So $r_0 \in (r_1)$ so $(r_0) \subseteq (r_1)$ but $(r_0) \neq (r_1)$ ⁷.

Now r_1 has all the defining attributes of r_0 , so we may inductively construct

$$(r) \subsetneq (r_1) \subsetneq (r_2) \subsetneq \dots$$

with every $r_i \neq 0$, $r_i \notin U_R$ and not factorable into irreducibles.

Let

$$I = \bigcup_{i \in \mathbb{N}} (r_i) \trianglelefteq R$$

as the union of an ascending chain of ideals is an ideal. Since R a PID, there is some $s \in R$ such that $I = (s)$. Hence for some i , $s \in (r_i)$. But then

$$I = (s) \subseteq (r_i) \subsetneq (r_{i+1}) \subseteq I$$

⁷as if $r_1 \in (r)$ then it follows that $b \in U_R$, a contradiction.

which is a contradiction as desired.

(Uniqueness) Suppose that r has rival irreducible factorisations

$$r = \pi_1 \cdots \pi_n = \pi_1' \cdots \pi_k'$$

$\therefore \pi_1' \cdots \pi_k' = r \in (\pi_1)$ a prime ideal of R since π_1 irreducible. By a finite induction on the defining property of prime ideals, we deduce $\pi_i' \in (\pi_1)$ for some i .

So $\pi_i' = s\pi_1$ for some $s \in R$. As π_i' irreducible and π_1 not a unit, $s \in U_R$. Relabelling if necessary to set $i = 1$ yields

$$\pi_1 \cdots \pi_n = \pi_1' \cdot \pi_2' \cdots \pi_k' = s\pi_1 \cdot \pi_2' \cdots \pi_k'$$

As we are in an integral domain we can cancel⁸ the non-zero π_1 and let “new π_2' ” be $s \cdot$ “old π_2' ”

$$\therefore \pi_2 \cdots \pi_n = \pi_2' \cdots \pi_k'$$

Inductively $1 = \pi_{n+1}' \cdots \pi_k'$ so, as the π_i' are not units, $n - k = 0$ i.e., $n = k$ and each π_i is an associate of a π_i' , up to multiplication by a unit. ■

1.15 Minimal Polynomials

Let K be a subfield of \mathbb{C} , such as \mathbb{Q} . Suppose that $\zeta \in \mathbb{C}$. Define a map

$$\epsilon_\zeta : K[x] \rightarrow \mathbb{C}$$

$$\sum_i' a_i x^i \mapsto \sum_i' a_i \zeta^i \text{ “evaluation at } \zeta \text{”}$$

As ϵ_ζ is a ring homomorphism, the image is a subring of \mathbb{C} . Thus it is an integral domain (as any 0 divisor would also be such in \mathbb{C} , itself an ID). Call the image $K[\zeta]$.

$\text{Ker } \epsilon_\zeta = (m_\zeta)$ is a prime ideal; it is either (0) or (m_ζ) for m_ζ an irreducible (in $K[x]$) polynomial. Now $m_\zeta(\zeta) = 0$ since $m_\zeta \in \text{Ker } \epsilon_\zeta$, moreover if $f \in K[x]$ with $f(\zeta) = 0$ then $f \in \text{Ker } \epsilon_\zeta$ so $f \in (m_\zeta)$ i.e., $m_\zeta | f$ in $K[x]$. Also if $m_\zeta | f$ in $K[x]$ then $f(\zeta) = 0$. Wlog we may assume m_ζ is monic, in which case it is called the *minimum polynomial of ζ over K* . It is the unique monic polynomial of smallest degree which has ζ as a root.

We have a dichotomy:

Ker $\epsilon_\zeta = (0)$ Then $\nexists f \in K[x] \setminus \{0\}$ such that $f(\zeta) = 0$.

Then ϵ_ζ is a monomorphism (that is, injective) $K[x] \rightarrow \mathbb{C}$ which, by pruning the codomain, establishes an isomorphism $K[x] \simeq K[\zeta] = \text{Im } \epsilon_\zeta$.

Example. π, e have $\text{Ker } \epsilon_\pi = (0) = \text{Ker } \epsilon_e$ when $K = \mathbb{Q}$ (results due to Lindemann, Hermite respectively.)

Jargon: We say ζ is *transcendental over K* . If you omit the field, it is implicity \mathbb{Q} . So π, e are transcendental numbers.

⁸ $ab = ac, a \neq 0 \Rightarrow a(b - c) = 0 \Rightarrow b - c = 0$ as an ID $\Rightarrow b = c$.

Ker $\epsilon_\zeta = (m_\zeta)$ Then

$$K[\zeta] = \text{Im } \epsilon_\zeta = K[x]/(m_\zeta)$$

$$f + (m_\zeta \mapsto f(\zeta)) \forall f \in K[x]$$

$K[\zeta]$ is then miraculously a field (since we have factored a ring by a maximal ideal), even though it doesn't seem to be one. We say ζ is *algebraic over* K (again, implicitly \mathbb{Q} if not otherwise specified).

Example. $1, i, \sqrt{2}, \sqrt{2}/39$ are all algebraic.

Example. When $K = \mathbb{R}$,

$$\mathbb{R}[i] = \left\{ \sum_{j=0}^{\infty} a_j i^j \mid a_j \in \mathbb{R} \forall j \right\} = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{C}$$

Definition. \mathbb{A} is the set of complex numbers which are algebraic over \mathbb{Q} , *the algebraic numbers*. This is a countable set, since $\mathbb{Q}[x]$ is countable.

Proposition 1.18. $K \leq \mathbb{C}, \alpha \in \mathbb{C}$

α algebraic over $K \Leftrightarrow |K(\alpha) : K| < \infty$ for $K(\alpha)$ the smallest subfield of \mathbb{C} containing K and α .

Proof. If α algebraic over K then it has a min.poly. m_α and $K[\alpha]$ is a field, specifically the set of complex numbers of the form

$$a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \quad a_i \in K \quad n = \deg m_\alpha$$

and each number is uniquely expressed via isomorphism $K[\alpha] \simeq K[y]/(\hat{m}_\alpha)$ for \hat{m}_α " m_α in y ". Thus $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ form a K -basis of the vector space $K[\alpha] = K(\alpha)$. Therefore

$$|K(\alpha) : K| = |K[\alpha] : K| = n = \deg m_\alpha < \infty$$

Conversely, if $|K(\alpha) : K| = n < \infty$ then $1, \alpha, \dots, \alpha^n$ is a list of length $n + 1$ and so cannot be linearly independent over K ; thus it is linearly dependent. Hence there are K_i not all zero such that $\sum_{i=0}^n K_i \alpha^i = 0$; α is therefore a root of $\sum_{i=0}^n K_i x^i = 0 \in K[x]$ so is algebraic over K . ■

Proposition 1.19. $K \leq \mathbb{C}$

$$L := \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraic over } K\}$$

is a field!

Proof. Suppose $\lambda_1, \lambda_2 \in L$, so $|K(\lambda_1) : K| < \infty$. Now λ_2 satisfies a nonzero polynomial $f \in K[x]$ and so $f \in K(\lambda_1)[x]$.

$$\therefore |K(\lambda_1)(\lambda_2) : K(\lambda_1)| < \infty$$

$$\therefore |K(\lambda_1)(\lambda_2) : K| < \infty \text{ (product)}$$

\therefore all elements of $K(\lambda_1)(\lambda_2)$ are algebraic over K . So $\lambda_1 \pm \lambda_2, \lambda_1 \lambda_2, \lambda_1/\lambda_2$ for $\lambda_2 \neq 0$ are all algebraic over K , i.e., elements of L . ■

Corollary 1.20. \mathbb{A} is a field.

Observe that if $f \in \mathbb{A}[x] \setminus \{0\}$, $f = \sum_{i=0}^n a_i x^i$ and $\alpha \in \mathbb{C}$ is a root of f , then $\alpha \in \mathbb{A}$. This is because if $K = \mathbb{Q}(a_0, \dots, a_n)$ then $|K : \mathbb{Q}| < \infty$ since $|\mathbb{Q}(a_0, \dots, a_i) : \mathbb{Q}(a_0, \dots, a_{i-1})| < \infty \forall i$. Also $|K(\alpha) : K| < \infty$, so $|K(\alpha) : \mathbb{Q}| < \infty$. But $\alpha \in K(\alpha)$ so α is algebraic. When doing Galois Theory, we often work with $\mathbb{Q} \leq K \leq \mathbb{C}$ with $|K : \mathbb{Q}| < \infty$ so $K \leq \mathbb{A}$.

1.15.1 Algebraic Integers

Definition. $\alpha \in \mathbb{C}$ is an *algebraic integer* if α is a root of a monic polynomial of integer coefficients.

Facts

- The algebraic integers are often called \mathcal{O} .
- \mathcal{O} is a ring.
- $\sqrt{2}, i, -7 \in \mathcal{O}$.
- If $\alpha \in \mathbb{C}$ a root of $f = x^n + \sum_{i=0}^{n-1} a_i x^i$ with $a_i \in \mathcal{O} \forall i$ then $\alpha \in \mathcal{O}$.
- $\mathbb{Q} \cap \mathcal{O} = \mathbb{Z}$.
- The study of \mathcal{O} and \mathbb{A} is *algebraic number theory*.
- If $K \leq \mathbb{C}$ then $K \cap \mathcal{O}$ is called \mathcal{O}_K and is a subring of K . In this context, “ \mathbb{Z} is to \mathbb{Q} ” as “ \mathcal{O}_K is to K ”, especially when $K \leq \mathbb{A}$.

Example. $K = \mathbb{Q}(i) = \mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ then $\mathcal{O}_K = \mathbb{G}$.

Example. $K = \mathbb{Q}(\sqrt{5})$ so $|K : \mathbb{Q}| = 2$; let $\lambda = \frac{1+\sqrt{5}}{2}$. Then λ satisfies $\lambda^2 - \lambda - 1 = 0$ so $\lambda \in \mathcal{O}_K$ despite the half! In fact $\mathcal{O}_K = \{a + b\lambda \mid a, b \in \mathbb{Z}\}$.

1.16 A few more prosaic details

Definition. $f \in \mathbb{Z}[x]$, $f \neq 0$, $f = \sum_{i=0}^n a_i x^i$

We say f is *primitive* if $\gcd\{a_0, a_1, \dots, a_n\} = 1$.

In general we write $c(f) = \gcd\{a_0, a_1, \dots, a_n\}$ for the *content* of f .

Observation: If $f \in \mathbb{Z}[x]$ is nonzero, then $f = c(f)\hat{f}$ with $\hat{f} \in \mathbb{Z}[x]$ primitive.

Proposition 1.21. If $f, h \in \mathbb{Z}[x]$ are primitive polynomials, then fh is primitive.

Proof. Suppose that $c(fh) \neq 1$ so $\exists p$ prime with $p < c(fh)$. Let

$$\pi : \mathbb{Z} \rightarrow \mathbb{Z}/(p) = \mathbb{Z}_p$$

$$z \mapsto z + (p) = [z]_p$$

Note that π a ring epimorphism and \mathbb{Z}_p a field. π induces

$$\hat{\pi} : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$$

$$\sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n (a_i) \pi x^i$$

which is also an epimorphism of rings.

Now $(fh)\hat{\pi} = 0$ but $\hat{\pi}$ a ring homomorphism so $(f)\hat{\pi} \cdot (h)\hat{\pi} = 0$. As $\mathbb{Z}_p[x]$ is an ID, $(f)\hat{\pi} = 0$ or $(h)\hat{\pi} = 0$ so $p|c(f) = 1$ or $p|c(h) = 1$ which is a contradiction. Thus $c(fh) = 1$. ■

Note that standard forms now multiply nicely: $f, h \in \mathbb{Z}[x], f = c(f)f_1, h = c(h)h_1$ for f_1, h_1 primitive then $fh = c(f)c(h)f_1h_1$ where f_1h_1 is primitive, so content is multiplicative ($c(fh) = c(f)c(h)$)!

In summary: if $f \in \mathbb{Z}[x], f \neq 0$ then $f = c(f)\hat{f}$ for \hat{f} primitive, and this decomposition is unique.

Proposition 1.22 (Gauss). *Suppose $0 \neq f \in \mathbb{Z}[x]$ and $f = hk$ for $h, k \in \mathbb{Q}[x]$. Then $\exists q \in \mathbb{Q} \setminus \{0\}$ st $qh, q^{-1}k \in \mathbb{Z}[x]$.*

Example.

$$x^2 - 1 = \left(\frac{x}{2} - \frac{1}{2}\right)(2x + 2) = (x - 1)(x + 1)$$

Proof. Choose $r, s \in \mathbb{N}$ st $rh, sk \in \mathbb{Z}[x]$.

Then $rh = c(rh)r\hat{h}$ and $sk = c(sk)s\hat{k}$ where $\hat{}$ denotes primitive.

Note that

$$r\hat{h} = \frac{r}{c(rh)}h, \hat{s}k = \frac{s}{c(sk)}k$$

Now

$$rsf = rshk = c(rh)c(sk)r\hat{h}s\hat{k}$$

$\therefore rsc(f)\hat{f} = zr\hat{h}s\hat{k}$ where $z \in \mathbb{Z}$. So $rs|z$. Hence

$$\begin{aligned} f &= c(f)\hat{f} \\ &= (z'r\hat{h})(s\hat{k}) \text{ where } 0 < z' = \frac{z}{rs} \in \mathbb{Z} \\ &= (uh) \cdot (vk) \text{ } u, v \in \mathbb{Q} \setminus \{0\} \end{aligned}$$

Where $uh = z'r\hat{h}, vk = s\hat{k}$.

Now $f = hk = uhvk = vhwk$ so let $q = u \in \mathbb{Q}, v = q^{-1}$. ■

Proposition 1.23 (Eisenstein's Criterion). Suppose that $f = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$, and that there is a prime number p such that

$$p \nmid a_0, p \mid a_i \forall i > 0, p^2 \nmid a_n$$

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

Proof. As before, $\pi : \mathbb{Z} \rightarrow \mathbb{Z}_p$ the natural epimorphism induces epimorphism $\hat{\pi} : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$. Now it suffices to show that if $f = hk$ with (Gauss) $h, k \in \mathbb{Z}[x]$ then either h or k has the same degree as f .

Now given such h, k ; $(f)\hat{\pi} = (h)\hat{\pi} \cdot (k)\hat{\pi}$ But $(f)\hat{\pi} \in \mathbb{Z}_p \setminus \{0\}$ so

$$\deg((h)\hat{\pi}), \deg((k)\hat{\pi}) = 0$$

$\therefore h = h_0 + px\bar{h}$ where $\bar{h} = \sum_i' h_i x^i \in \mathbb{Z}[x]$. Similarly $k = k_0 + px\bar{k}$, $\bar{k} \in \mathbb{Z}[x]$.

Therefore $hk = h_0 k_0 + px(\bar{h}k_0 + \bar{k}h_0) + p^2 x^2 \bar{h}\bar{k}$. We may assume for contradiction that $\deg h, \deg k \geq 1$. But then the coefficient of highest power of x is a multiple of p^2 , which is just such a contradiction. ■

Example.

$$2 + 9x^6 - 6x^7 + 3x^8 \in \mathbb{Q}[x]$$

is irreducible using $p = 3$.

Eisenstein backwards: If $f = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ with $a_n \neq 0 \neq a_0$, let

$$l = x^n f(1/x) = \sum_{i=0}^n a_{n-i} x^i$$

Now $x^n l(1/x) = f(x)$. Suppose $h, k \in \mathbb{Z}[x]$ of degrees n_1, n_2 resp. st $f = hk$ so $n_1 + n_2 = n$. Then

$$\begin{aligned} x^n f(1/x) &= x^n h(1/x)k(1/x) \\ &= x^{n_1} h(1/x)x^{n_2} k(1/x) \end{aligned}$$

Thus f is irreducible iff $x^n f(1/x)$ is irreducible in $\mathbb{Q}[x]$.

Corollary 1.24. $f = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ is irreducible if

$$p \nmid a_n, p \mid a_i \forall i < n, p^2 \nmid a_0$$

(This is also referred to as Eisenstein's criterion).

Observation: $f \in \mathbb{Q}[x]$ is irreducible iff $f(ax + b)$ is irreducible for $a, b \in \mathbb{Q}$, $a \neq 0$. In particular, f is irreducible iff $f(x + c)$ is irreducible for $c \in \mathbb{Z}$.

Example. p prime, $f = x^{p-1} + x^{p-2} + \dots + x + 1 \in \mathbb{Q}[x]$ is irreducible:

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = 1 \cdot x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \dots + \binom{p}{p-1}$$

But for $1 \leq i \leq p-1$,

$$\binom{p}{i} = \frac{p(p-1)(p-2)\cdots(p-i+1)}{i(i-1)\cdots 2 \cdot 1} \in \mathbb{N}$$

so the denominator cancels somehow, clearly not with p , so $p \mid \binom{p}{i}$. By Eisenstein's criterion, $f(x+1) \in \mathbb{Q}[x]$ is irreducible, hence $f = f(x) \in \mathbb{Q}[x]$ is irreducible ■

2 Galois Theory

2.1 Preliminaries

Suppose that K, L are fields with $K \leq L$.

Definition. For R a ring, an *automorphism* is an isomorphism from R to R .

Definition. The *Galois group* of this extension is

$$\text{Gal}_K L := \{g \mid g : L \rightarrow L \text{ is an automorphism of fields, } (k)g = k \forall k \in K\}$$

This is a group under composition of maps.

Definition. If $f \in K[x]$ then a field Σ_f st $K \leq \Sigma_f$, f factorises into linear polynomials in $\Sigma_f[x]$ and $\Sigma_f = K(\alpha_1, \dots, \alpha_n)$ for $\alpha_1, \dots, \alpha_n$ the roots of f in Σ_f is known as a *splitting field* for f .

Example. Calculate $\text{Gal}_{\mathbb{Q}} \Sigma_f$ where $f = x^2 + 1$.

Claim: $\mathbb{Q}(i) = \mathbb{Q}[i] \leq \mathbb{C}$ will do for Σ_f .

Certainly $x^2 + 1 = [x - i][x + i]$ is a factorisation of f in $\mathbb{Q}(i)[x]$; moreover $\mathbb{Q}(i, -i) = \mathbb{Q}(i)$ so $\mathbb{Q}(i)$ is a splitting field for f .

Suppose that $g \in \text{Gal}_{\mathbb{Q}} \mathbb{Q}(i)$. $\therefore (q)g = q \forall q \in \mathbb{Q}$. Also $i^2 + 1 = 0$.

So $(i^2 + 1)g = (0)g = 0 \Rightarrow (i)g^2 + 1 = 0 \Rightarrow (i)g = \pm i$.

Now if $(i)g = i$ then $(a + bi)g = a + bi \forall a, b \in \mathbb{Q}$ but $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ so $g = id_{\mathbb{Q}(i)}$.

If instead $(i)g = -i$ then $(a + bi)g = a - bi$ so g is complex conjugation, a well-known automorphism of \mathbb{C} which restricts to an automorphism of $\mathbb{Q}(i)$, called c .

Thus $\text{Gal}_{\mathbb{Q}} \mathbb{Q}(i) = \{id, c\}$ a cyclic group of order 2.

Example. $K = \mathbb{Q}, f = x^3 - 2$

Here we may take $\Sigma_f = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega = e^{2\pi i/3}$, because $\mathbb{Q}(\sqrt[3]{2}, \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

$|\Sigma_f : \mathbb{Q}| = |\Sigma_f : \mathbb{Q}(\sqrt[3]{2})| \cdot |\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}|$.

Now $x^3 - 2$ is irreducible over \mathbb{Q} (Eisenstein, $p = 2$) and has $\sqrt[3]{2}$ as a root so $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}] \simeq \mathbb{Q}[x]/(x^3 - 2)$ and hence $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$.

Also $\mathbb{Q}(\sqrt[3]{2}) \leq \mathbb{R}$ but $\omega \notin \mathbb{R}$ so $|\Sigma_f : \mathbb{Q}(\sqrt[3]{2})| \neq 1$.

However, $\omega^3 = 1$ so $(\omega - 1)(\omega^2 + \omega + 1) = 0$; as $\omega \neq 1$, ω is a root of $x^2 + x + 1$.

Therefore, if m_ω denotes the minimum polynomial of ω in $\mathbb{Q}(\sqrt[3]{2})[x]$ then $m_\omega | x^2 + x + 1$ in $\mathbb{Q}(\sqrt[3]{2})[x]$ and as $\deg m_\omega \neq 1$ it must be that $\deg m_\omega = 2$ and $m_\omega = x^2 + x + 1$. Thus $|\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})| = 2$.

Therefore

$$|\Sigma_f : \mathbb{Q}| = 6$$

Some elements of $\text{Gal}_{\mathbb{Q}} \Sigma_f$:

$$id : \Sigma_f \rightarrow \Sigma_f$$

complex conjugation c will induce an automorphism $\Sigma_f \rightarrow \Sigma_f$ fixing each $q \in \mathbb{Q}$

Claim: $x^3 - 2$ is irreducible over $\mathbb{Q}(\omega)$ i.e., in $\mathbb{Q}(\omega)[x]$

This is because if it factorised then either $\sqrt[3]{2}, \omega\sqrt[3]{2}$ or $\omega^2\sqrt[3]{2} \in \mathbb{Q}(\omega)$ but then $\sqrt[3]{2} \in \mathbb{Q}$. But $\omega \notin \mathbb{Q}$ so $|\mathbb{Q}(\omega) : \mathbb{Q}| = 2$ by $\omega^2 + \omega + 1 = 0$.

If $\sqrt[3]{2} \in \mathbb{Q}(\omega)$ then $2 = |\mathbb{Q}(\omega) : \mathbb{Q}(\sqrt[3]{2})| \underbrace{|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}|}_3$ i.e. $3|2$ in \mathbb{Z} which is a contradiction. Thus

the claim is established.

Now, $x^3 - 2$ factorises into linears in $\mathbb{Q}(\omega, \sqrt[3]{2})$ and we discovered $\sqrt[3]{2} \notin \mathbb{Q}(\omega)$. We seek more automorphisms of Σ_f which fix \mathbb{Q} .

Let $L = \mathbb{Q}(\omega)$, so $x^3 - 2 \in L[x]$ is irreducible. Let $\alpha, \beta \in \Sigma_f$ be roots of f . By the 1st isomorphism theorem we have

$$L(\alpha) = L[\alpha] \simeq L[x]/(f)$$

$$\sum a_i \alpha^i \leftarrow \sum_{i=0}^{(\deg f)-1} a_i x^i + (f) \rightarrow \sum a_i \beta^i$$

“themselves” \leftarrow constants of $L \rightarrow$ “themselves”

So $L[x]/(f) \simeq L[\beta] = L(\beta)$. Therefore we have an isomorphism of fields $\theta : L(\alpha) \rightarrow L(\beta)$ which is the identity map on $L \supseteq \mathbb{Q}$ and $(\alpha)\theta = \beta$.

Now $L \subseteq L(\alpha) \leq \Sigma_f$ but $|\Sigma_f : L| \underbrace{|L : \mathbb{Q}|}_2 = 6 \therefore |\Sigma_f : L| = 3$.

As $|L(\alpha) : L| \neq 1$ and $|L(\alpha) : L| |3|$, it must be that $|L(\alpha) : L| = 3$. Hence $|\Sigma_f : L(\alpha)| = 1$ so $\Sigma_f = L(\alpha)$ and by the same logic also equals $L(\beta)$. Hence θ is actually an automorphism i.e.

$$\theta \in \text{Gal}_{\mathbb{Q}} \Sigma_f$$

Let

$$\theta_1 : \sqrt[3]{2} \rightarrow \omega\sqrt[3]{2} \text{ and fixes } L$$

$$\theta_2 : \sqrt[3]{2} \rightarrow \omega^2\sqrt[3]{2} \text{ and fixes } L$$

then θ_1, θ_2 are elements of $\text{Gal}_{\mathbb{Q}} \Sigma_f$. Notice

$$\theta_2 = \theta_1^{-1}$$

$$\theta_1^3 = \theta_2^3 = \text{id}_{\Sigma_f}$$

If $g \in \text{Gal}_{\mathbb{Q}} \Sigma_f$ then g is determined by its action on $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$ and it must permute them since if $\alpha \in \Sigma_f$ is a root of f then

$$\begin{aligned} \alpha^3 - 2 &= 0 \\ \therefore (\alpha^3 - 2)g &= (0)g \\ \therefore ((\alpha)g)^3 - 2 &= 0 \\ \therefore g &\text{ is a root of } f \text{ in } \Sigma_f \end{aligned}$$

and further as an isomorphism the map on roots is injective and hence bijective i.e., a permutation.

$$\therefore \text{Gal}_{\mathbb{Q}} \Sigma_f \leq \text{Sym}(3) \text{ (subgroup)}$$

via this view of $Gal_{\mathbb{Q}}\Sigma_f$ as a permutation group on the three roots.

So $|Gal_{\mathbb{Q}}\Sigma_f|$ divides 6 but has at least 4 elements $id, c, \theta_1, \theta_2$ and hence must have 6 elements; that is

$$Gal_{\mathbb{Q}}\Sigma_f = \{id, c, \theta_1, \theta_2, \psi, \phi\} \simeq Sym(3)$$

where

$$\psi : \sqrt[3]{2} \leftrightarrow \omega^2 \sqrt[3]{2} \text{ fixing } \omega \sqrt[3]{2}$$

$$\phi : \sqrt[3]{2} \leftrightarrow \omega \sqrt[3]{2} \text{ fixing } \omega^2 \sqrt[3]{2}$$

2.2 Most celebrated application

Consider $f \in \mathbb{Q}[x]$. Under what circumstances can the roots of f in \mathbb{C} be expressed in terms of the coefficients using $+, -, \times, \div, \sqrt[m]{} \in \mathbb{N}$?

- $ax + b, a \neq 0$ has root $-\frac{b}{a}$.
- $ax^2 + bx + c, a \neq 0$ has roots $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.
- There are similar, more complicated, formulae for cubics and quartics.
- For quintics (and beyond) there is no general formula.

The answer to this question (Galois)

From f build Σ_f , let $G = Gal_{\mathbb{Q}}\Sigma_f$. Then f is “solvable by radicals” iff G is a “solvable⁹ group” i.e., there exist subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G$$

with each G_{i+1}/G_i abelian.

2.3 Technicalities

Suppose that $k \leq K$ is a field extension and $|K : k| < \infty$.

If $\text{char } K = 0$ (so $\text{char } k = 0$) or if K is a finite field then $\exists t \in K$ such that $K = k(t) = k[t]$ (An extension made by adjoining a single element is called a *simple* extension).

Proof. Omitted ■

⁹“soluble” in the UK

If $\text{char } k = 0$ or k is infinite and $f \in k[x]$ is irreducible then if K is an extension field of k and $\alpha \in K$ then α is not a repeated root of f i.e.

$$[x - \alpha]^2 \nmid f \text{ in } K[x]$$

Non-example. \mathbb{F}_p the field with p elements. Form $\mathbb{F}_p[t]$ an integral domain and then $k = \mathbb{F}_p(t)$ the field of fractions of $\mathbb{F}_p[t]$. Work in $k[x]$ and let $f = x^p - t \in k[x]$. A little work shows that $f \in k[x]$ is irreducible. Choose any K st $k \leq K$ and $\alpha \in K$ is a root of f . Then

$$[x - \alpha]^p = x^p - \alpha^p = x^p - t = f$$

Proof. Define a map

$$D : K[x] \rightarrow K[x]$$

$$f \mapsto f' \text{ (differentiation)} \quad \forall f \in K[x]$$

D is a K -linear map and satisfies the product rule. If f is irreducible and $[x - \alpha]^2 \mid f$ then $[x - \alpha] \mid f, f' = D(f)$ But if $f' \neq 0$ this is absurd because $(f, f') = (1)$ by irreducibility of f , as $\deg f' < \deg f$ so $f' \notin (f)$ and (f) is maximal and then $1 = \lambda f + \mu f'$ $\lambda, \mu \in K[x]$ and therefore in particular $1 = \lambda(\alpha)f(\alpha) + \mu(\alpha)f'(\alpha) = 0$ which is madness.

So $f' = 0$ and therefore f is a constant. But f is irreducible, so we have a contradiction.

This contradiction did not arise in the non-example as polynomials could differentiate to 0 modulo p . ■

From now on, we assume characteristic 0.

Definition. $k \leq K$ is a *finite (a) normal (b) extension* if:

- (a) $|K : k| < \infty$
- (b) If $f \in k[x]$ is irreducible and $\alpha \in K$ is a root of f then f factorises into linear polynomials in $K[x]$ ¹⁰

Theorem 2.1 (A Big Theorem!). *For $k \leq K$ a field extension, TFAE*

- $\exists f \in k[x]$ such that K is a splitting field for f .
- The extension is finite and normal.

¹⁰Ian Stewart calls this the 'trade union principle'- one out, all out!

2.4 Fundamental Theorem of Galois Theory

$k \leq K$ a field extension which is finite and normal, $G = \text{Gal}_k K$. If $H \leq G$ (subgroup), let

$$H^\dagger = \{x \mid x \in K, (x)h = x \forall h \in H\}$$

so $H^\dagger \leq K$ is a subfield st $k \leq H^\dagger \leq K$. Also if $k \leq M \leq K$, let

$$M^\star = \text{Gal}_M K \leq G \text{ (subgroup)}$$

Let $n = |K : k|$, then

(a) $|G| = n$

(b) If $H_1 \leq H_2 \leq G$ then $H_2^\dagger \leq H_1^\dagger$

(c) If $k \leq K_1 \leq K_2 \leq K$ then $K_2^\star \leq K_1^\star$

(d) In (b) and (c),

$$|H_2 : H_1| = |H_1^\dagger : H_2^\dagger| \text{ (index of group)}$$

$$|K_2 : K_1| = |K_1^\star : K_2^\star| \text{ (degree of field extension)}$$

(e) \dagger and \star are mutually inverse. Each of them is called *the Galois correspondence*.

(f) If $k \leq M \leq K$ then the extension $M \leq K$ is normal with Galois group M^\star . More interestingly, the extension $k \leq M$ is normal iff M^\star is a normal subgroup of G . In this case

$$\text{Gal}_k M \simeq G/M^\star$$

Define

$$\theta : G \rightarrow \text{Gal}_k M, g \mapsto g|_M$$

and by magic $g|_M \in \text{Gal}_k M$. Then one may show θ is a group epimorphism with kernel M^\star and the 1st isomorphism theorem applies.

Bits and bobs

Proposition 2.2. *If $f \in k[x]$ and Σ_f is a splitting field for f , then $|\Sigma_f : k| \leq n!$ where n is the degree of f .*

Proof. Induct on $\deg f$: if f is linear then $k = \Sigma_f$. Factorise $f = f_1 f_2 \cdots f_t$ (irreducibles; f assumed non-constant). Extend k to $k(\alpha) = k[\alpha]$ where α is a root of f_1 .

Now $|k(\alpha) : k| = \deg f_1 \leq \deg f = n$. Let $K = k(\alpha)$ and factorise f in $K[x]$, $f = (x - \alpha)g_1 \cdots g_s$. Let $f_{\text{new}} = g_1 \cdots g_s$, replace k by K and apply inductive hypothesis. ■

Proposition 2.3. *Under the preceding conditions, there exists a monomorphism $\text{Gal}_k \Sigma_f \rightarrow \text{Sym}(n)$.*

Proof. Let $\alpha_1, \dots, \alpha_u$ be the distinct roots of f in $\Sigma_f = k(\alpha_1, \dots, \alpha_u)$. Let $G = \text{Gal}_k \Sigma_f$ then $(\alpha_i)g$ is a root of f for each i so g respects $\Omega = \{\alpha_1, \dots, \alpha_u\}$. Hence we get a map $\theta : G \rightarrow \text{Sym}(\Omega)$ a group homomorphism by this action, with kernel 1 hence injective; and with $|\Omega| \leq \deg f = n$. ■

A final observation $f \in k[x]$ has a splitting field Σ_f . If h is an irreducible factor of f with roots $\alpha, \beta \in \Sigma_f$ then

$$k[\alpha] \simeq k[x]/(f) \simeq k[\beta]$$

Fact: $\exists g \in \text{Gal}_k \Sigma_f$ which restricts to this isomorphism $k[\alpha] \rightarrow k[\beta]$.