Galois Theory - Week 2 - Group Actions, Rings and Fields

Antonio León Villares

January 2023

Contents

Based on the notes by Tom Leinster, Chapter 2

1 Group Actions

1.1 Group Actions

1.1.1 Definition: Group Action

Let G be a ***group*** *and X be a* ***set****.*
An ***action*** *of G on X is a function:*

$$G \times X \to X$$
$$(g, x) \mapsto gx$$

satisfying:

- $$\forall g, h \in G, \forall x \in X \qquad (gh)x = g(hx)$$
- $$\forall x \in X \qquad 1_G x = x$$

(Definition 2.1.1)

1.1.2 Definition: The (Abstract) Symmetry Group

Let X be a set. The ***symmetry group*** *$Sym(X)$ contains all the* ***bijections****:*

$$X \to X$$

$Sym(X)$ is a ***group*** *under* ***function composition****, and with identity as the* ***identity function****.*
Note, when $X = [1, n]$, this is nothing but the standard symmetry group S_n.

1.1.3 Examples of Group Actions

- $Sym(X)$ is built specifically to act on X:
$$(g, x) \mapsto g(x)$$
- more generally, the group $Aut(X)$ is the group of **automorphisms** of some object X (such as a group!). This acts in a natural way:
$$(g, x) \mapsto g(x)$$
For example, in real, finite dimensional vector spaces:
$$Aut(X) \cong GL(\mathbb{R}; n)$$
the group of real, $n \times n$ invertible matrices. This acts over spaces like $\mathbb{R}^n$ via matrix multiplication.

- G can be the group of 48 **isometries** (rotations + reflections) of a cube. Then, G can act on:
  - the set of 6 faces
  - the set of 12 edges
  - the set of 8 vertices
  - the set of 4 long diagonals (diagonals which connect diammetrically opposed vertices)
- the **trivial action** is the action:

$$gx = x$$

1.1.4 Lemma: Actions Provide Homomorphisms to Symmetry Group

Let G be a group acting on X. Every $g \in G$ gives rise to a function:

$$\bar{g} : X \to X$$

defined by:

$$\bar{g}(x) = gx$$

This induces a homomorphism:

$$\Sigma : G \to Sym(X)$$

defined by:

$$g \mapsto \bar{g}$$

Proof. It is sufficient to show that $\bar{g}$ is a bijection, but this is trivial: $\overline{g^{-1}}$ is clearly an inverse for $\bar{g}$. In particular, this means that $\bar{g} \in Sym(X)$ (since it is a bijective mapping from X to itself). The fact that Σ is a group homomorphism is immediate:

$$\Sigma(gh)(x) = \overline{gh}(x) = (gh)x = g(hx) = \bar{g}(\bar{h}(x)) = \Sigma(g) \circ \Sigma(h)(x)$$

□

1.1.5 Examples of Group Actions Giving Rise to Homomorphisms

- when $Sym(X)$ acts on X, the function $\bar{g}$ will just be g, so $\Sigma : Sym(X) \to Sym(X)$ will be the identity mapping
- if X is a real vector space, $\Sigma : Aut(X) \to Sym(X)$ is an **inclusion**:

$$\Sigma(g) = g$$

  since $Aut(X)$ contains **linear** bijections, whilst $Sym(X)$ contains **all** bijections
- the action of isometries on cube vertices induces the homomorphism $\Sigma : G \to S_{12}$, since there are 12 vertices, and so, $Sym(X) \cong S_{12}$ (we can label each vertex with a number from 1 to 12, and any permutation of vertices corresponds to a permutation of the set of 12 elements)

1.2 Faithful Actions

1.2.1 Definition: Faithful Actions

*G acts on X **faithfully** if:*

$$\forall g, h \in G, \forall x \in X \ : \ gx = hx \implies g = h$$

That is, if 2 elements of G act on x in the same way, they must be the same element.
(Definition 2.1.7)

1.2.2 Lemma: Equivalent Conditions for Faithful Actions

*If G acts on a set X, the following are **equivalent**:*

1. *the action is **faithful***
2. *let $g \in G$. If:*
$$\forall x \in X, \ gx = x$$
then $g = 1_G$
3. *the homomorphism:*
$$\Sigma : G \to Sym(X)$$
*is **injective***
4. *$ker(\Sigma) = \{1_G\}$*

Proof.

- $\textcircled{1} \iff \textcircled{3}$ An action is faithful if and only if:
$$\Sigma(g) = \Sigma(h) \implies g = h$$
But this is precisely the definition of injectivity.
- $\textcircled{2} \iff \textcircled{4}$ The kernel is trivial if and only if the only element which acts trivially is 1_G, so $gx = x$ only when $g = 1_G$.
- $\textcircled{3} \iff \textcircled{4}$ A property of group homomorphisms is that they are injective if and only if they have a trivial kernel

□

1.2.3 Examples

- the action of $Sym(X)$ on X is faithful, since Σ is the identity mapping, which is injective
- similarly, the action of $Aut(X)$ on a vector space is faithful, since the inclusion $\Sigma : Aut(X) \to Sym(X)$ is injective
- the only isometry which doesn't change the faces/edges/vertices of a cube is the trivial action, so $ker(\Sigma)$ is trivial, and the action is faithful. However, this isn't true for the long diagonals: $Sym(X)$ has $4! = 24$ elements, whilst $|G| = 48$, so $\Sigma : G \to Sym(X)$ can never be injective
- the trivial action is only faithful when G is trivial, since $gx = x$ for any g, x

1.2.4 Lemma: G Acts Faithfully When $Sym(X)$ Has a Copy of G

This lemma tells us that when a group acts faithfully on X, it is because $Sym(X)$ contains a "copy" of the group!

*Let G be a group acting **faithfully** on the set X.*
*G is **isomorphic** to the **subgroup**:*

$$im(\Sigma) = \{\bar{g} = \Sigma(g) \mid g \in G\} \leq Sym(X)$$

where:

$$\Sigma : G \to Sym(X)$$

(Lemma 2.1.11)

Proof. Since G acts faithfully, Σ is injective. It is clear that any injective homomorphism $\varphi : G \to H$ induces an isomorphism between G and $im(\varphi)$, so:

$$G \cong im(\Sigma)$$

□

---

*For example, with the **isometries** acting on the **vertices**, the **subgroup** $im(\Sigma)$ consists of those permutations which switch the vertices around according to the isometry.*
*This tells us that, for example, there are no transpositions in $im(\Sigma)$, since there is no isometry which **only** changes 2 vertices, and leaves the rest unchanged.*

1.3 Fixed Sets

1.3.1 Definition: Fixed Set

*Let G be a **group** acting on X, and consider a subset $S \subseteq G$. The **fixed set** of S is:*

$$Fix(S) = \{x \mid x \in X,\ \forall s \in S\ :\ sx = x\}$$

(Definition 2.1.14)

1.3.2 Lemma: Fixed Set of Conjugate Group

*Let G be a **group** acting on X, and consider a subset $S \subseteq G$. Then:*

$$\forall g \in G\ :\ Fix(gSg^{-1}) = gFix(S)$$

(Lemma 2.1.15)

Proof.

$$\begin{aligned} & x \in Fix(gSg^{-1}) \\ \iff & \forall s \in S\ :\ gsg^{-1}x = x \\ \iff & \forall s \in S\ :\ sg^{-1}x = g^{-1}x \\ \iff & g^{-1}x \in Fix(S) \\ \iff & x \in gFix(S) \end{aligned}$$

□

2 Rings

*In **Galois Theory**, we will work with **rings**, which are defined a bit different to **Honours Algebra**. As such, **homomorphisms** and **subrings** which were valid in **Honours Algebra** won't be valid in this course!*

2.1 Rings in Galois Theory

2.1.1 Definition: Ring

*A **ring** is a special **set** armed with **2 operations**: addition and multiplication*

$$(R, +, \cdot)$$

Rings have the following properties:

1. $(R, +)$ *is an **abelian group**, with identity* 0_R
2. $(R, \cdot)$ *is a **commutative monoid**:*
   - *multiplication is **associative** and **commutative***
   - R *contains an identity element* 1_R *satisfying:*

   $$\forall a \in R \; : \; a \cdot 1_R = 1_R \cdot a = a$$

3. *the **distributive law** holds in* R*:*

   $$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

   $$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

2.1.2 Definition: Ring Homomorphism

*A **ring homomorphism** is a mapping between 2 rings R, S:*

$$\varphi : R \to S$$

such that if $r_1, r_2 \in R$:

1. $$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$$
2. $$\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$$
3. $$\varphi(1_R) = 1_S$$
4. $$\varphi(0_R) = 0_S$$
5. $$\varphi(-r) = -\varphi(r)$$

*To show that φ is a **ring homomorphism**, it is sufficient to show that the first 3 conditions hold.*

---

*In **Honours Algebra**, preserving the multiplicative identity wasn't necessary for a homomorphism. As such, homomorphisms such as:*

$$\varphi : \mathbb{R} \to GL(\mathbb{R}; 2)$$
$$\varphi(x) = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$$

*which were valid in **Honours Algebra** won't work for this course!*

2.1.3 Definition: Subring

*A **subring** of a **ring** R is a **subset** $S \subseteq R$, such that:*

1. $$0_R, 1_R \in S$$
2. *S is closed under **subtraction** and **multiplication***

- **How do subrings arise from ring homomorphisms?**
  - if $\varphi : R \to S$ is a **ring homomorphism**, then $im(\varphi)$ is a **subring** of S
- **How do ring homomorphisms arise from subrings?**
  - if S is a **subring** of R, the **inclusion** $\iota(s) = s$ is a **ring homomorphism**
- **What are subrings analogous to in group theory?**
  - they are analogous to **subgroups**

2.1.4 Definition: Ideal

*An **ideal** is a **subset** I of a **ring** R, satisfying:*

1. $I \neq \emptyset$
2. *I is closed under subtraction*
3. $\forall i \in I, \forall r \in R, ri, ir \in I$

- **How do ideals arise from ring homomorphisms?**
  - if $\varphi : R \to S$ is a **ring homomorphism**, then $ker(\varphi)$ is an **ideal** of R
- **What are ideals analogous to in group theory?**
  - an **ideal** is analogous to a **normal subgroup**
  - however, unlike in group theory, **ideals** are **not** a special type of **subring**
  - for instance, **subrings** contain 1_R, but most **ideals** won't

2.1.5 Exercises

1. *[Exercise 2.2.6]* **Prove that the only subring of a ring R that is also an ideal is R itself.**

   Let R be a ring, and S a subring of R. In particular, this implies that $1_R \in S$. If S is also an ideal, then for any $r \in R$, it follows that:
   $$r \cdot 1_R = 1_R \cdot r = r \in S$$
   In other words, if S is an ideal, $S = R$.

2. *[Exercise 2.2.8]* **The *trivial ring* or *zero ring* is the one-element set with its only possible ring structure ($0_R + 0_R = 0_R, 0_R \cdot 0_R = 0_R$). Show that the only ring in which $0_R = 1_R$ is the trivial ring.**

   Let R be the trivial ring, and let S be some other ring with $0_S = 1_S$. Let $s \in S$ be some non-zero element in S. Then:
   $$s \cdot 1_S = s \;\&\; s \cdot 0_s = 0_S \implies s = 0_S$$
   In particular, if $0_S = 1_S$, then S can only have one element, namely 0_S.

2.1.6 Definition: Integral Domain

*An **integral domain** is a **ring** R, such that:*

1. $0_R \neq 1_R$
2. $$\forall r_1, r_2 \in R \ : \ r_1 r_2 = 0_R \implies r_1 = 0_R \textit{ or } r_2 = 0_R$$

- **What is the cancellation law?**
  - in **integral domains**, the **cancellation law** applies:

    $$r_1 s = r_2 s \implies r_1 = r_2 \textit{ or } s = 0$$

  - in an arbitrary **ring**, this need not be the case. For instance, in $\mathbb{Z}_6$:

    $$1 \cdot 2 = 2 = 4 \cdot 2$$

    but $1 \neq 4$

2.1.7 Definition: Quotient/Factor Rings

*Let R be a **ring**, and I an **ideal**. A **quotient** or **factor ring**, is the **ring** R/I.*
*R/I is the set of **cosets** of the form:*

$$r + I = \{r + i \mid i \in I\}$$

We define addition and multiplication in the quotient ring via:

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$$

$$(r_1 + I)(r_2 + I) = (r_1 r_2) + I$$

Tom Leinster gives a nice way of visualising ***quotient rings****.*
We can think of a ***ring*** *as a* ***loaf of bread****. The* ***cosets*** $r + I$ *partition the loaf into* ***slices****, with each element of* $r + I$ *being a* ***crumb****. A* ***quotient ring*** *allows us to work with* ***slices****, instead of having to focus on the crumbs to operate.*
For example, consider the ***ring*** $\mathbb{Z}$*. Define* I *as the ideal containing the* ***multiples of 10*** *of the integers. The* ***quotient ring*** R/I *corresponds to* $\mathbb{Z}_{10}$*: the integers modulo 10. Our loaf (the* ***integers****) can be partitioned into 10 slices, each corresponding to a remainder. The crumbs would be our integers. For instance, 19 and 129 are both crumbs corresponding to the slice with remainder 9.*

2.2 Lemma: Intersection of Subrings is Subring

Let R *be a* ***ring****, and* $\mathcal{S}$ *be* ***any*** *set of* ***subrings*** *in* R*. Then, the* ***intersection****:*

$$\bigcap_{S \in \mathcal{S}} S$$

is also a ***subring*** *of* R*.*
(Lemma 2.2.3)

Proof. Let $T = \bigcap_{S \in \mathcal{S}} S$. Now:

1. since each S are subrings, they each contain $0_R, 1_R$, so by definition of intersection:

$$0_R, 1_R \in T$$

2. let $r_1, r_2 \in T$. In particular, this means that r_1, r_2 can be found in each subring S. Since S is a subring, $r_1 - r_2 \in S$ for each $S \in \mathcal{S}$, so:

$$r_1 - r_2 \in T$$

A similar argument shows that:

$$r_1, r_2 \in T \implies r_1 r_2 \in T$$

□

2.3 Lemma: Unique Homomorphism Between Integers and Rings

*For any **ring** R, there is exactly one **homomorphism**:*

$$\chi : \mathbb{Z} \to R$$

We can define χ via:

$$\chi(n) = \begin{cases} 0_R, & n = 0 \\ \chi(n-1) + 1_R, & n > 0 \\ -\chi(-n), & n < 0 \end{cases}$$

Alternatively, we can write:

$$\chi(n) = n \cdot 1_R = \sum_{i=1}^{n} 1_R$$

Proof. We first show that this is indeed a ring homomorphism:

1. $$\chi(1) = \chi(0) + 1_R = 0_R + 1_R = 1_R$$

2. let $n, m \in \mathbb{Z}$:
$$\chi(n+m) = \sum_{i=1}^{n+m} 1_R = \sum_{i=1}^{n} 1_R + \sum_{i=1}^{m} 1_R = \chi(n) + \chi(m)$$

3. let $n, m \in \mathbb{Z}$:
$$\chi(nm) = \sum_{i=1}^{nm} 1_R = \sum_{i=1}^{n} \left[1_R \left(\sum_{j=1}^{m} 1_R \right) \right] = \left(\sum_{i=1}^{n} 1_R \right) \left(\sum_{i=1}^{m} 1_R \right) = \chi(n)\chi(m)$$

Now, we show that it is unique. Assume that there exists some other homomorphism $\varphi : \mathbb{Z} \to R$. Certainly:

$$\varphi(0) = 0_R = \chi(0)$$

We can induct on n to show that $\phi(n) = \chi(n)$ for $n \geq 0$. Indeed, if ϕ, χ are homomorphisms, they preserve the identity, which gives the base case. Then:

$$\varphi(n+1) = \varphi(n) + 1_R = \chi(n) + 1_R = \chi(n+1)$$

Then, when $n < 0$:

$$\varphi(n) = -\varphi(-n) = -\chi(-n) = \chi(n)$$

Thus, $\forall n \in \mathbb{Z}$, it follows that $\varphi = \chi$, so χ is the unique homomorphism $\mathbb{Z} \to R$.

□

2.4 Theorem: Universal Property of Factor Rings

*Let I be an **ideal** of the **ring** R. Define the **canonical homomorphism**:*

$$\pi_I : R \to R/I$$

Then:

1. *π_I is **surjective**, and:*

   $$ker(\pi_I) = I$$

2. *If:*

   $$\varphi : R \to S$$

   *is a **ring homomorphism**, and:*

   $$\varphi(I) = \{0_S\}$$

   *(so that $I \subseteq ker(\varphi)$), then there exists a **unique ring homomorphism***

   $$\bar{\varphi} : R/I \to S$$

   such that:

   $$\varphi = \bar{\varphi} \circ \pi_I$$

   Diagrammatically, we have:

$$\begin{tikzcd}
R \arrow[d, "\pi_I"'] \arrow[dr, "\varphi"] & \\
R/I \arrow[r, dotted, "\bar{\varphi}"'] & S
\end{tikzcd}$$

2.5 Generating Ideals

2.5.1 Definition: The Ideal Generated by a Subset

*Let Y be a **subset** of a **ring** R.*
*The set $\langle Y \rangle$ is the **ideal generated by** Y, and it is the **smallest ideal** of R containing Y, in the sense that any other ideal I containing Y is such that $\langle Y \rangle \subseteq I$.*

- **What is the top-down definition of an ideal generated by Y?**
  - any **intersection** of **ideals** will again be an **ideal**
  - $\langle Y \rangle$ can be characterised as the **intersection** of all **ideals** of R containing Y
- **What is the bottom-up definition of an ideal generated by Y?**
  - alternatively, if $Y = \{r_1, \dots, r_n\}$ is some finite subset of R, we can define:

$$\langle Y \rangle = \left\{ \sum_{i=1}^{n} a_i r_i \mid a_i \in R \right\}$$

  - this defines an **ideal** (see Section 8.2 of my Honours Algebra Notes)
  - for any other ideal J containing Y, we know that $r_i \in J$. By closure of ideals, also $a_i r_i \in J$. By closure under addition, also $\sum_{i=1}^{n} a_i r_i \in J$. Hence, $\langle Y \rangle \subseteq J$, as required

2.5.2 Definition: The Principal Ideal

*A **principal ideal** is an **ideal** $\langle r \rangle$ generated by a **single element**:.*

2.5.3 Definition: Principal Ideal Domains

*A **principal ideal domain** is an **integral domain**, such that each **ideal** is a **principal ideal**.*

- **Is $\mathbb{Z}$ a principal ideal domain?**
  - it is clearly an **integral domain**, since only multiplying by 0 gives 0 back
  - intuitively, any ideal of $\mathbb{Z}$ must be composed of integers which are all multiples; otherwise, it would fail properties like $ri, ir \in I$ or closure under subtraction/multiplication
  - in particular, this means that each **ideal** of $\mathbb{Z}$ must be generated by the **smallest** number contained in the ideal, such that $I = \langle n \rangle$, so any **ideal** must be a **principal ideal**

2.5.4 Definition: Division in Rings

*Let R be a ring, and $r, s \in R$. We say that r **divides** s if:*

$$\exists a \in R \ : \ s = ar$$

in which case we write $r \mid s$.

Alternatively, $s \in \langle r \rangle$ or $\langle s \rangle \subseteq \langle r \rangle$.

2.5.5 Exercises

1. *[Exercise 2.2.15]* **Let r, s be elements of an integral domain. Show that for some unit u:**

$$r \mid s \mid r \iff \langle r \rangle = \langle s \rangle \iff s = ur$$

$r \mid s$ if and only if $s \in \langle r \rangle$, so $\langle s \rangle \subseteq \langle r \rangle$. Similarly, $s \mid r$ if and only if $r \in \langle s \rangle$, so $\langle r \rangle \subseteq \langle s \rangle$. Thus:

$$r \mid s \mid r \iff \langle r \rangle = \langle s \rangle$$

In particular, this is true if and only if $\exists u \in R$ such that:

$$s = ur$$

But also $\exists w \in R$ such that:

$$r = ws$$

so overall:

$$s = uws$$

Since we operate over an integral domain, and $s \neq 0_R$, by the cancellation law:

$$uw = 1$$

so u must be a unit.

2.6 Units in Rings

2.6.1 Definition: Units

> *Let R be a **ring**. An element $u \in R$ is a **unit** if it has a **multiplicative inverse**.*
>
> ---
>
> *Alternatively, u is a **unit** if:*
> $$\langle u \rangle = R$$

- **Why is the second condition equivalent to the first?**
  - notice, if u has an inverse, then any element $r \in R$ can be generated via:

$$r = (ru^{-1})u$$

  - since $ru^{-1} \in \langle u \rangle$, it thus follows that $r \in \langle u \rangle$ for any r

2.6.2 Lemma: Units Form a Group

*Let R be a **ring**. The set $R^\times$, containing all **units** of R, is a **group** under **multiplication**.*

Proof. We check the group axioms. Let $a, b \in R^\times$

1. **Closure**: consider ab. Since R is a ring, it is closed under multiplication, so $ab \in R$. This is a unit in R if and only if it has an inverse in R. Indeed, since a, b are units, then $\exists a^{-1}, b^{-1} \in R$. Moreover, $b^{-1}a^{-1} \in R$ too. But then:
$$(b^{-1}a^{-1})(ab) = b^{-1}b = 1_R$$
$$(ab)(b^{-1}a^{-1}) = aa^{-1} = 1_R$$
So in particular, $b^{-1}a^{-1} \in R$ is the inverse of $ab \in R$, so $ab \in R^\times$. Hence, $R^\times$ is closed under multiplication.
2. **Associativity**: multiplication in a ring R is associative; $R^\times \subseteq R$, so multiplication is associative in $R^\times$ too.
3. **Identity**: since 1_R is always its own inverse, it follows that $1_R \in R^\times$, and 1_R is the identity of $R^\times$.
4. **Existence of Inverse**: trivially, if $a \in R^\times$, its inverse a^{-1} must also be in $R^\times$

□

2.6.3 Definition: Coprimes in Rings

*Let R be a ring. $r, s \in R$ are **coprime** if for some $a \in R$:*

$$a \mid r \textbf{ and } a \mid s \implies a \text{ is a } \textbf{unit}$$

*In other words, 2 **ring** elements are **coprime** if the only element which divides both is a **unit**.*

2.6.4 Proposition: Bezout's Identity

*Let R be a **principal ideal domain**, and let $r, s \in R$. Then:*

$$r, s \text{ coprime} \iff \exists a, b \in R \,:\, ar + bs = 1_R$$

(Proposition 2.2.16)

Proof.

- ($\implies$): assume that r, s are coprime. Since R is a principal ideal domain, the ideal generated by r, s must be principal, so:
$$\exists u \in R \ : \ \langle r, s \rangle = \langle u \rangle$$
Thus, it follows that $r, s \in \langle u \rangle$, so:
$$u \mid r \qquad u \mid s$$
Since r, s are coprime, it must be the case that u is a unit, and so, $\langle u \rangle = R$. But then, we must have that $1_R \in \langle u \rangle$. Going back to the definition of $\langle r, s \rangle$, we must then have that:
$$1_R \in \langle r, s \rangle = \{ar + bs \mid a, b \in R\}$$
as required.

- ($\impliedby$): suppose that $ar + bs = 1_R$. If $u \in R$ is such that:
$$u \mid r \qquad u \mid s$$
then:
$$u \mid (ar + bs) \implies u \mid 1_R$$
But this is only possible if $\exists a \in R$ such that:
$$ua = 1_R$$
In other words, u has an inverse $a = u^{-1}$, and so, u is a unit. Thus, r, s must be coprime.

□

3 Fields

3.1 Fields in Galois Theory

3.1.1 Definition: Field

*A **field** is a **commutative ring** R, such that:*

- $0_R \neq 1_R$
- *every non-zero $r \in R$ is a **unit***

*In particular, every **field** is an **integral domain**.*

- **Are all integral domains fields?**
  - no. For example, $\mathbb{Z}$ is an **integral domain**, but not a **field**
  - however, in **Honours Algebra**, we showed at all **finite integral domains** are **fields** (see Section 5.5 of my Honour Algebra notes)
- **How many ideals does a field have?**
  - a **field** K only has **trivial ideals**: $\{0_K\}, K$
  - if I were some non-trivial ideal, then $u \in I$ is a unit, so $\langle u \rangle = K$
  - but I will be generated by u, so $I = K$

3.1.2 Definition: Rational Expressions

*A **rational expression** over a **field** K is a **ratio** of 2 **polynomials** over K:*

$$\frac{f(t)}{g(t)}, \quad f(t), g(t) \neq 0 \in K[t]$$

---

*Two **rational expressions** $\frac{f_1}{g_1}, \frac{f_2}{g_2}$ are **equal** if:*

$$f_1 g_2 = f_2 g_2$$

over the field $K[t]$.

---

*The set of **rational expressions** over K is denoted by $K(t)$ (and this is a **field**).*
(Example 2.3.2)

3.1.3 Definition: Subfields

*A **subfield** of a **field** K is a **subring** of K which is also a **field**.*

3.2 Field Homomorphisms

3.2.1 Lemma: Field Homomorphisms are Injective

*Every **field homomorphism** is **injective**.*

Proof. Let $\varphi : K \to L$ be a field homomorphism. By properties of rings, $ker(\varphi)$ is an ideal of K, so:

$$ker(\varphi) = \{0_K\} \textit{ or } ker(\varphi) = K$$

Now, it is impossible that $ker(\varphi) = K$, since this implies that $\varphi(1_K) = 0_L$, but by definition of a ring homomorphism we must have that $\varphi(1_K) = 1_L$. This would imply that $0_L = 1_L$, which contradicts the fact that L is a field. Hence, the only possibility is $ker(\varphi) = \{0_K\}$, so φ is injective. □

3.2.2 Lemma: Images and Preimages of Homomorphisms are Subfields

*Consider the **field homomorphism**:*

$$\varphi : K \to L$$

1. *For any **subfield** A of K, the **image** $\varphi(A)$ is a **subfield** of L*
2. *For any **subfield** B of L, the **preimage** $\varphi^{-1}(B)$ is a **subfield** of K*

(Lemma 2.3.6)

Proof. We prove the first part, since the second part follows a similar argument.

We begin by showing that the image $\varphi(A)$ is a subring of L. Since φ is a ring homomorphism:

$$\varphi(0_A) = \varphi(0_K) = 0_L \qquad \varphi(1_A) = \varphi(1_K) = 1_L$$

so $0_L, 1_L \in \varphi(A)$. Moreover, if $a, b \in A$ by closure of the ring $a - b \in A$ and $ab \in A$ so:

$$\varphi(a) - \varphi(b) = \varphi(a - b) \in \varphi(A)$$

$$\varphi(a)\varphi(b) = \varphi(ab) \in \varphi(A)$$

Hence, $\varphi(A)$ is a subring. To show that it is a subfield, we already know that $0_L \neq 1_L$, so it is sufficient to show that every element in $\varphi(A)$ is a unit. Indeed, since A is a subfield, if $a \neq 0_A \in A$, then $a^{-1} \in A$. Since fields are groups under multiplication, and group homomorphisms preserve inverses:

$$\varphi(a^{-1}) = \varphi(a)^{-1}$$

and so any $\varphi(a) \in \varphi(A)$ is a unit, so $\varphi(A)$ is a field.

□

3.3 The Equalizer

*We now look at the **equalizer**: a way of generating **fields** from **homomorphisms** between any 2 fields.*

3.3.1 Definition: The Equalizer

Let X, Y be sets, and let S be a subset of all functions of the form $X \to Y$.
*The **equalizer** of S is:*

$$Eq(S) = \{x \mid x \in X, \forall f, g \in S : f(x) = g(x)\}$$

*That is, the **equalizer** is the set of all $x \in X$ which are equal under all functions in S.*
(Definition 2.3.7)

3.3.2 Lemma: Equalizers are Subfields

*Let K, L be **fields**, and let S be a subset of all **homomorphisms** of the form $K \to L$.*
*Then, the **equalizer** $Eq(S)$ is a **subfield** of K.*
(Lemma 2.3.8)

*For example, consider $K = L = \mathbb{C}$, and $S = \{id_{\mathbb{C}}, \kappa\}$, where κ denotes **complex conjugation**. Then:*

$$Eq(S) = \{z \mid \bar{z} = z\} = \mathbb{R}$$

and $\mathbb{R}$ is a subfield of $\mathbb{C}$.

Proof. By definition of ring homomorphisms, we know that $0_K, 1_K \in Eq(S)$.

Now, let $a, b \in Eq(S)$. That is, for all $\varphi, \theta \in S$:

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

Then:

$$\varphi(a) - \varphi(b) = \theta(a) - \theta(b) \implies \varphi(a - b) = \theta(a - b)$$

so $a - b \in Eq(S)$. Similarly:

$$\varphi(a)\varphi(b) = \theta(a)\theta(b) \implies \varphi(ab) = \theta(ab)$$

so $ab \in Eq(S)$.

Finally, since K is a field, any $a \in K$ has an inverse $a^{-1} \in K$. Moreover, $\varphi(K), \theta(K)$ are subfields of L, so it follows that $\varphi(a)^{-1}, \theta(a)^{-1}$ exist. Hence, and using the cancellation property:

$$\varphi(a)\varphi(a)^{-1} = \theta(a)\theta(a)^{-1} \implies \varphi(a^{-1}) = \theta(a^{-1})$$

Thus, $Eq(S)$ is a subfield of K as required.

□

3.4 The Characteristic of a Ring

3.4.1 Definition: The Characteristic

Let R be a ***ring****. We define the* ***characteristic*** *of R, $char(R)$, as the smallest $n \in \mathbb{N}$, such that:*

$$n \cdot 1_R = 0_R$$

If no such n exists, then $char(R) = 0$.

An alternative way of viewing $char(R)$ arises by considering the unique homomorphism:

$$\chi : \mathbb{Z} \to R$$

Since $\mathbb{Z}$ is a principal ideal domain, the kernel $ker(\chi)$ will be a ***principal ideal****, so:*

$$\exists n \geq 0 \ : \ ker(\chi) = \langle n \rangle$$

and $char(R) = n$.

3.4.2 Examples of Characteristics

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ all have characteristic 0
- the characteristic of $\mathbb{Z}_p$ (integers modulo p) is p
- if K is a field, then:

  $$char(K) = char(K(t))$$

  where recall, $K(t)$ is the **field of rational expressions**

3.4.3 Lemma: Characteristic of Integral Domains

In fact, turns out that we have already seen all the possible characteristics in the above example (at least for ***integral domains****).*

Let K be an ***integral domain****, then:*

- *$char(K) = 0$*
- *or $char(K) = p$ (p is* ***prime****)*

In particular, if R is a ***field****, then $char(R) = 0$ or $char(R) = p$.*
(Lemma 2.3.11)

Proof. Let R be an integral domain, and define:

$$n = char(R)$$

If $n = 0$, we are done, so assume that $n > 0$.

R is an integral domain, so $0_R \neq 1_R$, and so, $n \neq 1$. Now, since n is a positive integer:

$$\exists k, m > 0 \ : \ km = n$$

Then:

$$\chi(k)\chi(m) = \chi(km) = \chi(n) = 0_R$$

by definition of the characteristic and χ. R is an integral domain, so:

$$\chi(k) = 0_R \ or \ \chi(m) = 0_R$$

Without loss of generality, we may assume that $\chi(k) = 0_R$. But then, again by the definition of the characteristic, $ker(\chi) = \langle n \rangle$, so:

$$k \in \langle n \rangle \implies n \mid k$$

Thus, since $k \mid n$ and $n \mid k$, it follows that $k = n$. Since this holds for any possible factorisation of n, it must be the case that n is prime, as required.

□

3.4.4 Lemma: Homomorphisms Between Fields of Same Characteristic

Let:

$$\varphi : K \to L$$

be a ***field homomorphism****. Then:*

$$char(K) = char(L)$$

(Lemma 2.3.12)

Proof. Let χ_K, χ_L be the unique homomorphisms:

$$\chi_K : \mathbb{Z} \to K \quad \chi_L : \mathbb{Z} \to L$$

Now, if we have some homomorphism $\varphi : K \to L$, it follows by the uniqueness that:

$$\chi_L = \varphi \circ \chi_K$$

Moreover, since φ is a field homomorphism, it is injective, so:

$$ker(\varphi) = \{0_K\}$$

so $ker(\varphi \circ \chi_K)$ contains all the elements of $\mathbb{Z}$, for which χ_K evaluates to 0_K; in other words:

$$ker(\varphi \circ \chi_K) = ker(\chi_K)$$

But since $\chi_L = \varphi \circ \chi_K$, it follows that:

$$ker(\chi_L) = ker(\varphi \circ \chi_K) = ker(\chi_K)$$

which is equivalent to:

$$char(K) = char(L)$$

An alternative is that we must have:

$$\chi_L(n) = n \cdot 1_L = \varphi(n \cdot 1_K)$$

The injectivity of φ implies that:

$$n \cdot 1_L = 0_L \iff n \cdot 1_K = 0_K$$

so again $char(K) = char(L)$. □

3.5 Prime Subfields

3.5.1 Definition: The Prime Subfield

*The **prime subfield** of some **field** K is the **smallest subfield** of K (in the sense that any othe **subfield** of K contains it).*

This can be defined more concretely:

- ***[top-down view]**: the **prime subfield** of K is the **intersection** of **all** subfields of K (similarly to how intersections of subrings are subrings, intersections of subfields are subfields)*
- ***[bottom-up view]**: the **prime subfield** of K is defined by the set:*

$$\left\{ \frac{m \cdot 1_K}{n \cdot 1_K} \mid m, n \in \mathbb{Z} \ : \ n \cdot 1_K \neq 0_K \right\}$$

Proof. For completeness, we show that the bottom-up view indeed defines the smallest subfield, call it S.

Firstly, it is a subfield. We first show it is a subring:

- $0_K \in S$ (just set $m = 0, n \neq 0$
- $1_K \in S$ (just set $m = n \neq 0$)

- let $a, b \in S$, such that:
$$\exists m_a, n_a, m_b, n_b \ : \ a = \frac{m_a \cdot 1_K}{n_a \cdot 1_K} \qquad b = \frac{m_b \cdot 1_K}{n_b \cdot 1_K}$$
In particular, we also know that there exists z_a, z_b such that we can write:
$$(z_a \cdot 1_K)(n_a \cdot 1_K) = m_a \cdot 1_K \iff (z_a n_a) \cdot 1_K = m_a \cdot 1_K$$
$$(z_b \cdot 1_K)(n_b \cdot 1_K) = m_b \cdot 1_K \iff (z_b n_b) \cdot 1_K = m_b \cdot 1_K$$
using the fact that χ is a homomorphism. Furthermore:
$$(z_a n_a n_b) \cdot 1_K = (m_a n_b) \cdot 1_K \qquad (z_b n_a n_b) \cdot 1_K = (m_b n_a) \cdot 1_K$$
so:
$$((n_a n_b) \cdot 1_K)((z_a - z_b) \cdot 1_K) = (m_a n_b - m_b n_a) \cdot 1_K \implies a - b = \frac{(m_a n_b - m_b n_a) \cdot 1_K}{(n_a n_b) \cdot 1_K} \in S$$

- similar work shows that $ab \in S$ aswell

Moreover, each element in S will be a unit. In particular:
$$a = \frac{m \cdot 1_K}{n \cdot 1_K}$$
and define:
$$b = \frac{n \cdot 1_K}{m \cdot 1_K}$$
Then:
$$ab((nm) \cdot 1_K) = ((nm) \cdot 1_K) \iff ab = 1_K$$
so b is the inverse of a, and $a \in S$.

Moreover, S will be the smallest subfield, for if we have some other subfield L, then:
$$1_K \in L \implies m \cdot 1_K \in L$$
But then for some $n \cdot 1_K \neq 0_K$, certainly we have that by closure of the subfield:
$$(m \cdot 1_K)(z \cdot 1_K) = n \cdot 1_K \implies \frac{m \cdot 1_K}{n \cdot 1_K} = z \cdot 1_K \in L$$

□

3.5.2 Examples of Prime Subfields

- the **prime subfield** of $\mathbb{Q}$ is $\mathbb{Q}$ itself:
  - from the top-down perspective, since $\mathbb{Q}$ has no proper subfields (except itself), the intersection of all it subfields is itself
  - from the bottom-up view, the prime subfield is precisely the definition of the rationals (since $1_{\mathbb{Q}} = 1$)
- in fact, the **prime subfield** of $\mathbb{R}, \mathbb{C}$ are also $\mathbb{Q}$ (proving this with the top-down view is harder than with the bottom-up view)
- the **prime subfield** of $\mathbb{Z}_p$ is again $\mathbb{Z}_p$ itself

3.5.3 Lemma: Only 2 Prime Subfields

*In fact, the example above showcases **all** possible prime subfields.*

> *Let K be a **field**:*
>
> - *if $char(K) = 0$, then the **prime subfield** of K is (isomorphic to) $\mathbb{Q}$*
> - *if $char(K) = p$, then the **prime subfield** of K is (isomorphic to) $\mathbb{Z}_p$*
>
> *(Lemma 2.3.16)*

Proof. Begin by assuming that $char(K) = 0$. Then, for any $n > 0, n \cdot 1_K \neq 0$. Using the fact that χ is a homomorphism, one can see that the mapping:

$$\varphi : \mathbb{Q} \to K$$

defined by:

$$\varphi : \frac{m}{n} \to \frac{m \cdot 1_K}{n \cdot 1_K}$$

is well-defined. Since φ is a field homomorphism, it is injective, so it defines an isomorphism:

$$im(\varphi) \cong \mathbb{Q}$$

Now, $\mathbb{Q}$ has no proper subfields, so $im(\varphi)$ can't have any subfields. Moreover, $im(\varphi)$ is a subfield of K. Since it doesn't have any proper subfield, in particular it must be the smallest subfield of K, and thus, its prime subfield.

Alternatively, assume that $char(K) = p > 0$, where p is prime. Then, the unique mapping χ has:

$$ker(\chi) = \langle p \rangle$$

by definition of the charcteristic. But then, recalling the first isomorphism theorem, we have that:

$$\mathbb{Z}/\langle p \rangle \cong im(\chi) \implies \mathbb{Z}_p \cong im(\chi)$$

Again, $\mathbb{Z}_p$ has no proper subfields, so $im(\chi)$ doesn't either. The fact that $im(\chi)$ is a subfield of K then implies that it must be the prime subfield.

□

3.5.4 Lemma: Finite Fields Have Positive Characteristic

> *Every **finite field** has **positive characteristic**.*
> *(Lemma 2.3.17)*

Notice however that this need not mean that infinite fields have 0 characteristic. For example, the field of ***rational expressions*** *over $\mathbb{Z}_p$, $\mathbb{Z}_p(t)$, is an infinite field of positive characteristic.*

Proof. A field of characteristic 0 must have a subfield isomorphic to $\mathbb{Q}$, which is infinite.

□

3.6 Rings of Prime Characteristic

3.6.1 Lemma: Prime Divisibility

Let p be ***prime****. Then:*

$$\forall i \in (0,p) \;:\; p \left| \begin{pmatrix} p \\ i \end{pmatrix} \right.$$

(Lemma 2.3.19)

Proof. From definition:

$$\begin{pmatrix} p \\ i \end{pmatrix} = \frac{p!}{(p-i)!i!} \implies p! = i!(p-i)! \begin{pmatrix} p \\ i \end{pmatrix}$$

Now, the LHS is clearly divisble by p. However, on the RHS neither $i!$ nor $(p-i)!$ are. This means that p must divide $\begin{pmatrix} p \\ i \end{pmatrix}$ as required. □

3.6.2 Proposition: The Frobenius Map

Let p be a ***prime****, and R a* ***ring*** *of* ***characteristic*** *p. Then:*

1. *The* ***Frobenius map****:*

$$\theta : R \to R$$
$$\theta(r) = r^p$$

   is a ***homomorphism****.*

2. *If R is a* ***field****, then θ is* ***injective.***
3. *If R is a* ***finite field****, then θ is an* ***automorphism*** *of R.*

(Proposition 2.3.20)

Proof.

① **Frobenius Map is Homomorphism**

- $$\theta(0_R) = 0_R^p = 0_R$$

- $$\theta(1_R) = 1_R^p = 1_R$$

- $$\theta(r+s) = (r+s)^p = \sum_{i=0}^{p} \begin{pmatrix} p \\ i \end{pmatrix} r^i s^{p-i}$$

  But since $\begin{pmatrix} p \\ i \end{pmatrix}$ is divisible by p, and $char(R) = p$, then:

  $$\forall i \in (0,p), \ \begin{pmatrix} p \\ i \end{pmatrix} r^i s^{p-i} = 0_R$$

  Thus:

  $$\theta(r+s) = (r+s)^p = r^p + s^p = \theta(r) + \theta(s)$$

- $$\theta(rs) = (rs)^p = r^p s^p = \theta(r)\theta(s)$$

Hence, as required θ is a ring homomorphism.

② **Injectivity**

Any field homomorphism is injective.

③ **Automorphism**

If R is a finite field, θ is an injective homomorphism to a finite field, so in particular it must be an isomorphism.

This follows by the fact that every injection from a finite set to itself is bijective (the mapping is between 2 finite sets of the same order, and injectivity implies that each element in the set is mapped to another (unique) element of the set, so in particular, every element of the set must be mapped to, and so, the mapping is also surjective)

□

3.6.3 Example: The Frobenius Map for $\mathbb{Z}_p$

Consider the ring $\mathbb{Z}_p$. Recall, for a group G of finite order n, Lagrange's Theorem states that for any element $g \in G$, we must have $g^n = 1_G$.

Applying this over the multiplicative group $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0_G\}$ implies that:

$$\forall a \in \mathbb{Z}_p^\times \ a^{p-1} = 1_G$$

In particular, this means that if θ is the Frobenius Map:

$$\theta(a) = a^p = a^{p-1}a = a$$

In other words, the Frobenius automorphism is the identity, and every element of $\mathbb{Z}_p$ is its own pth root!

3.6.4 Corollary: pth Roots in Fields of Characteristic p

*Let p be a **prime**:*

1. *In a **field** of **characteristic** p, every element has **at most one** pth root*
2. *In a **finite field** of **characteristic** p, every element has **exactly one** pth root*

(Corollary 2.3.22)

Proof.

①

This is equivalent to saying that the Frobenius map is injective (each a is mapped to a unique a^p, so each a^p has at most one pth root a).

②

This is equivalent to saying that the Frobenius map is bijective (which is true for finite fields).

□

3.6.5 Examples: pth Roots

- if R is a field of characteristic 2, then each element has **at most** one square root
- over the field $\mathbb{C}$, there are p different pth roots of unity; however, in a field K of characteristic p, there will only be one such root (namely 1_K)
- it can be shown (next chapter) that $t \in \mathbb{Z}_p(t)$ is an example of an element without any pth root (over fields of characteristic p there is at most one pth root - this is a situation in which there are no roots!)

3.7 Irreducible Ring Elements

3.7.1 Definition: Irreducible Element

*Let R be a **ring**. $r \in R$ is **irreducible** if:*

- $r \neq 0_R$
- *r is not a **unit***
- $$\forall a, b \in R \ : \ ab = r \implies a \text{ or } b \text{ is a unit}$$

- **Are 0_R or the units of R reducible or irreducible?**
  - neither
  - this is similar to how $0, 1$ are neither primes nor composite over the integers
- **How many irreducible elements are there in a field?**
  - none, since all the elements of a field are either units or 0

3.7.2 Proposition: Irreducible Ring Elements in Principal Ideal Domains

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

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

(Proposition 2.3.26)

Proof. Denote with π the canonical homomorphism:

$$\pi : R \to R/\langle r \rangle$$

- ($\implies$): assume that r is irreducible. We seek to show that $F = R/\langle r \rangle$ is a field:
  1. 0_F corresponds to all the elements in $\langle r \rangle$. Since r is not a unit, in particular $1_R \notin \langle r \rangle$, so:
  $$\pi(1_R) = 1_F \neq 0_F$$
  2. Now we just need to show that every element in F is a unit. Let $s \notin \langle r \rangle$ (r is not a unit, so such an s exists). Then, we must have that $r \not| s$. Moreover, since r is irreducible, it is only divisible by a unit, so anything that divides r and s will be a unit. In particular, this implies that r and s will be coprime, so by Bezout's:
  $$\exists a, b \in R \ : \ ar + bs = 1_R$$
  Thus:
  $$\pi(a)\pi(r) + \pi(b)\pi(s) = 1_F \implies \pi(b)\pi(s) = 1_F \iff \pi(s)^{-1} = \pi(b)$$
  using the fact that $\pi(r) = 0$, and properties of ring homomorphisms. Thus, it follows that $\pi(s)$ will be a unit, so any non-zero element of F is a unit, so F is a field.
- ($\impliedby$): now assume that $F = R/\langle r \rangle$ is a field. We seek to show that r is irreducible:
  1. We can show that r can't be a unit. Since F is a field, $0_F \neq 1_F$, so:
  $$\pi(1_R) = 1_F \neq 0_F \implies 1_R \notin ker(\pi) = \langle r \rangle$$
  Thus, $r \not| 1_R$, so r won't be a unit (it doesn't have an inverse)

2. Next, we show that if $r = ab$ for some $a, b \in R$, then a or b is a unit. Notice:

$$0_F = \pi(r) = \pi(a)\pi(b)$$

Since we operate over an integral domain, WLOG we may assume that $\pi(a) = 0_F$, which implies that $a \in ker(\pi) = \langle r \rangle$. Thus $a = rz$ for some $z \in R$, so:

$$r = ab = rzb$$

Since $r \neq 0_R$, and R is an integral domain, the Cancellation Law implies that $zb = 1_R$, so b is a unit, as required.

□

3.7.3 Example: Building New Fields

The proposition above allows us to construct new fields from **irreducible elements** (provided we have a **principal ideal domain**). For example, $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$ are **fields**, precisely because $\mathbb{Z}$ is a principal ideal domain, and the primes are irreducible in the integers (since a prime p only factorises as $\pm 1 \cdot \mp p$, and ± 1 are the units of $\mathbb{Z}$).