Fields and Galois Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Definitions and Basic Properties

Rings and Commutative Rings

- A **ring** $R=(R,+,\cdot)$ is a non-empty set R furnished with two binary operations + (called **addition**) and $\cdot$ (called **multiplication**) with the following properties:
  - (R1) **The associative law for addition**: $(a+b)+c=a+(b+c)$, for all $a,b,c\in R$;
  - (R2) **The commutative law for addition**: $a+b=b+a$, for all $a,b\in R$;
  - (R3) **The existence of** 0: there exists 0 in R, such that, for all a in R, $a+0=a$;
  - (R4) **The existence of negatives**: for all a in R, there exists $-a$ in R, such that $a+(-a)=0$;
  - (R5) **The associative law for multiplication**: $(ab)c=a(bc)$, for all $a,b,c\in R$;
  - (R6) **The distributive laws**: $a(b+c)=ab+ac$, $(a+b)c=ac+bc$, for all $a,b,c\in R$.
- We shall be concerned only with **commutative rings**, which have the following extra property:
  - (R7) **The commutative law for multiplication**: $ab=ba$, for all $a,b\in R$.

Rings with 1, Integral Domains and Fields

- A **ring with unity** R has the properties (R1)-(R6), together with the following property:
  (R8) **The existence of** 1: there exists $1 \neq 0$ in R, such that, for all a in R, $a1 = 1a = a$.

  The element 1 is called the **unity element**, or the (**multiplicative**) **identity** of R.
- A commutative ring R with unity is called an **integral domain** or, if the context allows, just a **domain**, if it has the following property:
  (R9) **Cancellation**: for all a, b, c in R, with $c \neq 0$, $ca = cb$ implies $a = b$.
- A commutative ring R with unity is called a **field** if it has the following property:
  (R10) **The existence of inverses**: for all $a \neq 0$ in R, there exists a^{-1} in R, such that $aa^{-1} = 1$.

  We frequently denote a^{-1} by $\frac{1}{a}$.

Cancelation versus Existence of Inverses

- Recall the properties:
  - (R9) **Cancellation**: for all a, b, c in R, with $c \neq 0$, $ca = cb$ implies $a = b$.
  - (R10) **The existence of inverses**: for all $a \neq 0$ in R, there exists a^{-1} in R, such that $aa^{-1} = 1$.
- It is easy to see that (R10) implies (R9).
- The converse implication, however, is not true.

  The ring $\mathbb{Z}$ of integers is an obvious example.
- It is worth noting also that (R9) is equivalent to:
  - (R9)′ **No divisors of zero**: for all a, b in R, $ab = 0$ implies $a = 0$ or $b = 0$.

Groups and Abelian Groups

- A **group** $G = (G, \cdot)$ is a non-empty set furnished with a binary operation $\cdot$ with the following properties:
  - (G1) **The associative law**: $(ab)c = a(bc)$, for all $a, b, c \in G$;
  - (G2) **The existence of an identity element**: there exists e in G, such that, for all a in G, $ea = a$;
  - (G3) **The existence of inverses**: for all a in G, there exists a^{-1} in G, such that $a^{-1}a = e$.
- An **abelian group** has the following extra property:
  - (G4) **The commutative law**: $ab = ba$, for all $a, b \in G$.
- From the previous definitions, we get the following observations.
  - If $(R, +, \cdot)$ is a ring, then $(R, +)$ is an abelian group.
  - If $(K, +, \cdot)$ is a field and $K^* = K \setminus \{0\}$, then $(K^*, \cdot)$ is an abelian group.

Group of Units and Associates

- Let R be a commutative ring with unity, and let

$$U = \{u \in R : (\exists v \in R)(uv = 1)\}.$$

- It is easy to verify that U is an abelian group with respect to multiplication in R.
- We say that U is the **group of units** of the ring R.
- If a, b in R are such that $a = ub$, for some u in U, we say that a and b are **associates**, and write $a \sim b$.

  Example: In the ring $\mathbb{Z}$,
  - The group of units is $\{1, -1\}$;
  - $a \sim -a$, for all a in $\mathbb{Z}$.

Example

- Show that $R = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ forms a commutative ring with unity with respect to the addition and multiplication in $\mathbb{R}$.

  First, we show closure under the operations

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in R.$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in R.$$

  Since R is a subset of $\mathbb{R}$, the properties (R1), (R2), (R5), (R6) and (R7) are automatically satisfied.

  The ring also has the properties (R3), (R4) and (R8):
  - The zero element is $0 + 0\sqrt{2}$;
  - The negative of $a + b\sqrt{2}$ is $(-a) + (-b)\sqrt{2}$;
  - The unity element is $1 + 0\sqrt{2}$.

Example (Cont'd)

- Next, we show that the group of units of R is infinite.
  Since $(1+\sqrt{2})(-1+\sqrt{2})=1$, $1+\sqrt{2}$ is in the group of units.
  The powers of this element are all distinct, since $1+\sqrt{2}>1$.
  So $1+\sqrt{2}<(1+\sqrt{2})^2<(1+\sqrt{2})^3<\cdots$.
  All these powers are in the group of units, which is therefore infinite.
- The group of units is in fact

$$\{a+b\sqrt{2}: a,b\in\mathbb{Z}, |a^2-2b^2|=1\}.$$

  This can be seen by noticing that

$$(a+b\sqrt{2})(c+d\sqrt{2})=1 \quad \text{implies} \quad a^2-2b^2=\pm 1.$$

Group of Units in a Field

- The group of units of a field K is the group K^* of all non-zero elements of K.

  Suppose, first, that u is a unit in K.

  Then, there exists v in K, such that $uv = 1$.

  Since $1 \neq 0$, $u \neq 0$.

  Suppose, conversely, that $u \neq 0$ is an element of K.

  Then, there exists u^{-1} in K, such that $uu^{-1} = 1$.

  Therefore, u is a unit in K.

Divisibility and Proper Divisibility

- Let D be an integral domain.
- If $a \in D \setminus \{0\}$ and $b \in D$, we say that a **divides** b, or that a is a **divisor** of b, or that a is a **factor** of b, if there exists z in D such that

$$az = b.$$

- We write $a \mid b$, and occasionally write $a \nmid b$ if a does not divide b.
- We say that a is a **proper divisor**, or a **proper factor**, of b, or that a **properly divides** b, if z is not a unit.
- Equivalently, a is a proper divisor of b if and only if $a \mid b$ and $b \nmid a$.

Subsection 2

Subrings, Ideals and Homomorphisms

Subrings

- We assume that all our rings are commutative.
- We use standard shorthands, e.g., $a-b$ instead of $a+(-b)$.
- A **subring** U of a ring R is a non-empty subset of R with the property that, for all a, b in R,

$$a, b \in U \quad \text{implies} \quad a-b \in U \text{ and } ab \in U.$$

- Equivalently, $U(\neq \emptyset)$ is a subring if, for all a, b in R,

$$\begin{array}{rcl} a, b \in U & \text{implies} & a+b, ab \in U; \\ a \in U & \text{implies} & -a \in U. \end{array}$$

- It is easy to see that $0 \in U$. Choose a from the non-empty set U. Deduce by definition that $0 = a - a \in U$.

Subfields

- A **subfield** of a field K is a subring which is a field.
- Equivalently, it is a subset E of K, containing at least two elements, such that

$$\begin{array}{rcl} a, b \in E & \text{implies} & a - b \in E; \\ a \in E, b \in E \backslash \{0\} & \text{implies} & ab^{-1} \in E. \end{array}$$

- Again, we may replace the second implication of by the two implications

$$\begin{array}{rcl} a, b \in E & \text{implies} & ab \in E; \\ a \in E \backslash \{0\} & \text{implies} & a^{-1} \in E. \end{array}$$

- If $E \subset K$, we say that E is a **proper subfield** of K.

Ideals

- An **ideal** of R is a non-empty subset I of R with the properties

$$\begin{array}{rcl} a,b\in I & \text{implies} & a-b\in I; \\ a\in I \text{ and } r\in R & \text{implies} & ra\in I. \end{array}$$

- An ideal is certainly a subring, but not every subring is an ideal.
  E.g., consider the field $\mathbb{Q}$ of rational numbers.
  The subring $\mathbb{Z}$ of integers is not an ideal.
- Among the ideals of R are $\{0\}$ and R.
- An ideal I such that $\{0\}\subset I\subset R$ is called **proper**.

Ideal Generated by A

Theorem

Let $A = \{a_1, a_2, \dots, a_n\}$ be a finite subset of a commutative ring R. Then

$$Ra_1 + Ra_2 + \cdots + Ra_n = \{x_1 a_1 + x_2 a_2 + \cdots + x_n a_n : x_1, x_2, \dots, x_n \in R\}$$

is the smallest ideal of R containing A.

- The set $Ra_1 + Ra_2 + \cdots + Ra_n$ is certainly an ideal.
  For all $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n$ in R and for all r in R,

  $$\begin{aligned} &(x_1 a_1 + \cdots + x_n a_n) - (y_1 a_1 + \cdots + y_n a_n) = (x_1 - y_1) a_1 + \cdots + (x_n - y_n) a_n, \\ &r(x_1 a_1 + \cdots + x_n a_n) = (r x_1) a_1 + \cdots + (r x_n) a_n \in Ra_1 + \cdots + Ra_n. \end{aligned}$$

  Every ideal I containing $\{a_1, \dots, a_n\}$ contains the element $x_1 a_1 + \cdots + x_n a_n$, for any $x_1, \dots, x_n$ in R. So $Ra_1 + \cdots + Ra_n \subseteq I$.
- We refer to $Ra_1 + \cdots + Ra_n$ as the **ideal generated by** $a_1, \dots, a_n$.
- We write it as $\langle a_1, \dots, a_n \rangle$.
- An ideal $Ra = \langle a \rangle$ generated by a single element a in R is called a **principal ideal**.

Ideals and Divisibility

Theorem

Let D be an integral domain with group of units U, and let $a, b \in D \setminus \{0\}$. Then:

(i) $\langle a \rangle \subseteq \langle b \rangle$ iff $b \mid a$;

(ii) $\langle a \rangle = \langle b \rangle$ iff $a \sim b$;

(iii) $\langle a \rangle = D$ iff $a \in U$.

(i) Suppose first that $b \mid a$. Then $a = zb$, for some z in D. So

$$\langle a \rangle = Da = Dzb \subseteq Db = \langle b \rangle.$$

Conversely, suppose that $\langle a \rangle \subseteq \langle b \rangle$. Then there exists z in D, such that $a = zb$. So $b \mid a$.

Ideals and Divisibility

(ii) Suppose first that $a \sim b$. Then there exists u in U, such that $a = ub$ and $b = u^{-1}a$. Thus, $b \mid a$ and $a \mid b$. So, by (i), $\langle a \rangle = \langle b \rangle$.

Conversely, suppose that $\langle a \rangle = \langle b \rangle$. Then there exist u, v in D, such that $a = ub, b = va$. Hence

$$(uv)a = u(va) = ub = a = 1a.$$

So, by cancelation, $uv = 1$. Thus u and v are units. So $a \sim b$.

(iii) It is clear that $\langle 1 \rangle = D$.

Hence, by (ii), $\langle a \rangle = D$ if and only if $a \sim 1$.

I.e., $\langle a \rangle = D$ if and only if a is a unit.

Ring Homomorphisms

- A **homomorphism** from a ring R into a ring S is a mapping $\varphi : R \to S$ with the properties:

$$\varphi(a+b) = \varphi(a) + \varphi(b), \qquad \varphi(ab) = \varphi(a)\varphi(b).$$

- Among the homomorphisms from R into S is the **zero mapping** ζ given by

$$\zeta(a) = 0, \text{ for all } a \in R.$$

- Homomorphism other than ζ are called **non-zero**.

Theorem

Let R, S be rings, with zero elements 0_R, 0_S, respectively, and let $\varphi : R \to S$ be a homomorphism. Then:

(i) $\varphi(0_R) = 0_S$;

(ii) $\varphi(-r) = -\varphi(r)$, for all r in R;

(iii) $\varphi(R)$ is a subring of S.

Properties of Ring Homomorphisms

(i) We have $\varphi(a)+\varphi(0_R)=\varphi(a+0_R)=\varphi(a)$.
Therefore, $\varphi(0_R)=-\varphi(a)+\varphi(a)=0_S$.

(ii) For all r in R, we have

$$\varphi(r)+\varphi(-r)=\varphi(r+(-r))=\varphi(0_R)=0_S=\varphi(r)+(-\varphi(r)).$$

Hence, $\varphi(-r)=-\varphi(r)$.

(iii) Let $\varphi(a),\varphi(b)$ be arbitrary elements of $\varphi(R)$, with $a,b\in R$. Then

$$\begin{array}{rcl}\varphi(a)\varphi(b) & = & \varphi(ab)\in\varphi(R);\\ \varphi(a)-\varphi(b) & = & \varphi(a)+\varphi(-b)=\varphi(a+(-b))\in\varphi(R).\end{array}$$

Thus $\varphi(R)$ is a subring.

Corollary

If $\varphi:R\to S$ is a ring homomorphism, then $\varphi(a-b)=\varphi(a)-\varphi(b)$, $a,b\in R$.

Embeddings and Isomorphisms

- Let $\varphi : R \to S$ be a homomorphism.
- If φ is one-to-one, we call it a **monomorphism**, or an **embedding**.
- If φ is also onto we call it an **isomorphism**.
- If $\varphi : R \to S$ is an isomorphism, the rings R and S are **isomorphic** (to each other) and we write $R \cong S$.
- An isomorphism from R onto itself is called an **automorphism**.

Example

- Consider the rings:
  - $R = \{m + n\sqrt{2} : m, n \in \mathbb{Z}\}$, with ordinary addition and multiplication;
  - $S = \left\{\begin{pmatrix} m & n \\ 2n & m \end{pmatrix} : m, n \in \mathbb{Z}\right\}$, with the operations of matrix addition and multiplication.
- The mapping $\varphi : R \to S$, with $\varphi(m + n\sqrt{2}) = \begin{pmatrix} m & n \\ 2n & m \end{pmatrix}$ is an isomorphism.

  We have

$$\begin{aligned} &\varphi((m+n\sqrt{2}) + (p+q\sqrt{2})) = \varphi(m+p+(n+q)\sqrt{2}) \\ &= \begin{pmatrix} m+p & n+q \\ 2(n+q) & m+p \end{pmatrix} = \begin{pmatrix} m & n \\ 2n & m \end{pmatrix} + \begin{pmatrix} p & q \\ 2q & p \end{pmatrix} \\ &= \varphi(m+n\sqrt{2}) + \varphi(p+q\sqrt{2}). \end{aligned}$$

Example (Cont'd)

- Similarly,

$$\begin{aligned}\varphi((m+n\sqrt{2})(p+q\sqrt{2})) &= \varphi((mp+2nq)+(mq+np)\sqrt{2}) \\ &= \begin{pmatrix} mp+2nq & mq+np \\ 2(mq+np) & mp+2nq \end{pmatrix} = \begin{pmatrix} m & n \\ 2n & m \end{pmatrix}\begin{pmatrix} p & q \\ 2q & p \end{pmatrix} \\ &= \varphi(m+n\sqrt{2})\varphi(p+q\sqrt{2}).\end{aligned}$$

Let $\begin{pmatrix} m & n \\ 2n & m \end{pmatrix} \in S$ be given. Then $m+n\sqrt{2} \in R$ and

$\varphi(m+n\sqrt{2}) = \begin{pmatrix} m & n \\ 2n & m \end{pmatrix}$. Hence, φ is onto.

Suppose $\varphi(m+n\sqrt{2}) = \varphi(p+q\sqrt{2})$. Then $\begin{pmatrix} m & n \\ 2n & m \end{pmatrix} = \begin{pmatrix} p & q \\ 2q & p \end{pmatrix}$.
Therefore, $m=p$ and $n=q$. This shows that $m+n\sqrt{2} = p+q\sqrt{2}$.
Thus, φ is also one-to-one.
We conclude that $\varphi : R \to S$ is an isomorphism.

Identification "Up To Isomorphism"

- If $\varphi : R \to S$ is a monomorphism, then the subring $\varphi(R)$ of S is isomorphic to R.
- Since the rings R and $\varphi(R)$ are abstractly identical, we often wish to identify $\varphi(R)$ with R and regard R itself as a subring of S.

  Example: If S is the ring defined previously, there is a monomorphism $\theta : \mathbb{Z} \to S$ given by

$$\theta(m) = \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix}, \text{ for all } m \in \mathbb{Z}.$$

  The identification of the integer m with the 2×2 scalar matrix $\theta(m)$ allows us to consider $\mathbb{Z}$ as effectively a subring of S.

  We say that S contains $\mathbb{Z}$ **up to isomorphism**.

The Kernel of a Homomorphism

- Let $\varphi : R \to S$ be a homomorphism, where R and S are rings, with zero elements $0_R, 0_S$, respectively.
- The set
$$K = \varphi^{-1}(0_S) = \{a \in R : \varphi(a) = 0_S\}$$
is the **kernel** of the homomorphism φ, written $\ker\varphi$.
- The kernel of a homomorphism $\varphi : R \to S$ is an ideal of R.
If $a, b \in K$, then $\varphi(a) = \varphi(b) = 0_S$.
  - So certainly
  $$\varphi(a-b) = \varphi(a) - \varphi(b) = 0_S - 0_S = 0_S.$$
  Hence $a - b \in K$.
  - If $r \in R$ and $a \in K$, then
  $$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0_S = 0_S.$$
  Hence $ra \in K$.

Residue Classes Modulo an Ideal

- Let I be an ideal of a ring R, and let $a \in R$. The set

$$a + I = \{a + x : x \in I\}$$

  is called the **residue class of a modulo I**.

- We have that, for all a, b in R,

$$a + I = b + I \quad \Longleftrightarrow \quad a - b \in I.$$

  Suppose that $a + I = b + I$. Then, in particular, $a = a + 0 \in a + I = b + I$. So, there exists x in I, such that $a = b + x$. Thus, $a - b = x \in I$.

  Conversely, suppose that $a - b \in I$. Then, for all x in I, we have that $a + x = b + y$, where $y = (a - b) + x \in I$. Thus, $a + I \subseteq b + I$. The reverse inclusion is proved in the same way.

Operations on Residue Classes

- We show that, for all a, b in R,

$$(a+I)+(b+I)=(a+b)+I, \qquad (a+I)(b+I)\subseteq ab+I.$$

Let $x, y \in I$ and let $u=(a+x)+(b+y)\in(a+I)+(b+I)$. Then $u=(a+b)+(x+y)\in(a+b)+I$.

Conversely, suppose $z\in I$ and $v=(a+b)+z\in(a+b)+I$. Then $v=(a+z)+(b+0)\in(a+I)+(b+I)$.

Next, let $x, y\in I$ and let $u=(a+x)(b+y)\in(a+I)(b+I)$. Then $u=ab+(ay+xb+xy)\in ab+I$.

The Residue Class Ring

- The set R/I of all residue classes modulo I forms a ring with respect to the operations

$$(a+I)+(b+I)=(a+b)+I, \quad (a+I)(b+I)=ab+I,$$

  called the **residue class ring** modulo I.

  The zero element is $0+I=I$.

  The negative of $a+I$ is $-a+I$.

- The mapping $\theta_I : R \to R/I$, given by

$$\theta_I(a)=a+I, \quad a \in R,$$

  is a homomorphism onto R/I, with kernel I.

  It is called the **natural homomorphism** from R onto R/I.

The Ring $\mathbb{Z}_n$ of Integers mod n

- The motivating example of a residue class ring is the ring $\mathbb{Z}_n$ of integers mod n.
- The ideal is $\langle n \rangle = n\mathbb{Z}$, the set of integers divisible by n.
- The elements of $\mathbb{Z}_n$ are the classes $a + \langle n \rangle$, with $a \in \mathbb{Z}$.
- There are exactly n classes

$$\langle n \rangle,\ 1 + \langle n \rangle,\ 2 + \langle n \rangle,\ \ldots,\ (n-1) + \langle n \rangle.$$

The Field $\mathbb{Z}_n$

Theorem

Let n be a positive integer. The residue class ring $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$ is a field if and only if n is prime.

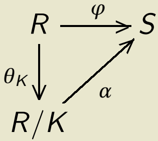
- Suppose first that n is not prime. Then $n = rs$, where $1 < r < n$ and $1 < s < n$. Then $r + \langle n \rangle \neq 0 + \langle n \rangle$ and $s + \langle n \rangle \neq 0 + \langle n \rangle$. On the other hand, $(r + \langle n \rangle)(s + \langle n \rangle) = n + \langle n \rangle = 0 + \langle n \rangle$. Thus, $\mathbb{Z}_n$ contains divisors of 0. So it is certainly not a field.

  Now let p be a prime, and suppose that $(r + \langle p \rangle)(s + \langle p \rangle) = 0 + \langle p \rangle$. Then $p \mid rs$. So (since p is prime) either $p \mid r$ or $p \mid s$. That is, either $r + \langle p \rangle = 0$ or $s + \langle p \rangle = 0$. Thus, $\mathbb{Z}_p$ has no divisors of zero. So it is an integral domain. But every finite integral domain is a field. Hence, $\mathbb{Z}_p$ is a field.

First Homomorphism Theorem

Theorem

Let R be a commutative ring, and let φ be a homomorphism from R onto a commutative ring S, with kernel K. Then, there is an isomorphism $\alpha : R/K \to S$, such that the diagram on the right commutes:



- Define α by the rule that $\alpha(a+K) = \varphi(a)$, for all $a+K \in R/K$.
  This mapping is both well-defined and injective:
  $a+K = b+K$ iff $a-b \in K$ iff $\varphi(a-b) = 0$ iff $\varphi(a) = \varphi(b)$.
  It maps onto S, since φ is onto. It is a homomorphism, since

$$\begin{aligned} \alpha((a+K)+(b+K)) &= \alpha((a+b)+K) = \varphi(a+b) \\ &= \varphi(a)+\varphi(b) = \alpha(a+K)+\alpha(b+K); \\ \alpha((a+K)(b+K)) &= \alpha(ab+K) = \varphi(ab) = \varphi(a)\varphi(b) = \alpha(a+K)\alpha(b+K). \end{aligned}$$

  Hence α is an isomorphism. The commuting of the diagram is clear, since, for all a in R, $\alpha(\theta_K(a)) = \alpha(a+K) = \varphi(a)$. So $\alpha \circ \theta_K = \varphi$.

Subsection 3

The Field of Fractions of an Integral Domain

The Equivalence Relation $\equiv$

- Let D be an integral domain. Let

$$P = D \times (D \setminus \{0\}) = \{(a,b) : a, b \in D, b \neq 0\}.$$

- Define a relation $\equiv$ on the set P by the rule that

$$(a,b) \equiv (a',b') \text{ if and only if } ab' = a'b.$$

Lemma

The relation $\equiv$ is an equivalence.

- We must prove that, for all $(a,b),(a',b'),(a'',b'')$ in P,
  (i) $(a,b) \equiv (a,b)$ (the **reflexive law**);
  (ii) $(a,b) \equiv (a',b')$ implies $(a',b') \equiv (a,b)$ (the **symmetric law**);
  (iii) $(a,b) \equiv (a',b')$ and $(a',b') \equiv (a'',b'')$ imply $(a,b) \equiv (a'',b'')$ (the **transitive law**).

The Equivalence Relation ≡ (Cont'd)

(i) Since $ab = ab$, we get $(a,b) \equiv (a,b)$.

(ii)
$$\begin{aligned}(a,b) \equiv (a',b') \quad &\text{iff} \quad ab' = a'b \\ &\text{iff} \quad a'b = ab' \\ &\text{iff} \quad (a',b') \equiv (a,b).\end{aligned}$$

(iii) From $(a,b) \equiv (a',b')$ and $(a',b') \equiv (a'',b'')$, we have that $ab' = a'b$ and $a'b'' = a''b'$. Hence,

$$b'(ab'') = (ab')b'' = a'bb'' = b(a'b'') = ba''b' = b'(a''b).$$

Since $b' \neq 0$, we can use cancelation to obtain $ab'' = a''b$.

Therefore, $(a,b) \equiv (a'',b'')$.

Operations on the Set of Equivalence Classes mod ≡

- The quotient set $P/\equiv$ is denoted by $Q(D)$.
- Its elements are equivalence classes

$$[a,b] = \{(x,y) \in P : (x,y) \equiv (a,b)\}.$$

- For reasons that will become obvious, we choose to denote the classes by fraction symbols a/b or $\frac{a}{b}$.
- Two classes are equal if their (arbitrarily chosen) representative pairs in the set P are equivalent:

$$\frac{a}{b} = \frac{c}{d} \text{ if and only if } ad = bc.$$

- In particular, note that $\frac{a}{b} = \frac{ka}{kb}$, for all $k \neq 0$ in D.
- We define **addition** and **multiplication** in $Q(D)$ by the rules

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Addition and Multiplication are Well-Defined

Lemma

Addition and multiplication in $Q(D)$ are well-defined.

- Suppose that $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$. Then $ab' = a'b$ and $cd' = c'd$. So

$$(ad + bc)b'd' = ab'dd' + bb'cd' = a'bdd' + bb'c'd = (a'd' + b'c')bd.$$

Hence,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'} = \frac{a'}{b'} + \frac{c'}{d'}.$$

Similarly,

$$(ac)(b'd') = (ab')(cd') = (a'b)(c'd) = (a'c')(bd).$$

So

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{a'c'}{b'd'} = \frac{a'}{b'} \cdot \frac{c'}{d'}.$$

The Field of Fractions $Q(D)$ of D

- These operations turn $Q(D)$ into a commutative ring with unity.

  The verifications are tedious but not difficult.

  E.g., for distributivity,

$$\begin{array}{rcl} \frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right) & = & \frac{a}{b}\cdot\frac{cf+de}{df}=\frac{acf+ade}{bdf}, \\ \frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f} & = & \frac{ac}{bd}+\frac{ae}{bf}=\frac{acbf+aebd}{b^2df}=\frac{acf+ade}{bdf}. \end{array}$$

  The zero element is $\frac{0}{1}(=\frac{0}{b}$ for all $b \neq 0$ in $D)$.

  The unity element is $\frac{1}{1}(=\frac{b}{b}$ for all $b \neq 0$ in $D)$.

  The negative of $\frac{a}{b}$ is $\frac{-a}{b}$.

  The ring $Q(D)$ is in fact a field, since for all $\frac{a}{b}$ with $a \neq 0$, we have that $\frac{a}{b}\cdot\frac{b}{a}=\frac{ab}{ab}=\frac{1}{1}$.
- The field $Q(D)$ is called the **field of fractions** of the domain D.

Embedding of D into $Q(D)$

Lemma

The mapping $\varphi : D \to Q(D)$ given by

$$\varphi(a) = \frac{a}{1}, \quad a \in D,$$

is a monomorphism.

- From the definition of the operations on $Q(D)$,

$$\begin{aligned} \varphi(a) + \varphi(b) &= \tfrac{a}{1} + \tfrac{b}{1} = \tfrac{a+b}{1} = \varphi(a+b); \\ \varphi(a)\varphi(b) &= \tfrac{a}{1} \cdot \tfrac{b}{1} = \tfrac{ab}{1} = \varphi(ab). \end{aligned}$$

  Also,

$$\varphi(a) = \varphi(b) \ \Rightarrow \ \frac{a}{1} = \frac{b}{1} \ \Rightarrow \ a = b.$$

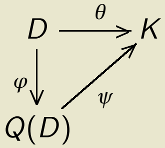
  Identifying $\frac{a}{1}$ with a, we can regard D as a subring of $Q(D)$.

Minimality of $Q(D)$

- The field $Q(D)$ is the smallest field containing D.

Theorem

Let D be an integral domain, let φ be the monomorphism from D into $Q(D)$ and let K be a field with the property that there is a monomorphism θ from D into K. Then, there exists a monomorphism $\psi : Q(D) \to K$ such that the diagram commutes:



- Define a mapping $\psi : Q(D) \to K$ by the rule that $\psi(\frac{a}{b}) = \frac{\theta(a)}{\theta(b)}$. Here $\theta(b) \neq 0$, since θ is a monomorphism. This is well-defined and one-to-one, since

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc \Leftrightarrow \theta(a)\theta(d) = \theta(b)\theta(c) \Leftrightarrow \frac{\theta(a)}{\theta(b)} = \frac{\theta(c)}{\theta(d)}.$$

Minimality of $Q(D)$ (Cont'd)

- It is a homomorphism, since

$$\begin{aligned}
\psi\left(\tfrac{a}{b}+\tfrac{c}{d}\right) &= \psi\left(\tfrac{ad+bc}{bd}\right)=\tfrac{\theta(ad+bc)}{\theta(bd)}=\tfrac{\theta(a)\theta(d)+\theta(b)\theta(c)}{\theta(b)\theta(d)} \\
&= \tfrac{\theta(a)}{\theta(b)}+\tfrac{\theta(c)}{\theta(d)}=\psi\left(\tfrac{a}{b}\right)+\psi\left(\tfrac{c}{d}\right); \\
\psi\left(\tfrac{a}{b}\cdot\tfrac{c}{d}\right) &= \psi\left(\tfrac{ac}{bd}\right)=\tfrac{\theta(ac)}{\theta(bd)}=\tfrac{\theta(a)\theta(c)}{\theta(b)\theta(d)} \\
&= \tfrac{\theta(a)}{\theta(b)}\cdot\tfrac{\theta(c)}{\theta(d)}=\psi\left(\tfrac{a}{b}\right)\cdot\psi\left(\tfrac{c}{d}\right).
\end{aligned}$$

  The commuting of the diagram is clear, since, for all a in D,

$$\psi(\varphi(a))=\psi\left(\frac{a}{1}\right)=\frac{\theta(a)}{\theta(1)}=\theta(a).$$

- When $D=\mathbb{Z}$, it is clear that $Q(D)=\mathbb{Q}$.

Subsection 4

The Characteristic of a Field

Multiples of Ring Elements

- In a ring R containing an element a, we denote $a+a$ by $2a$.
- More generally, if n is a natural number, we write na for the sum

$$\underbrace{a+a+\cdots+a}_{n \text{ summands}}.$$

- If we define $0a=0_R$ and $(-n)a$ to be $n(-a)$, we can give a meaning to na for every integer n.
- For $m,n\in\mathbb{Z}$ and $a,b\in R$, we have
  - $(m+n)a=ma+na$;
  - $m(a+b)=ma+mb$;
  - $(mn)a=m(na)$;
  - $m(ab)=(ma)b=a(mb)$;
  - $(ma)(nb)=(mn)(ab)$.

The Characteristic of a Ring

- Let R be a commutative ring with unity element 1_R.
  Then there are two possibilities:
  (i) The elements $m1_R$ $(m=1,2,\ldots)$ are all distinct;
  (ii) There exist m,n in $\mathbb{N}$, such that $m1_R=(m+n)1_R$.
- In the former case we say that R has **characteristic** zero, and write $\operatorname{char} R=0$.
- In the latter case, $m1_R=(m+n)1_R=m1_R+n1_R$. So $n1_R=0_R$.
  The least positive n for which this holds is called the **characteristic** of the ring R and we write $\operatorname{char} R=n$.
- Note that, if R is a ring of characteristic n, then, for all a in R,

$$na=(n1_R)a=0_Ra=0_R.$$

The Case of a Field

Theorem

The characteristic of a field is either 0 or a prime number p.

- The former possibility can certainly occur.

  $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all fields of characteristic 0.

  Let K be a field and suppose that $\text{char} K = n \neq 0$, where n is not prime.

  Then $n = rs$, where $1 < r < n$ and $1 < s < n$.

  The minimal property of n implies $r1_K \neq 0_K$ and $s1_K \neq 0_K$.

  On the other hand,

  $$(r1_K)(s1_K) = (rs)1_K = n1_K = 0_K.$$

  But this is impossible, since K, being a field, has no zero divisors.

The Prime Subfield

- Let K be a field with characteristic 0.
- The elements $n1_K$, $n \in \mathbb{Z}$, are all distinct, and form a subring of K isomorphic to $\mathbb{Z}$.
- The set
$$P(K) = \left\{ \frac{m1_K}{n1_f} : m, n \in \mathbb{Z}, n \neq 0 \right\}$$
is a subfield of K isomorphic to $\mathbb{Q}$.
- Any subfield of K must contain 1 and 0 and so must contain $P(K)$.
- $P(K)$ is called the **prime subfield** of K.
- If K has prime characteristic p, the prime subfield is
$$P(K) = \{1_K, 2(1_K), \ldots, (p-1)(1_K)\}.$$
- In this case $P(K)$ is isomorphic to $\mathbb{Z}_p$.

Characterizing the Prime Subfield

Theorem

Let K be a field. Then K contains a prime subfield $P(K)$ contained in every subfield.

- If $\text{char} K = 0$, then $P(K)$ is isomorphic to $\mathbb{Q}$.
- If $\text{char} K = p$, a prime number, then $P(K)$ is isomorphic to $\mathbb{Z}_p$.

- The fields $\mathbb{Q}$ and $\mathbb{Z}_p$ play a central role in the theory of fields.
- They have no proper subfields, and every field contains as a subfield an isomorphic copy of one or other of them.
- We express this by saying:
  - Every field of characteristic 0 is an **extension** of $\mathbb{Q}$;
  - Every field of prime characteristic p is an **extension** of $\mathbb{Z}_p$.

The Expression a/n

- Given an element a of a field K, we sometimes like to denote $\frac{a}{n1}$ simply by $\frac{a}{n}$.
  - If $\text{char} K = 0$, this is no problem;
  - If $\text{char} K = p$, then we cannot assign a meaning to $\frac{a}{n}$, if n is a multiple of p.

Example: The formula

$$xy = \frac{1}{4}\left((x+y)^2 - (x-y)^2\right)$$

is not valid in a field of characteristic 2, since the quantity on the right reduces to $\frac{0}{0}$ and so is undefined.

Power of Sum in Characteristic p

Theorem

Let K be a field of characteristic p. Then, for all x, y in K,

$$(x+y)^p = x^p + y^p.$$

- By the binomial theorem, valid in any commutative ring with unity, we have that

$$(x+y)^p = \sum_{r=0}^{p} \binom{p}{r} x^{n-r} y^r.$$

For $r = 1, \ldots, p-1$, the coefficient $\binom{p}{r} = \frac{p(p-1)\cdots(p-r+1)}{r!}$ is an integer. So $r!$ divides $p(p-1)\cdots(p-r+1)$. Since p is prime and $r < p$, no factor of $r!$ can divide p. Hence, $r!$ divides $(p-1)\cdots(p-r+1)$. So $\binom{p}{r}$ is an integer divisible by p. Thus,, for $r = 1, \ldots, p-1$, $\binom{p}{r} x^{n-r} y^r = 0$. So, in $(x+y)^p = \sum_{r=0}^{p} \binom{p}{r} x^{n-r} y^r$, only the first and last terms survive.

Representation of Elements in $\mathbb{Z}_p$

- The fields $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$ are important building blocks in field theory.
- We usually find it convenient to write $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, with addition and multiplication carried out modulo p.
- For example, the multiplication table for $\mathbb{Z}_5$ is

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

	0	1	2	−2	−1
0	0	0	0	0	0
1	0	1	2	−2	−1
2	0	2	−1	1	−2
−2	0	−2	1	−1	2
−1	0	−1	−2	2	1

- Occasionally, it is more convenient to write $\mathbb{Z}_3 = \{0, 1, -1\}$.
- Similarly, we may write $\mathbb{Z}_5 = \{0, \pm 1, \pm 2\}$, obtaining the table on the right.

Subsection 5

Reminder of Some Group Theory

Groups, Abelian Groups and Finite Groups

- A **group** $G = (G, \cdot)$ is a non-empty set furnished with a binary operation $\cdot$ with the following properties:
  - (G1) **The associative law**: $(ab)c = a(bc)$, for all $a, b, c \in G$;
  - (G2) **The existence of an identity element**: there exists e in G, such that, for all a in G, $ea = a$;
  - (G3) **The existence of inverses**: for all a in G, there exists a^{-1} in G, such that $a^{-1}a = e$.
- An **abelian group** has an additional property:
  - (G4) **The commutative law**: $ab = ba$, for all $a, b \in G$.
- The element e and the element a^{-1} are both unique, and
$$ae = ea = a, \qquad aa^{-1} = a^{-1}a = e.$$
- For all $a, b \in G$,
$$(ab)^{-1} = b^{-1}a^{-1}.$$
- The group $(G, \cdot)$ is called a **finite group** if the set G is finite.
- The cardinality $|G|$ of G is called the **order** of the group.

Cyclic Groups

- We write $a^2, a^3, \ldots$, where $a \in G$, for the products $aa, aaa, \ldots$.
- We write a^{-n} to mean $(a^{-1})^n = (a^n)^{-1}$.
- By a^0 we mean the identity element e.
- A group G is called **cyclic** if there exists an element a in G such that

$$G = \{a^n : n \in \mathbb{Z}\}.$$

  - If the powers a^n are all distinct, G is the **infinite cyclic group**.
  - Otherwise, there is a least $m > 0$, such that $a^m = e$.
    Given $n \in \mathbb{Z}$, the division algorithm gives integers q and r, such that $n = qm + r$ and $0 \le r \le m - 1$.
    Therefore, $a^n = a^{qm+r} = (a^m)^q a^r = a^r$.
    Thus, $G = \{e, a, a^2, \ldots, a^{m-1}\}$, the **cyclic group of order** m.
- Both the infinite cyclic group and the cyclic group of order m are abelian.

Subgroups and Orders of Elements

- A non-empty subset U of G is called a **subgroup** of G if, for all $a, b \in G$,
$$a, b \in U \quad \text{implies} \quad ab \in U;$$
$$a \in U \quad \text{implies} \quad a^{-1} \in U;$$
or, equivalently,
$$a, b \in U \quad \text{implies} \quad ab^{-1} \in U.$$
- Every subgroup contains the identity element e.
- For each element a in the group G, the set $\{a^n : n \in \mathbb{Z}\}$ is a subgroup, called the **cyclic subgroup generated by** a, and denoted by $\langle a \rangle$.
- If G is finite, $\langle a \rangle$ cannot be the infinite cyclic group.
- The order of $\langle a \rangle$ is called the **order of the element** a.
- The order of a is the smallest positive integer n, such that $a^n = e$, and is denoted by $o(a)$.

Left Cosets and Lagrange's Theorem

- Let U be a subgroup of a group G and let $a \in G$.
- The subset
$$Ua = \{ua : u \in U\}$$
is called a **left coset** of U.
- We have $Ua = Ub$ if and only if $ab^{-1} \in U$.
Suppose $Ua = Ub$. Then, there exist $u_1, u_2 \in U$, such that $u_1 a = u_2 b$. So $ab^{-1} = u_1^{-1} u_2 \in U$. Conversely, suppose $ab^{-1} \in U$. If $u \in U$, then:
  - $ua = ua(b^{-1}b) = u(ab^{-1})b \in Ub$. So $Ua \subseteq Ub$.
  - $ub = ub(a^{-1}a) = u(ab^{-1})^{-1}a \in Ua$. So $Ub \subseteq Ua$.
- Among the left cosets is U itself.
This is clear, since $Ue = U$.
- The distinct left cosets form a partition of G, i.e., every element of G belongs to exactly one left coset of U.
Indeed, suppose $c \in Ua \cap Ub$. Then, there exist $u_1, u_2 \in U$, such that $c = u_1 a = u_2 b$. Thus, $ab^{-1} = u_1^{-1} u_2 \in U$. Therefore, $Ua = Ub$.

Left Cosets and Lagrange's Theorem

Theorem (Lagrange's Theorem)

If U is a subgroup of a finite group G, then $|U|$ divides $|G|$.

- The mapping U into Ua; $u \mapsto ua$, is one-one and onto.
  So, in a finite group, every left coset has $|U|$ elements.
  Thus, $|G| = |U| \times$ (the number of left cosets).
- It follows that, for all a in G, the order of a divides the order of G.

Index and Normal Subgroups

- Exactly the same thing can be done with **right cosets** aU.
- The right coset aU and the left coset Ua may not be identical, but the number of right cosets is the same as the number of left cosets.
- This number is called the **index** of the subgroup.
- U is a **normal subgroup** of G, writtten $U \trianglelefteq G$, if $Ua = aU$ for all a.
- U is normal if and only if, for all a in G, $a^{-1}Ua = U$.

  Suppose, first, that $Ua = aU$, for all a. Let $u \in U$.
  - There exists $u' \in U$, such that $au = u'a$. So $u = a^{-1}u'a \in a^{-1}Ua$. So $U \subseteq a^{-1}Ua$.
  - There exists $u' \in U$, such that $ua = au'$. So $a^{-1}ua = a^{-1}au' = u' \in U$. So $a^{-1}Ua \subseteq U$.

  Assume, conversely, $a^{-1}Ua = U$, for all a. Let $u \in U$.
  - There exists $u' \in U$, such that $a^{-1}ua = u'$. So $ua = aa^{-1}ua = au' \in aU$. So $Ua \subseteq aU$.
  - There exists $u' \in U$, such that $u = a^{-1}u'a$. So $au = aa^{-1}u'a = u'a \in Ua$. So $aU \subseteq Ua$.

Quotient Groups

- Given a group G, if $U \trianglelefteq G$, we can define a group operation on the set of cosets of U:
$$(Ua)(Ub) = U(ab).$$
This is well-defined.
For all u, v in U,
$$\begin{array}{rcl} (ua)(vb) & = & u(av)b \\ & = & u(v'a)b \quad \text{(for some } v' \text{ in } U\text{, since } U \text{ is normal)} \\ & = & (uv')(ab) \in U(ab). \end{array}$$
Associativity is clear.
The identity of the group is the coset $U = Ue$.
The inverse of Ua is Ua^{-1}.
- The group is denoted by G/U, and is called the **quotient group**, or the **factor group**, of G by U.

Homomorphisms and Natural Homomorphisms

- Let G, H be groups, with identity elements e_G, e_H, respectively.

  A mapping $\varphi : G \to H$ is called a **homomorphism** if, for all $a, b \in G$,

  $$\varphi(ab) = \varphi(a)\varphi(b).$$

- If $\varphi : G \to H$ is a homomorphism:
  - $\varphi(e_G) = e_H$;
  - $\varphi(a^{-1}) = (\varphi(a))^{-1}$, for all a in G.
- If N is a normal subgroup of G, the mapping $\nu_N : G \to G/N$, given by

  $$\nu_N(a) = Na, \quad a \in G,$$

  is a homomorphism.

  It is called the **natural homomorphism**, onto G/N.

Isomorphisms and Homomorphic Images

- If a homomorphism $\varphi : G \to H$ is one-one and onto, we say that it is an **isomorphism**.
- In such a case $\varphi^{-1} : H \to G$ is also an isomorphism, and we say that H is **isomorphic** to G, writing $H \cong G$.
- If φ maps onto H, but is not necessarily one-one, we say that H is a **homomorphic image** of G.

Kernels and First Homomorphism Theorem

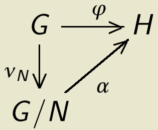
- Let $\varphi : G \to H$ be a homomorphism.
- The **kernel** $\ker\varphi$ of φ is defined by

$$\ker\varphi = \varphi^{-1}(e_H) = \{a \in G : \varphi(a) = e_H\}.$$

- $\ker\varphi$ is a normal subgroup of G.
- Every homomorphic image of G is isomorphic to a quotient group of G by a suitable normal subgroup.

Theorem

Let G, H be groups, and let φ be a homomorphism from G onto H, with kernel N. Then there exists a unique isomorphism $\alpha : G/N \to H$, such that the diagram comutes:



- The mapping $\alpha : Na \mapsto \varphi(a)$ is well-defined, one-one, onto, and a homomorphism. Moreover, $\alpha \circ \nu_N = \varphi$.