MTH4104 Cheat Sheet

Shu Sasaki

25th March 2024

1 Chapter 2 and Chapter 3 (Week 1-3)

GOAL: Get used to an axiomatic approach to mathematics– given definitions/axioms, derive general statements about integers (that we know too well) via proofs and careful inspection of definitions etc.

Proposition 1. Let a and b be integers and suppose $b > 0$. Then $a = bq + r$ for some integers q and $0 \leq r < b$. The pair (q, r) is unique.

Definition. Let a and b be integers. We say that a divides b if there exists an integer c such that $b = ac$.

Remark. The only integer 0 divides is 0 itself.

Definition. Let a and b be integers. A common divisor of a and b is a non-negative integer s such that s divides both a and b. A gcd of a and b is the common divisor r satisfying the property that if s is another (different) common divisor of a and b, then $s < r$.

Proposition 2. s divides r.

We can say something similar for the lcm of a and b.

Proposition 4. If a is a non-negative integer, $\gcd(a, 0) = a$. This is not a definition.

Lemma 5. $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$. This is not a definition.

Theorem 7 (Bezout's identity). Let a and b be integers. Then there exist integers r and s such that $ar + bs = \gcd(a, b)$.

The proof of Bezout explains only that these integers r and s exist and does not shed any light on how to actually find them. In practice, we make appeal to Euclid's algorithm instead.

Euclid's algorithm is based on the following proposition:

Proposition 6. Let a and b be integers. Suppose $b > 0$. By Proposition 1, there exists a uniqe pair of integers q and $0 \le r < b$ such that $a = bq + r$. Then $\gcd(a, b) = \gcd(b, r)$.

How do we use Euclid's algorithm to find r and s satisfying $ar + bs = \gcd(a, b)$?

(NON-EXAMINABLE) If your Euclid's algorithm looks like:

$$\begin{array}{rrcl} & & \vdots & \\ (s_n) & r_{n-2} & = & r_{n-1}q_n + r_n \\ (s_{n+1}) & r_{n-1} & = & r_n q_{n+1} + r_{n+1} \\ & & \vdots & \\ (s_N) & r_{N-1} & = & r_N q_{N+1} + r_{N+1} \\ (s_{N+1}) & r_N & = & r_{N+1} q_{N+2} \end{array}$$

then we know that $\gcd(a, b)$ is r_{N+1}, because we may repeat Proposition 6 to deduce that

$$\gcd(a, b) = \cdots = \gcd(r_{n-2}, r_{n-1}) \overset{(s_n)}{=} \gcd(r_{n-1}, r_n) \overset{(s_{n+1})}{=} \gcd(r_n, r_{n+1}) = \cdots = \\ \gcd(r_{N-1}, r_N) \overset{(s_N)}{=} \gcd(r_N, r_{N+1}) \overset{(s_{N+1})}{=} r_{N+1}.$$

We also see from (s_N) that $r_{N+1} = -q_{N+1}r_N + r_{N-1}$. Indeed, for every n (e.g. $N, N-1, \ldots$), there exist integers X_n and Y_n satisfying

$$r_{N+1} = X_n r_n + Y_n r_{n-1}.$$

This will find us r and s such that $ar + bs = r_{N+1}$.

We may prove the assertion by induction 'in reverse' (one can reindex all to make this rigorous). We saw $(X_N, Y_N) = (-q_N, 1)$ does the job. Supposing that there exist integers X_n and Y_n such that

$$r_{N+1} = X_n r_n + Y_n r_{n-1},$$

we aim at proving that there exists X_{n-1} and Y_{n-1} such that

$$r_{N+1} = X_{n-1} r_{n-1} + Y_{n-1} r_{n-2}.$$

We will spell out X_{n-1} and Y_{n-1} in terms of X_n and Y_n. To see this, plug $r_n = (-q_n)r_{n-1} + r_{n-2}$ obtained from (s_n) into $r_{N+1} = X_n r_n + Y_n r_{n-1}$. We then get

$$r_{N+1} = X_n((-q_n)r_{n-1} + r_{n-2}) + Y_n r_{n-1} = (-q_n X_n + Y_n)r_{n-1} + X_n r_{n-2},$$

hence $(X_{n-1}, Y_{n-1}) = (-q_n X_n + Y_n, X_n)$ does the job. It is possible to use this inductively (as n decreases) to find X's and Y's, starting with $(X_N, Y_N) = (-q_N, 1)$.

Definition. A prime number is a positive integer n whose positive integer divisor is 1 or itself. Alternatively, we may define it as a positive integer whose integer divisors are $\{\pm 1, \pm n\}$.

By Bezout, this is equivalent to the following: if a and b are integers and n divides ab, then n divides either a or b. The latter definition allows us to prove:

Theorem 8 (the Fundamental Theorem of Arithmetic). Every integer is of the form

$$(-1)^{r_\infty} \prod_p p^{r_p}$$

for some non-negative integers r_∞ and r_p, up to reordering of prime factors. The power r_p is the maximum number of time p divides the integer. For example, $45 = 3^2 \cdot 5$ so $r_p = 0$ if p is not 3 nor 5, $r_3 = 2, r_5 = 1$ and $r_\infty = 0$.

Let $\mathcal{R}$ be a relation on S. We let $[a] = [a]_{\mathcal{R}}$ denote the subset of all b in S which are related to a, i.e. $a\mathcal{R}b$. If $\mathcal{R}$ is an equivalence relation (satisfying a set of conditions), then

$$a\mathcal{R}b \text{ if and only if } [a] = [b].$$

Theorem 9. Given a set S, there exists a bijective correspondence between

- the equivalence relations $\mathcal{R}$ on S,
- the partitions $\mathcal{P}$ (a set of subsets of S satisfying certain conditions) on S.

Proposition 10. Let n be a positive integer. Then $(\mathcal{R}, S) = (\equiv \mathbb{Z})$, defined such that $a \equiv b$ mod n if and only if n divides $b - a$ (for integers a and b), is an equivalence relation.

Definition. Let $\mathbb{Z}_n$ denote the set of equivalence classes $[a]$ with respect to $(\equiv, \mathbb{Z})$.

Since $a \equiv b$ mod n if and only if $[a] = [b]$, a lot of equivalence classes may be identified. Indeed,

Proposition 11. $|\mathbb{Z}_n| = n$.

Proposition 1 proves Proposition 11. Indeed, if a is an integer (n is, by definition, a positive integer), then there exists q and $0 \leq r < n$ such that $a = nq + r$. Therefore $a \equiv r$, i.e. $[a] = [r]$. The proof also elaborates that $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$. The element $[r]$ is nothing other than the set of integers b with remainder r when divided by n (i.e. $b \equiv r$ mod n).

On $\mathbb{Z}_n$, we define $+, -, \times$:

$$\begin{aligned} [a] + [b] &= [a+b] \\ [a] - [b] &= [a-b] \\ [a][b] &= [ab] \end{aligned}$$

but no division. These do not depend on choice of representatives, i.e. if $a \equiv a'$ mod n, then $[a] + [b] = [a'] + [b]$ etc.

No division is defined but:

Definition. We say that $[a]$ of $\mathbb{Z}_n$ has multiplicative inverse if there exists an integer b such that $[a][b] = [1]$ (or equivalently $ab \equiv 1$ mod n). This plays the role of $1/[a]$ but not literally ($1/[a]$ or $[1/a]$ simply does not make sense!). The multiplicative inverse is often written as $[a]^{-1}$.

Remark. The multiplicative inverse, if exists, is unique. Suppose that $[b]$ and $[c]$ are elements of $\mathbb{Z}_n$ such that $[a][b] = [1]$ and $[a][c] = [1]$. Multiplying both sides of $[c][a] = [1]$ by $[b]$, we obtain $[c][a][b] = [1][b]$, i.e. $[c] = [b]$.

Theorem 12. An element $[a]$ of $\mathbb{Z}_n$ has multiplicative inverse if and only if $\gcd(a, n) = 1$.

The proof explains how to find the multiplicative inverse explicitly. If a is an integer such that $\gcd(a, n) = 1$ (which one can check in practice by Euclid's algorithm), Euclid's algorithm finds integers b and c such that $ab + nc = \gcd(a, n) = 1$. It then follows that $ab \equiv 1 \bmod n$, i.e. $[a][b] = [ab] = [1]$.

Proposition 13. An element $[a]$ of $\mathbb{Z}_n$ has no multiplicative inverse if and only if there exists b, not congruent to 0 mod n, such that $[a][b] = [0]$.

Example. $[2]_6[3]_6 = [0]_6$.

It is possible to compute the number of elements in $\mathbb{Z}_n$ with multiplicative inverses, using the fundamental theorem of arithmetic: if $= \prod\limits_p p^{r_p}$, then it is computed by $\prod_p (p-1)p^{r_p - 1}$.

What is it useful for? It is possible to solve 'linear congruence equations': $ax + b \equiv c \bmod n$ (when $\gcd(a, n) = 1$). Indeed, $[x] = [c - b][a]^{-1}$ where $[a]^{-1}$ is the multiplicative inverse of $[a]$ (this is NOT $1/[a]$). What if $\gcd(a, n) > 1$? Take Number Theory next year!

2 Chapter 4

Goal. Understand axioms of groups, ring and fields, together with their elementary properties. Wrap your head around the idea that $+$ and $\times$ are just operations that satisfy axioms.

Definition. A group is a set G with an operation $*$ on G satisfying the following axioms:

(G0) If a, b are elements of G, then $a * b$ is an element of G.

(G1) If a, b, c are elements of G, then $a * (b * c) = (a * b) * c$.

(G2) There is an element e in G (called the identity element) such that $a * e = e * a = a$ for every element of G.

(G3) For every element a of G, there exists b in G such that $a * b = b * a = e$. The element b is called the inverse of a.

(G4) If a, b are elements of G, then $a * b = b * a$.

When these five conditions hold, we say $(G, *)$ (or simply G if the operation $*$ is clear from the context) is a commutative/abelian group. By groups, I shall mean abelian groups unless otherwise specified.

Example. Let S be a non-empty set. Let Sym(S) be the set of *bijective* functions $a : S \to S$ and $*$ be the composition $\circ$– if a and b are elements of G, then $a \circ b$ is the composite $S \xrightarrow{b} S \xrightarrow{a} S$ sending s to $a(b(s))$. Then $(\mathrm{Sym}(S), \circ)$ is a group.

Proposition 14. Let $(G, *)$ be a group.

- The identity element of G is unique.
- Each element a of G has a unique inverse (written multiplicatively as a^{-1}).
- If $a * b = a * c$, then $b = c$. Similarly, if $b * a = c * a$, then $b = c$.
- For any a, b in G, then $(a * b)^{-1} = b^{-1} * a^{-1}$.

Definition. A ring is a set R which comes equipped with two operations, $+$ (addition) and $\times$ (multiplication), satisfying the following axioms:

(R+0) If a, b are elements of R, then $a + b$ is an element of R.

(R+1) If a, b, c are elements of R, then $a + (b + c) = (a + b) + c$.

(R+2) There is an element 0 in R such that $a+0 = 0+a = a$ for every element of R– the element is sometimes referred to as the additive identity element, or the identity element with respect to $+$/addition.

(R+3) For every element a of R, there exists b in G such that $a + b = b + a = 0$.

(R+4) If a, b are elements of R, then $a + b = b + a$.

(R×0) If a, b are elements of R, then $a \times b$ is an element of R.

(R×1) If a, b, c are elements of R, then $a \times (b \times c) = (a \times b) \times c$.

(R×+) If a, b, c are elements of R, then

$$a \times (b + c) = a \times b + a \times c.$$

(R+×) If a, b, c are elements of R, then

$$(b + c) \times a = b \times a + c \times a.$$

Remark. The first five axioms say that $(G, *) = (R, +)$ is an additive (abelian) group.

Remark. As seen in groups, the operations $+$ and $\times$ are just symbols/names given to operations that satisfy a bunch of conditions that pin down $+$ and $\times$ on $\mathbb{Z}$ (it is precisely for this reason that the symbols '+' and '×' are used conventionally). See examples below.

Remark. We often write ab instead of $a \times b$.

Definition. A ring R is said to be a commutative ring if $a \times b = b \times a$ holds for all a, b in R.

Example. The set of 2-by-2 matrices with entries in the real numbers $\mathbb{R}$ is a non-commutative ring. For example, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ but $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. The non-commutativity holds more generally (see Proposition 35).

Proposition 15. Let $(R, +, \times)$ be a ring.

- There is a unique zero element,
- Any element has a unique additive inverse.
- If $a + b = a + c$, then $b = c$.

Proposition 16. Let R be a ring. For every element a of R, we have $0a = a0 = 0$.

Definition. Let R be a ring. If R has an element 1 (the multiplicative identity element) such that, for every a in R, we have $a \times 1 = 1 \times a = a$, then we say R is a ring with identity (commonly understood as *multiplicative* identity). The additive identity 0 and the multiplicative identity (if exists) do not have to be distinct.

Theorem 17. The set $\mathbb{Z}_n$, with addition and multiplication modulo n as defined before, is a commutative ring with identity [1].

Examples (of rings without identity).
- The set of even integers is a ring (with respect to usual $+$ and $\times$) without identity– the set of odd integers is not even a ring!
- Let R be the set of continuous functions $f : \mathbb{R} \to \mathbb{R}$ such that $\int_0^\infty f < \infty$. This is a ring. However, the identity function 1 is not an element of R as $\int_0^\infty 1 = \infty$.
- A group $(G, *)$ with trivial multiplication is not a ring with identity, unless $G = \{e\}$.

Definition. Let R be a ring with identity element 1. An element a in R is called a unit if there is an element b in R such that $ab = ba = 1$. The element b is called the inverse of b, and is written as a^{-1}.

Remark. If R is a ring with identity, an element a is a unit if and only if a has multiplicative inverse. To put it another way,

$$\{\text{units in } R\} = \{\text{elements in } R \text{ with multiplicative inverses}\}.$$

Definition. We will denote by $R^\times$ the units of R.

Proposition 18. The units of $\mathbb{Z}_n$ are the subset of equivalence classes $[a]$ in $\mathbb{Z}$ represented by integers a such that $\gcd(a, n) = 1$. Furthermore, $|\mathbb{Z}_n| = \phi(n)$.

The following proposition puts together some of the key properties of the multiplicative identity 1.

Proposition 19. Let R be a ring with (multiplicative) identity 1.

- The identity element 1 is unique.
- If 1 is distinct from the additive identity 0, then 0 is NOT a unit.
- 1 is a unit and its inverse is 1 itself.

Proposition 20. Let R be a ring with (multiplicative) identity 1.

- If a is a unit, the inverse of a is unique.
- If a is a unit, then so is a^{-1}– the inverse of a^{-1} is indeed a.
- If a and b are units, then so is ab; and its inverse is $b^{-1}a^{-1}$.

The frequency with which the proof of Proposition 14 was useful in proving statements in the propositions is suggestive of:

Theorem 21. If $(R, +, \times)$ is a ring with identity, $(R^{\times}, \times)$ is a group. If, furthermore, $(R, +, \times)$ is commutative, $(R^{\times}, \times)$ is abelian.

Example. Let $(\mathbb{Z}, +, \times)$ be the ring of integers with usual addition $+$ and multiplication $\times$. Define new addition $\boxplus$:

$$a \boxplus b = a + b + 1$$

and new multiplication

$$a \boxtimes b = a + b + ab$$

in terms of old $+$ and $\times$. Then this is a commutative ring with identity, where the zero identity (the identity element with respect to addition, as prescribed by (R+2)) is -1 and the multiplicative identity is 0!

Checking why this is true involves a lot of work:

- (R+0) Since $a + b + 1 \in \mathbb{Z}$, we have $a \boxplus b = a + b + 1 \in \mathbb{Z}$.

- (R+1) On one hand,

$$a \boxplus (b \boxplus c) = a \boxplus (b + c + 1) = a + (b + c + 1) + 1 = a + b + c + 1.$$

On the other hand,

$$(a \boxplus b) \boxplus c = (a + b + 1) \boxplus c = (a + b + 1) + c + 1 = a + b + c + 1.$$

Therefore

$$a \boxplus (b \boxplus c) = (a \boxplus b) \boxplus c.$$

- (R+2) (-1) is the identity element with respect to $\boxtimes$. Indeed,

$$a \boxplus (-1) = a + (-1) + 1 = a$$

and

$$(-1) \boxplus a = (-1) + a + 1 = a.$$

[To find the identity, we need to find b in $\mathbb{Z}$ such that $a \boxplus b = a$ holds for any a. By definition, this is equivalent to finding b satisfying $a + b + 1 = a$, i.e. $b + 1 = 0$. Therefore $b = -1$.]

- (R+3) The inverse of a with respect to $\boxplus$ is $-a - 2$. Indeed,

$$a \boxplus (-a - 2) = a + (-a - 2) + 1 = -1$$

and

$$(-a - 2) \boxplus a = (-a - 2) + a + 1 = -1.$$

[To find the inverse of a, we need to find b such that $a \boxplus b = -1$ (since -1 is the identity with respect to $\boxplus$!) for example. This is equivalent to $a + b + 1 = -1$, i.e., $b = -a - 2$.]

- (R+4)

$$a \boxplus b = a + b + 1 = b + a + 1 = b \boxplus a.$$

- (R×0) Since $a + b + ab \in \mathbb{Z}$, we have $a \boxtimes b = a + b + ab \in \mathbb{Z}$.

- (R× 1) On one hand,

$$a \boxtimes (b \boxtimes c) = a \boxtimes (b + c + bc) = a + (b + c + bc) + a(b + c + bc).$$

On the other hand,

$$(a \boxtimes b) \boxtimes c = (a + b + ab) \boxtimes c = (a + b + ab) + c + (a + b + ab)c.$$

It follows from (R+4), (R×1), (R×+) and (R+×) for $(\mathbb{Z}, +, \times)$ that

$$a \boxtimes (b \boxtimes c) = (a \boxtimes b) \boxtimes c.$$

- (R×+) On one hand,

$$a \boxtimes (b \boxplus c) = a \boxtimes (b + c + 1) = a + (b + c + 1) + a(b + c + 1).$$

On the other hand,

$$(a \boxtimes b) \boxplus (a \boxtimes c) = (a + b + ab) \boxplus (a + c + ac) = (a + b + ab) + (a + c + ac) + 1.$$

It then follows from (R+4), (R×+) and (R+×) for $(\mathbb{Z}, +, \times)$ that

$$a \boxtimes (b \boxplus c) = (a \boxtimes b) \boxplus (a \boxtimes c).$$

- (R+×) On one hand,

$$(b \boxplus c) \boxtimes a = (b + c + 1) \boxtimes a = (b + c + 1) + a + (b + c + 1)a.$$

On the other hand,

$$(b \boxtimes a) \boxplus (c \boxtimes a) = (b + a + ba) \boxplus (c + a + ca) = (b + a + ba) + (c + a + ca) + 1.$$

It then follows from (R+4), (R×+) and (R+×) for $(\mathbb{Z}, +, \times)$ that

$$(b \boxplus c) \boxtimes a = (b \boxtimes a) \boxplus (c \boxtimes a).$$

- $(\mathbb{Z}, \boxplus, \boxtimes)$ is commutative. Since $(\mathbb{Z}, +, \times)$ is a commutative ring,

$$a \boxtimes b = a + b + ab = b + a + ba = b \boxtimes a.$$

- The multiplicative identity with respect to $\boxtimes$ is 0. Indeed,

$$a \boxtimes 0 = a + 0 + a0 = a$$

and

$$0 \boxtimes a = 0 + a + 0a = a.$$

[To find this, we need to find b in $\mathbb{Z}$ such that $a \boxtimes b = a$ holds for every a. This is equivalent to finding b satisfying $a + b + ab = a$, i.e. $b(1 + a) = 0$, holds for every a. Therefore $b = 0$.]

The units of $(\mathbb{Z}, \boxplus, \boxtimes)$ are $\{0, -2\}$. To see this, we need to find integers a (and b) such that $a \boxtimes b = 0$, i.e. $a + b + ab = 0$. This is equivalent to $(a+1)(b+1) = -1$. Therefore, $(a+1, b+1)$ is either $(1, -1)$ or $(-1, 1)$. In other words, (a, b) is either $(0, -2)$ or $(-2, 0)$.

Definition. A field is a *commutative* ring $(F, +, \times)$ satisfying the axioms

- $(F, +)$ is an (abelian) additive group (with identity element 0)
- $(F - \{0\}, \times)$ is a multiplicative group (with identity element 1). Since $(F, +, \times)$ is assumed to be commutative, $(F - \{0\}, \times)$ is necessarily an abelian multiplicative group.
- The additive identity '0' (the identity element in the group $(F, +)$) is distinct from the multiplicative identity '1' (the identity element in the group $(F - \{0\}, \times)$).

Remark. If $1 = 0$, then $a = 1 \times a = 0 \times a = 0$ (the last equality needs to be justified; see Proposition ?). So the condition $1 \neq 0$ denies any set with one element $\{1 = 0\}$ any chance of being a field.

Remark. By definition,

$$\text{Field} \Rightarrow \text{Ring} \Rightarrow \text{Group}$$

Remark. Groups encapsulate 'symmetry'. Why rings (and not fields)? In general, elements of a ring do not have (multiplicative) inverses and this is not a bad things and this actually makes rings interesting. For example, the division algorithm would be vacuous if everything in $\mathbb{Z}$ had an inverse (i.e. is divisible).

Theorem 22. If p is a prime number, then $\mathbb{F}_p = \mathbb{Z}_p$ is a field.

Definition. The set $\mathbb{C}$ of complex numbers is the set of elements of the form $a + b\sqrt{-1}$ where a, b are real numbers.

We define addition and multiplication on $\mathbb{C}$ by

$$(a + b\sqrt{-1}) + (c + d\sqrt{-1}) = (a + c) + (b + d)\sqrt{-1}$$

$$(a + b\sqrt{-1}) \times (c + d\sqrt{-1}) = (ac - bd) + (ad + bc)\sqrt{-1}.$$

Theorem 23. The set $\mathbb{C}$ is a field.

We have special names for rings which satisfy some, but not all, of the axioms a field needs to satisfy.

Definition. We say that a ring R with identity is called a division ring/skew field if it satisfies all the axioms except the commutativity of multiplication ($a \times b = b \times a$ for all a, b in R)– a field assumes the set of non-zero elements is an abelian group with respect to $\times$.

The name 'division ring' is justified by the following assertion:

Proposition 24. Let R be a division ring and a is non-zero element of R. If $ab = ac$, then $b = c$.

Example. Let $\mathbb{H}$ be the set of elements of the form

$$c1 + c(p)p + c(q)q + c(r)r$$

where

- $c, c(p), c(q), c(r)$ range over $\mathbb{R}$
- $1, p, q, r$ are symbols subject to the 'multiplicative relations'
    - $1p = p1 = p$, $1q = q1 = q$, $1r = r1 = r$
    - $p^2 = -1, q^2 = -1, r^2 = -1$
    - $pqr = -1$

In terms of natural addition and multiplication (prescribed by the relations), $\mathbb{H}$ defines a division ring. This is often referred to as Hamilton's quaternions.

The table of (row)(column) is as follows:

	1	p	q	r
1	1	p	q	r
p	p	-1	r	$-q$
q	q	$-r$	-1	p
r	r	q	$-p$	-1

By assumption, $pq = -qp, qr = -rq, rp = -pr$ and therefore the ring is evidently non-commutative. The multiplicative inverse is 1 (the element of $\mathbb{H}$ given by $(c, c(p), c(q), c(r)) = (1, 0, 0, 0)$).

Every non-zero element of $\mathbb{H}$ has multiplicative inverse. To see this let a be a non-zero element of $\mathbb{H}$ of the form $c + c(p)p + c(q)q + c(r)r$. By the assumption, the non-negative real numver

$$\mathcal{R} = c^2 + c(p)^2 + c(q)^2 + c(r)^2$$

is indeed positive. Then the inverse of a is

$$\frac{b}{\mathcal{R}}$$

where $b = c - c(p)p - c(q)q - c(r)r$, i.e.,

$$\frac{1}{\mathcal{R}}\left(c - c(p)p - c(q)q - c(r)r\right) = \frac{1}{\mathcal{R}}c - \frac{1}{\mathcal{R}}c(p)p - \frac{1}{\mathcal{R}}c(q)q - \frac{1}{\mathcal{R}}c(r)r \in \mathbb{H}.$$

The element b plays the same role as the complex conjugation in $\mathbb{C}$!

The set $\mathbb{Z}_n$ of equivalence classes with respect to 'congruence mod n' is a rich source of non-trivial examples of groups, rings and fields:

- $(\mathbb{Z}_n, +)$ is a group.
- $(\mathbb{Z}_n, +, \times)$ is a commutative ring with identity. There are $\phi(n)$ units in $\mathbb{Z}_n$. If n is not a prime number, this is neither a field nor a division ring.
- If n is a prime number p, then $\mathbb{Z}_p = \mathbb{F}_p$ is a field.

3 Polynomials

Definition. Let R be a ring. A polynomial f in one variable X with coefficients in R is:

$$f = c_n X^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c$$

where $c_n, c_{n-1}, \ldots, c_1, c$ are elements of R which are often referred to as the coefficients of f.

The set of all polynomials in one variable X with coefficients in R will be denoted by $R[X]$.

Definition. The degree, denoted $\deg(f)$, of a non-zero polynomial f (in one variable X) is the largest integer n for which its coefficient 'c_n' of X^n is non-zero. The degree is not defined for the zero polynomial.

Definition. A non-zero polynomial $f = c_n X^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c$ of degree n is called monic if the leading coefficient $c_n = 1$. The zero polynomial is defined to be monic.

Theorem 25. If R is a ring, then so is $R[X]$ in terms of addition

$$(f+g)(X) = f(X) + g(X) = \sum_n (c_n(f) + c_n(g))X^n$$

and multiplication

$$(fg)(X) = f(X)g(X) = \sum_n \left(\sum_r c_r(f)c_{n-r}(g)\right) X^n.$$

If R is a ring with identity, then so is $R[X]$. If R is commutative, then so is $R[X]$.

Proposition 26. If $(R, +, \times)$ is a ring with identity 1, then $R[X]$ is not a division ring.

Proposition 27. Let $(F, +, \times)$ be a field. The units $F[X]^\times$ of $F[X]$ are $F^\times = F - \{0\}$.

Theorem 28 (Division algorithm in the context of the polynomial ring $F[X]$). Let F be a field. Let f and g be two polynomials in $F[X]$ and assume, in particular, that g is non-zero. Then there exists polynomials q and r in $F[X]$ such that

$$f = gq + r$$

where either $r = 0$ or $\deg(r) < \deg(g)$.

Definition. Let f and g be polynomials in $F[X]$. We say that g divides f, or g is a factor of f, if there exists a polynomial q in $F[X]$ such that $f = gq$.

Remark. One needs to be careful when it come to polynomial division. Suppose g divides f. Then, for every unit γ in $F[X]$, the product $g\gamma$ also divides f! By Proposition 27, we know that $F[X]^\times = F - \{0\}$, hence this assertions amounts to saying that if g divides f, then any non-zero constant multiple of g also divides f.

The divisibility of a polynomial depends on F:

Examples.

$X + \sqrt{-1}$ divides $X^2 + 1$ in $\mathbb{C}[X]$. Indeed, $(X + \sqrt{-1})(X - \sqrt{-1}) = X^2 - (\sqrt{-1})^2 = X^2 + 1$. On the other hand, no non-trivial polynomial in $\mathbb{Q}[X]$ divides $f(X) = X^2 + 1$ in $\mathbb{Q}[X]$!

Corollary 29. Let F be a field. Let f in $F[X]$ and α be an element of F. Then there exists q in $F[X]$ and r in F such that

$$f = (X - \alpha)q + r.$$

Corollary 30. Let f in $F[X]$ and α in F. The remainder of f when divided by $(X - \alpha)$ is $f(\alpha)$. In particular, $f(\alpha) = 0$ if and only if $X - \alpha$ is a factor of $f(X)$ in $F[X]$.

We may use the corollary to check if a given polynomial factorises or not factorises at all.

Theorem 31.(The Fundamental Theorem of Algebra) Let $n \geq 1$. Let $c, c_1, \ldots, c_n$ be complex numbers, where c_n is assumed to be non-zero. Then the polynomial $c_n X^n + \cdots + c$ has at least one root inside $\mathbb{C}$.

Theorem 32.(The Fundamental Theorem of Algebra with multiplicities) Let $n \geq 1$. Let $c, c_1, \ldots, c_n$ be complex numbers, where c_n is assumed to be non-zero. Then the polynomial $f(X) = c_n X^n + \cdots + c$ has exactly n roots in $\mathbb{C}$ counted with multiplicities, i.e. there exist complex numbers $\alpha_1, \ldots, \alpha_n$ such that

$$f(X) = c_n(X - \alpha_n)(X - \alpha_{n-1}) \cdots (X - \alpha_1).$$

Theorem 33.

- Any two polynomials f and g have a greatest common divisor in $F[X]$.
- The gcd of two polynomials in $F[X]$ can be found by Euclid's algorithm.
- If $\gcd(f, g) = \gamma$ (a polynomial in $F[X]$), then there exist p, q in $F[X]$ such that

  $$fp + gq = \gamma;$$

  these polynomials p and q can also be found from the extended Euclid's algorithm.

4 Matrices

Let $(R, +, \times)$ be a ring and let $\mathrm{M}_2(R)$ be the set of 'matrices'

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where a, b, c, d are elements of R, together with addition

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}$$

and multiplication

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + db' \end{pmatrix}.$$

Theorem 34. $\mathrm{M}_2(R)$ is a ring. If R is a ring with identity, then so is $\mathrm{M}_2(R)$.

Remark. The additive identity, the identity element with respect to $+$ defined above, is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, where each entry 0 is the additive identity in R as defined in (R+2). If R is a ring with identity 1, then $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity.

Remark. In contrast to Theorem 25, $\mathrm{M}_2(R)$ is never commutative, even if R is commutative.

Proposition 35. If $(R, +, \times)$ is a ring with identity but is not a ring with the property that for every elements a, b in R, the product is always $ab = 0$, then $\mathrm{M}_2(R)$ is neither commutative nor a division ring.

Remarks. An example of those rings *excluded* is the ring $(G, *, \times)$ given by a group $(G, *)$ with multiplication $a \times b = e$ for all a, b in G. A field is an example of those rings considered in the proposition.