More sophisticated operations/properties

Absolute value

For $a \in \mathbb{Z}$ (or $\mathbb{Q}$ or $\mathbb{R}$), the absolute value or modulus of a is defined as follows:

$$|a| = \begin{cases} a, & \text{if } a \geq 0 \\ -a, & \text{if } a < 0 \end{cases}$$

e.g. $|-2| = 2$, $|2| = 2$.

Note that $|a|$ is always non-negative.

Division Algorithm

If $b \neq 0$, then for all integers a there exist integers q (quotient) and r (remainder) such that:

(i) $a = q \cdot b + r$

(ii) $|r| < |b|$ <u>or</u> $-\frac{|b|}{2} < r \leq \frac{|b|}{2}$

Note that if we insist that $a \leq r < |b|$, then q and r are unique.

Examples:

- $a = 13,\ b = 3 \Rightarrow q = 4,\ r = 1$, since $13 = 4 \cdot 3 + 1$
- $a = 17,\ b = -5 \Rightarrow q = -3,\ r = 2$, since $17 = (-3)(-5) + 2$
- $a = -1,\ b = 4 \Rightarrow q = -1,\ r = 1$, since $-1 = -1 \cdot 4 + 3$

  For $-\frac{|b|}{2} < r \leq \frac{|b|}{2}$, $q = 0,\ r = -1$. (check)
- $a = 5,\ b = 3 \Rightarrow q = 1,\ r = 2$, since $5 = 1 \cdot 3 + 2$

  For $-\frac{|b|}{2} < r \leq \frac{|b|}{2}$, $q = 2,\ r = -1$. (check)

Definition:

Let a, b be integers. We say that
"a divides b"
and write "$a | b$", if
there exists ($\exists$) an integer c such that
$$a \cdot c = b.$$

e.g. $2 | 6$, because $2 \cdot 3 = 6$.

Properties

- $a | b \Rightarrow a | nb$, $\forall$ integer n, e.g. $2|6 \Rightarrow 2|18$
- $a|b$ and $a|c \Rightarrow a | b+c$, e.g. $2|6, 2|12 \Rightarrow 2|18$
  and
  $a | b-c$, e.g. $2|6, 2|12 \Rightarrow 2|-6$
- $a|b$ and $b|c \Rightarrow a|c$, e.g. $2|6$ and $6|12 \Rightarrow 2|12$
- $a|b$ and $z|b \not\Rightarrow (a+z)|b$, e.g. $1|2, 2|2 \not\Rightarrow 3|2$

Definition:

Let $a, b \in \mathbb{Z}$. We say that a is a divisor of b, if $a | b$.

Definition:

An integer a is prime if:

- a is at least 2 and
- the only positive divisor of a are 1 and itself.

If m is an integer greater than 2 and is not prime, then m is composite.

*NB. 1 is neither prime nor composite.

Smallest primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 31, 37, ...

There are infinitely many primes, so we cannot list them all.

Fundamental Theorem of Arithmetic

Each positive integer can be written as a product of primes <u>and</u> this expression is unique, up to the ordering of these primes.

Examples:

$$10 = 2 \cdot 5 = 5 \cdot 2$$

$$30 = 2 \cdot 3 \cdot 5 = 2 \cdot 5 \cdot 3 = 3 \cdot 2 \cdot 5 = 3 \cdot 5 \cdot 2$$
$$= 5 \cdot 2 \cdot 3 = 5 \cdot 3 \cdot 2$$

$$12 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2 = 2 \cdot 2 \cdot 3$$

Binomial Law

For $a, b \in \mathbb{Z}, \mathbb{Q}, \mathbb{R}$,

$$(a+b)^0 = 1$$

$$(a+b)^1 = a+b$$

$$(a+b)^2 = a^2+2ab+b^2$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3$$

$$(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4$$

and so on...

In general, the coefficients of $(a+b)^n$ are given by the n-th row of Pascal's triangle.

1 → row 0

1 1 → row 1

1 2 1 → row 2

1 3 3 1 → row 3

1 4 6 4 1 → row 4

1 5 10 10 5 1 → row 5

Each entry is the sum of the two entries above it.

Except for the top 1 as well as starting and ending 1's.

Factorisation of Polynomials:

Assuming $P(x), Q(x), R(x)$ are non-zero polynomials and $P(x) = Q(x) \cdot R(x)$.

Then, $\deg P = \deg Q + \deg R$.

(degree of the polynomial $P(x)$)

We say that $Q(x) \cdot R(x)$ is a factorisation of $P(x)$ and also that it is a proper factorisation of $P(x)$ if: $\deg Q, \deg R < \deg P$.

Examples:

- $x^2 - 1 = (x+1)\cdot(x-1)$ ⇝ proper
- $x^2 + x - 2 = (x+2)\cdot(x-1)$ ⇝ proper
- $2x^2 - 2 = 2(x^2-1)$ ⇝ <u>im</u>proper

  $= 2(x-1)(x+1)$ ⇝ proper
- $2x+2 = 2(x+1)$ ⇝ <u>im</u>proper.

Irreducible Polynomials:

A polynomial over $\mathbb{Q}$ or $\mathbb{R}$ of degree ≥ 1 is irreducible, if it has no proper factorisation.

Constants (zero and non-zero) are not irreducible.

A non-constant polynomial is reducible, if it is not irreducible.

Irreducible polynomials are analogous to primes.

Examples:

- $x^2 - 1 = (x+1)\cdot(x-1)$ is reducible.
- $x + 1$ is irreducible.
- $x^3 + 1 = (x+1)\cdot(x^2 - x + 1)$ is reducible.

Remark: Any linear polynomial over $\mathbb{Q}$ and $\mathbb{R}$ is irreducible.

e.g. $x^2 + 1$ is irreducible (over $\mathbb{Q}, \mathbb{R}$).

Show that x^2+1 is irreducible over $\mathbb{Q}, \mathbb{R}$.

Proof:

Suppose on contrary, that x^2+1 is reducible. Then we can write:

$$x^2+1 = (ax+b)(cx+d),$$

for some $a, b, c, d \in \mathbb{Q}, \mathbb{R}$ with $a, c \neq 0$.

Equivalently,

$$\boxed{x^2+1 = (x+b')\cdot(c'\cdot x+d)} \quad (1)$$

when $b' = \frac{b}{a}$, $c' = c\cdot a$, $d' = d\cdot a$

(by multiplying RHS of (1) by $\frac{1}{a}\cdot a (=1)$).

From (1) we get:

$$x^2+1 = c'\cdot x^2 + (b'\cdot c'+d')\cdot x + b'd'$$

or equivalently,

$$\begin{cases} c' = 1, \quad b'\cdot c'+d' = 0 \\ \quad\quad \text{and} \\ b'd' = 1 \end{cases}$$

Therefore, $d' = -b' \Rightarrow (b')^2 = -1$,

which is not possible for $b \in \mathbb{Q}, \mathbb{R}$.

Hence our initial assumption was wrong.
So, x^2+1 is irreducible.

Remarks:

→ In general, testing polynomials for irreducibility is not easy.

→ x^4+1 is irreducible over $\mathbb{Q}$, but it is reducible over $\mathbb{R}$.

(Why? – $x^4+1=(x^2+\sqrt{2}\cdot x+1)\cdot(x^2-\sqrt{2}\cdot x+1)$)

Definition:

Suppose a non-zero polynomial $P(x)$:

$$P(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n$$

, for some n such that $a_n\neq 0$. Then,

- $n=\deg P$ (degree of P as defined previously)
- $a_n=\mathrm{lc}P$ (leading coefficient (lc) of P)
- $a_nx^n=\mathrm{lt}P$ (leading term (lt) of P)

We say that P is MONIC, if $a_n=1$, i.e. $\mathrm{lc}P=1$

e.g.
- x^2+x+2 is monic.
- $x+3x^2+4x^3$ is not monic ($\because \mathrm{lc}=4\neq 1$)
- 0 is not monic (No lc).

Fundamental Theorem of Algebra

Every monic polynomial over $\mathbb{Q}$ or $\mathbb{R}$ can be factor(is)ed into a product of irreducible monic polynomials.

This factorisation is unique up to the ordering of factors.

Examples:

- $x+1 = x+1$ (irreducible)
- $x^2-2 = x^2-2$ (irreducible over $\mathbb{Q}$)
- $x^2-2 = \underbrace{(x+\sqrt{2})}_{\text{irreducible}}\underbrace{(x-\sqrt{2})}_{\text{irreducible}}$ over $\mathbb{R}$.
- $x^3-1 = (x-1)\cdot(x^2+x+1)$

Alternative Form of the...
Fundamental Theorem of Algebra

Every non-zero polynomial $P(x)$ over $\mathbb{Q}$ or $\mathbb{R}$ has an expression of the following form:

$$P(x) = c \cdot P_1(x) \cdot P_2(x) \cdot \ldots \cdot P_n(x),$$

with c some non-zero constant,

n a natural number,

$P_1, P_2, \ldots, P_n$ are irreducible monic polynomials

The expression above is unique apart from the ordering of $P_1, P_2, \ldots, P_n$.

$\boxed{\text{Examples}}$

- $x^3 - 6x^2 + 11x - 6 = (x-1)(x-2)(x-3)$
- $x^3 + 6x^2 - x - 6 = x^2(x+6) - 1(x+6)$
$$= (x+1)(x-1)(x+6)$$
- $2x^2 + x - 1 = 2(x - \frac{1}{2})(x+1)$

Division of Polynomials

Let $P(x)$, $S(x)$ be polynomials.
We say that $S(x)$ divides $P(x)$ and write $S(x) \mid P(x)$ or $S \mid P$, if there exists $Q(x)$ such that:

$$P(x) = Q(x) \cdot S(x)$$

Example:

$$x^2 + x - 12 = (x+4)(x-3)$$

So, $x+4 \mid x^2+x-12$ and $x-3 \mid x^2+x-12$.

Division algorithm for Polynomials

Suppose $P(x)$ and $S(x)$ are polynomials over $\mathbb{Q}$ or $\mathbb{R}$ with $S(x) \neq 0$.

Then, there are polynomials $Q(x)$ (quotient) and $R(x)$ (remainder) such that:

(i) $P(x) = Q(x) \cdot S(x) + R(x)$

(ii) $R(x) = 0$ or $\deg R < \deg S$

The polynomials $Q(x)$ and $R(x)$ are unique.

Example:

- Divide $x^3 - 2x^2 + x - 1$ by $x - 3$.

$$x^2 + x + 4 \longrightarrow Q(x)$$

$$\begin{array}{r|l}
x-3 & x^3 - 2x^2 + x - 1 \\
 & \underline{-\cancel{x^3} + 3x^2} \\
 & \quad x^2 + x - 1 \\
 & \quad \underline{-\cancel{x^2} + 3x} \\
 & \qquad 4x - 1 \\
 & \qquad \underline{-\cancel{4x} + 12} \\
 & \qquad\quad 11
\end{array}$$

$$11 \longrightarrow R(x)$$

Therefore,

$$\underbrace{x^3-2x^2+x-1}_{P(x)} = \underbrace{(x^2+x+4)}_{Q(x)}\cdot\underbrace{(x-3)}_{S(x)} + \underbrace{11}_{R(x)}$$

$$\deg R < \deg S,$$

since

$$\deg R = 0 < 1 = \deg S$$

• Divide x^3-2x^2+x-1 by x^2-3

$$\begin{array}{r|l}
 & x-2 \longrightarrow Q(x) \\
\hline
x^2-3 & x^3-2x^2+x-1 \longrightarrow S(x) \\
 & -\cancel{x^3} \qquad\;\; +3x \\
\hline
 & \quad -\cancel{2x^2}+4x-1 \\
 & \quad +\cancel{2x^2} \qquad -6 \\
\hline
 & \qquad 4x-7 \longrightarrow R(x)
\end{array}$$

We have:

$$x^3-2x^2+x-1 = (x-2)(x^2-3)+4x-7.$$