# MTH 4104

Mondays 16 – 18

Fridays 14 – 15

29/03
01/04 } no lectures

We have Week 7 lectures

04/03 (Monday) 16 – 18
Skeel LT

08/03 (Friday) 14 – 15 AHS 2

Tutorials start in Week 2

---

What I do:

every week, I'll give you

- typed-up notes

  Everything in here is examinable

- hand-written notes

  as you see in lectures.

---

5 Example sheets.

# Assessments

$2 \times 10\%$ mid-term

( Week 6
Week 12

$80\%$ Final exam.

---

What this course is about?

We axiomatise what we know very well (e.g. integers, Euclid's algorithm, modular arithmetic, complex numbers, polynomials, matrices).

> ie spot "common denominators" of these mathematical concepts.

For example, we'll see

$$\mathbb{Z} := \{ , -2, -1, 0, 1, 2 \dots \}$$

" the set of integers

rings

& the set of polynomials in

1-variable with coeffts in $\mathbb{Q}$

$$x^2+2x+4, \quad \frac{1}{2}x^2+\frac{1}{3}x+\frac{1}{4} \text{''}$$

have similar "algebraic structures

Similarly,

$\mathbb{Q}$ := the set of rational numbers

$$= \left\{ \frac{r}{s} \quad \begin{matrix} r, s \in \mathbb{Z} \\ s \neq 0 \end{matrix} \right\}$$

&

the set of Laurent series

in 1-variable with coeffts in $\mathbb{Q}$

$$\sum_{n \geq -N} c_n x^n \quad \text{etc.}$$

fields

$N > 0 \qquad c_n \in \mathbb{Q}.$

e.g. $x^{-1} + 2x + 2x^2 + 2x^3 + \cdots$

$x^{-10} + x^{-9} + \frac{1}{2}x^{-4}$ etc.

also have similar algebraic structures.

we'll prove general statements about rings, fields etc.

This is useful because once

we prove those things,

those statements would hold for

any examples.

## Main Reference

- Alex Fink's lecture notes

2022-2023

(QMplus).

- R. Allenby
  "Rings, fields and groups: Introduction to abstract algebra"
- P. Cameron
  "Intro to Algebra"

## §1 Revising bits and bobs from NSF.

Let $\mathbb{Z}$ be the set of integers.

By a non-negative integer,

I mean an integer $\geq 0$

By a positive integer

I mean —"— $> 0$

By a negative integer

I mean —"— $< 0$

**Proposition 1** Let $a$ and $b$ be integers.

Assume $b > 0$

(but $a$ can still be negative)

Then there exist integers

$q$ and $r$

s.t. $a = bq + r$

with $0 \leq r < b$

$q$ is often referred to as

the quotient

$r$ —"—

the remainder

Moreover,

$q$ and $r$ are unique, i.e.

## Example

$a = 100 \quad b = 7$

if $(q_1, r_1)$ $\quad 0 \le r_1 < b$

$a = bq_1 + r_1$

& $(q_2, r_2)$ $\quad 0 \le r_2 < b$

$a = bq_2 + r_2$

$$100 = \underset{\substack{= \\ q}}{7} \cdot 14 + \underset{\substack{= \\ r}}{2}$$

then $q_1 = q_2$

$r_1 = r_2$

$$0 \le 2 < 7$$

$a = -100 \quad b = 7$

$$-100 = (-15) \cdot 7 + 5$$

$$0 \le 5 < 7$$

$a = 2 \quad b = 3$

$$2 = 0 \cdot 3 + 2$$

$0 \leq 2 < 3$

$a = -2 \quad b = 3$

$-2 = (-1) \cdot 3 + 1$

$0 \leq 1 < 3$

Proof of Proposition 1.

Existence

Let $S$ be the set of integers of the form $a + sb \geq 0$ (where $s$ ranges over $\mathbb{Z}$)

Since $a = a + 0b$,

$S'$ contains $a$

and therefore $S'$ is non-empty.

Let $r$ be the smallest element of $S'$.

Because $r \in S'$,

it is of the form

$$\underline{\underline{r = a + (-q) b \geq 0}}$$

for some integer $q$.

These $q$ and $r$ are what we are looking for. It remains to check $r < b$.

Suppose $r \geq b$

(The goal is to find contradiction).

Then

$$r - b = (a - qb) - b$$

$$= a - (q+1)b$$

$$< a - bq = r$$

because $b > 0$

So $r - b$ defines an element of $S$

that is smaller than $r$,

contradicting the minimality of $r$ $\#$.

**Def** Let $a$ & $b$ be integers.

We say that $a$ divides $b$

if there exists an integer $c$

s.t. $b = a \cdot c$.

What happens if $a = 0$ ?

For the statement "0 divides b"

to make sense, $\exists\, c$ s.t. $b = 0 \cdot c$
$= 0$

forcing $b$ to be zero!

In other words, the only integer 0 divides is zero itself.

Note that I'm only talking about "0 divides 0" and not about "$0/0$".

__Example__

Every integer $a$, including 0, divides 0.

$$\underset{\underset{b}{=}}{0} = a \cdot \underset{c}{0}$$

__Def__ Let $a$ & $b$ be integers.

A <u>common divisor</u> of $a$ & $b$

is a non-negative integer r

with the property that r divides a

& r divides b.

A common divisor of a & b
$r$

is called the greatest common divisor

(and written as gcd(a, b))

if any other common divisor is

smaller than r.

i.e. if s is another common divisor,

then $s' < r$.

**Examples** $a = 12 \quad b = 18$

$$\gcd(12, 18) = 6$$

$$a = 12 \quad b = -18$$

$$\gcd(12, -18) = 6$$

If $a$ is a non-negative integer,

$$\gcd(a, 0) = a$$

This requires a proof.

**Rk** Any common divisor of $a$ & $b$ divides $\gcd(a, b)$.

Example $a=50$ $\gcd(50,100)=50$
$b=100$

2, 5, 10, 25 are all common divisors

& they all divide $50 = \gcd$ !!

Compute $\gcd(198, 78) = 6$

$$198 = 78 \cdot 2 + 42$$

$$78 = 42 \cdot 1 + 36$$

$$42 = 36 \cdot 1 + 6$$

$$36 = 6 \cdot 6 + 0$$

$\gcd(-78, 198) = 6$

Recall $a, b$ & $b > 0$

$a = bq + r$

$0 \le r < b$

$-78 = 198 \cdot (-1) + 120$

$198 = 120 \cdot 1 + 78$

$120 = 78 \cdot 1 + 42$

$78 = 42 \cdot 1 + 36$

$42 = 36 \cdot 1 + 6$

$36 = 6 \cdot 6 + 0$

This Euclid's algorithm is based on the following statement:

<u>**Prop 6**</u> Let $a$ & $b$ be integers

Suppose $b > 0$

& $a = bq + r$

$0 \le r < b$

Then $\gcd(a, b) = \gcd(b, r)$

Recall

$\gcd(198, 78)$

$198 = 78 \cdot 2 + 42$

By Prop 6, $\gcd(198, 78) = \gcd(78, 42)$

What is $\gcd(78, 42)$?

$$78 = 42 \cdot 1 + 36$$

new "a" new "b" new "r"

By Prop 6, $\gcd(78, 42)$

$\parallel$

$\gcd(42, 36)$

Repeating this process,

we get

$\gcd(198, 78) = \gcd(78, 42) = \gcd(42, 36)$

$\parallel$

$\gcd(36, 6)$
$= 6.$

**Lemma** $a, b \in \mathbb{Z}$

$$\gcd(a,b) = \gcd(-a,b) = \gcd(a,-b) = \gcd(-a,-b).$$

**Theorem 7** If $a$ & $b$ are integers, there exist integers $r$ & $s$

s.t. $\quad ar + bs = \gcd(a, b)$

To put it another way,

the equation $\quad ax + by = \gcd(a, b)$

has an integer solution.

Find $r$ & $s$ s.t.

$$198r + 78s = 6$$

$$198 = 78 \cdot 2 + 42$$

$$78 = 42 \cdot 1 + 36$$

$$42 = 36 \cdot 1 + 6$$

$$36 = 6 \cdot 6 + 0$$

$$6 = 42 - 1 \cdot 36$$

$$= 42 - 1 \cdot (78 - 1 \cdot 42)$$

rearrange!!

$$= 2 \cdot 42 - 1 \cdot 78$$

$$= 2 \cdot (198 - 2 \cdot 78) - 1 \cdot 78$$

$$= 2 \cdot 198 - 5 \cdot 78$$

$$6 = 2 \cdot 198 + (-5) \cdot 78.$$

$$(r, s) = (2, -5).$$

It is possible to do this for

**Exercise.** $\gcd(-78, 198)$.