MTH1001M-Algebra

Slides Week 3

Primes and unique factorisation in the integers.
Writing numbers in a certain base.
Arithmetic and geometric progressions.
Polynomials.
The degree of a polynomial.
Polynomial division with remainder.

Primes and unique factorisation in the integers

- DEFINITION. A positive integer is *composite* if it can be written as $a = bc$, where $b > 1$ and $c > 1$ are also integers.
- DEFINITION. We say that $a > 1$ is *prime* if it is not composite.
  So a being prime means that whenever $a = bc$ for some positive integers b and c, then either $b = 1$ or $c = 1$.
- Equivalently, $a > 1$ is prime if its only positive divisors are 1 and a.
- By design, 1 is neither prime nor composite.
- THEOREM (Unique factorisation). *Every integer larger than* 1 *factorises into a product of primes, and in a unique way.*
- EXAMPLE. $180 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 3 \cdot 5 \cdot 2 \cdot 3 \cdot 2$ are really the same: the order of the factors does not count. Best write $180 = 2^2 \cdot 3^2 \cdot 5$.

- Existence is easy. Uniqueness (optional proof in Notes) uses:
- LEMMA. *Let p be a prime (integer), and let a, b be integers. If p divides the product ab, then p divides either a or b.*
- PROOF. If $p \mid a$ we are done, so suppose that p does not divide a.
  - Then (p, a) divides p, but is not p because $p \nmid a$, so it must be 1 because p is prime. So p divides ab but $(p, a) = 1$.
  - Arithmetical Lemma B then implies that p divides b. $\square$
- The theorem on unique factorisation implies the school's rule for finding GCD and lcm (which requires factorising a and b).
- EXAMPLE. $a = 12 = 2^2 \cdot 3^1 \cdot 5^0$, $b = 45 = 2^0 \cdot 3^2 \cdot 5^1$. Then
  - $(12, 45) = 2^0 3^1 5^0 = 3$ (take each prime with the lower exponent)
  - $[12, 45] = 2^2 3^2 5^1 = 180$ (take each prime with the higher exponent)
  - If we multiply them together we get $(12, 45) \cdot [12, 45] = 2^0 3^1 5^0 \cdot 2^2 3^2 5^1 = 2^2 3^1 5^0 \cdot 2^0 3^2 5^1 = 12 \cdot 45.$

Writing integers in a certain base

- When we write a positive integer in decimal notation, say 237, we mean $237 = (237)_{10} = 2 \cdot 10^2 + 3 \cdot 10 + 7$.
- The same number can be written in any base $b > 1$, using digits from $0, 1, 2, \ldots, b-1$, for example
  - $237 = (456)_7 = 4 \cdot 7^2 + 5 \cdot 7 + 6$,
  - $237 = (1422)_5 = 1 \cdot 5^3 + 4 \cdot 5^2 + 2 \cdot 5 + 2$,
  - $237 = (11101101)_2 = 2^7 + 2^6 + 2^5 + 2^3 + 2^2 + 1$ (binary),
  - $237 = (ED)_{16} = 14 \cdot 16 + 13$ (hexadecimal, $0, \ldots, 9, A, B, C, D, E, F$)
- The notation extends from integers to positive real numbers by writing further digits (possibly infinitely many) after a point:
  - $237/25 = (9.48)_{10} = (14.22)_5 = 1 \cdot 5 + 4 + 2 \cdot 5^{-1} + 2 \cdot 5^{-2}$
  - Notation for periodic numbers: $(1.2\dot{3}4\dot{5})_7 = (1.2345345345\cdots)_7$.
  - Some numbers can be written in two ways: $(1.2\dot{6})_7 = (1.3)_7$.

Converting integers from base b to decimal

- To convert $(1422)_5$ from base 5 to decimal, we may just compute $(1422)_5 = 1 \cdot 5^3 + 4 \cdot 5^2 + 2 \cdot 5 + 2 = \cdots = 237$. But the calculation will be faster if arranged as follows (fewer operations):

$$\begin{aligned}(1422)_5 &= ((1 \cdot 5 + 4) \cdot 5 + 2) \cdot 5 + 2 \\ &= (9 \cdot 5 + 2) \cdot 5 + 2 \\ &= 47 \cdot 5 + 2 = 237.\end{aligned}$$

  Good also on a pocket calculator, doing operations in a sequence.
- EXAMPLE. $(61405)_7 = ((6 \cdot 7 + 1) \cdot 7 + 4) \cdot 7 \cdot 7 + 5 = 14950$. Can also be arranged as follows (see Ruffini's rule later on):

$$\begin{array}{c|cccc|c} & 6 & 1 & 4 & 0 & 5 \\ 7 & & 42 & 301 & 2135 & 14945 \\ \hline & 6 & 43 & 305 & 2135 & 14950 \end{array}$$

Converting integers from decimal to base b

- This is done by reversing the previous procedure: to convert n into $n = (\cdots d_3\, d_2\, d_1\, d_0)_5 = \cdots + d_3 \cdot 5^3 + d_2 \cdot 5^2 + d_1 \cdot 5 + d_0$ note that d_0 is the remainder of dividing n by 5; the quotient will be $\cdots + d_3 \cdot 5^2 + d_2 \cdot 5 + d_1$; now divide that by 5; and so on.
- EXAMPLE. To convert 14950 to base 7 keep dividing as follows:

$$\begin{aligned} 14950 &= 7 \cdot 2135 + 5 \\ 2135 &= 7 \cdot 305 + 0 \\ 305 &= 7 \cdot 43 + 4 \\ 43 &= 7 \cdot 6 + 1 \\ 6 &= 7 \cdot 0 + 6 \end{aligned}$$

  The digits in base 7 are the remainders read from the bottom up, so $(14950)_{10} = (61405)_7$.

Converting real numbers from base b to decimal

- If the number of digits in base b after the point is finite, say s digits, remove the point (which is the same as multiplying the number by b^s), convert into decimal, and divide the result by b^s.
- EXAMPLE. To convert $(14.22)_5$ to decimal, remove the point (which means multiplying by 5^2), convert $(1422)_5 = 237$, and then divide by 5^2: $\qquad (14.22)_5 = 237/25 = 9.48.$
- If the number to be converted has infinitely many digits, can do the same with an approximation (keep a few digits after the point).
- EXAMPLE. To convert $(2.\dot{1})_3 = (2.11111\cdots)_3$ to decimal, we may convert the approximation $(2.111)_3 = (2111)_3/27 = 67/27$, which equals $2 + \frac{13}{27} = 2.\dot{4}8\dot{1}$, so roughly just a bit over 2.48.
- Actually, $(2.\dot{1})_3 = 2.5$, because $(2.\dot{1})_3 \cdot 2 = (11.\dot{2})_3 = (12)_3 = 5$.

Converting real numbers from decimal to base b

- Split the decimal number into its integer part (what comes before the decimal point) plus a fractional part (hence less than 1), and convert them to base b separately.
- For the fractional part, multiply it by b, then the integer part of the result will be the first digit in base b after the point.
  Now take the fractional part and repeat the procedure.
- EXAMPLE. To convert 5.481 to base 3, write it as $5 + 0.481$.
  - $0.481 \cdot 3 = 1.443$, so first digit after point will be 1;
  - $0.443 \cdot 3 = 1.329$, so second digit after point will be 1;
  - $0.329 \cdot 3 = 0.987$, so third digit after point will be 0;
  - $0.987 \cdot 3 = 2.961$, so fourth digit after point will be 2;
  - $0.961 \cdot 3 = 2.883$, so fifth digit after point will be 2; and so on.
  - In conclusion, $5.481 = (12.11022\cdots)_3$.

Arithmetic progressions

- A sequence $a_1, a_2, \ldots, a_n$ of (complex) numbers is an *arithmetic progression* if the difference $d = a_{k+1} - a_k$ does not depend on k.
  - Formula for the nth term: $a_n = a_1 + d(n-1)$.
  - *Arithmetic series* $a_1 + a_2 + \cdots + a_n$:

$$\sum_{k=1}^{n} a_k = a_1 + a_2 + \cdots + a_n = \frac{(a_1 + a_n) \cdot n}{2}.$$

PROOF.
$$\begin{aligned} 2(a_1 + a_2 + \cdots + a_n) = &\quad (a_1 + a_2 + \cdots \qquad +a_n) \\ &+ (a_n + a_{n-1} + \cdots \quad +a_1) \\ = &\ (a_1 + a_n) \cdot n. \end{aligned}$$

  - Best memorised as *the sum of the first and last term, times the total number of terms, divided by two*. Or *the arithmetic mean (average) of the first and last term, times the total number of terms*.

Geometric progressions

- A sequence $a_1, a_2, \ldots, a_n$ of nonzero numbers is a *geometric progression* if the ratio $r = a_{k+1}/a_k$ does not depend on k.
  - Formula for the nth term: $a_n = a_1 \cdot r^{n-1}$.
  - The product of all terms is analogue to an arithmetic series. If a_1 and r are real and positive then
$$\prod_{k=1}^{n} a_k = a_1 \cdot a_2 \cdots a_n = \sqrt{(a_1 a_n)^n}.$$
  - Sum of a geometric progression:
$$a_1+a_2+a_3+\cdots+a_n = a_1(1+r+r^2+\cdots+r^{n-1}) = a_1\frac{r^n-1}{r-1} = a_1\frac{1-r^n}{1-r}.$$
PROOF.
$$\begin{aligned}(1+r+\cdots+r^{n-1})(r-1) = &\qquad\quad r+r^2+\cdots+r^{n-1}+r^n\\ &-1-r-r^2-\cdots-r^{n-1}\\ &= r^n-1.\end{aligned}$$
  - If it does not terminate, and $|r| < 1$: $a_1 + a_2 + a_3 + \cdots = a_1/(1-r)$.

Converting a periodic decimal number to a fraction

- $0.171717\cdots = 0.\dot{1}\dot{7} = 0.17 \cdot 1.\dot{0}\dot{1}$
  $= 0.17 \cdot \left(1 + (0.01) + (0.01)^2 + \cdots\right) = \frac{0.17}{1-0.01} = \frac{17}{99}.$
- More generally, for a number with a *periodic decimal expansion* (or *recurring decimal*), with both an *integer part* and a *pre-period*:
  - $1234.56789789789\cdots = 1234.56\dot{7}8\dot{9} = \dfrac{123456789 - 123456}{99900}.$
  - The numerator of the fraction equals

    [integer part|pre-period|period]   minus   [integer part|pre-period],

    ignoring the decimal point.
  - The denominator has as many nines as the number of digits of the period, followed by as many zeroes as the digits of the pre-period.
- The rule works in base b instead of 10, if you replace 9 with $b - 1$.

Polynomials

- A polynomial is the result after simplification of any expression made from numbers and letters using only additions, subtractions, and multiplications (but no divisions).
- We will only consider polynomials involving just one letter, the *indeterminate* x. If the expression contains parentheses, they can always be removed through the usual simplification rules:

  $x^2 \cdot 5x - 2(4x - 3x \cdot 2 - \frac{1}{2}) - \frac{2}{3}x^2$ can be simplified to $5x^3 - \frac{2}{3}x^2 + 4x + 1$, which is *a polynomial in normal form*.
- It is important to be clear on which kind of numbers are allowed as coefficients: $x^2 - 2$ cannot be factorised using only rationals, but it can using reals, because $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.
- We specify a *field* F for the coefficients, such as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (roughly a set of numbers which can also be divided, not just $+, -, \cdot$).

- EXAMPLE. The set of integers $\mathbb{Z}$ is not a field: $2/3 \notin \mathbb{Z}$.
  One can consider polynomials with integer coefficients, but theory gets harder if we are not allowed divisions in the coefficients.
- So a polynomial with coefficients in F is something of the form $f(x) = a_n x^n + \cdots + a_1 x + a_0$, with $a_0, a_1, \ldots, a_n \in F$, for some n. (We can always put it in this normal form if it is not.)
- The set of all such polynomials is denoted by $F[x]$.
- That includes the zero polynomial: $0 = 0x + 0 = 0x^2 + 0x + 0, \ldots$
- Notation $f(x)$ borrowed from Calculus, as a special type of function of the 'variable' x, a *polynomial function*. (This is not quite the same thing as a polynomial, but is equivalent if $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$.)
- If β is any element of F, we may *evaluate $f(x)$ on β, or for $x = \beta$,* and compute the value $f(\beta) = a_n\beta^n + \cdots + a_1\beta + a_0$.

The degree

- The degree of a non-zero polynomial $f(x)$ is the largest integer n such that $a_n \neq 0$, and is denoted by $\deg(f) = n$.
- Such a_n is *the leading coefficient*, and $a_n x^n$ is *the leading term*.
- If $a_n = 1$ then we call $f(x)$ *monic*. Call a_0 *the constant term*.
- Writing $f(x) = a_n x^n + \cdots + a_1 x + a_0$ we *do not* assume $a_n \neq 0$.
- EXAMPLE. The polynomial $(t-2)x^2 + 3x - \frac{t}{2}$ depends on a parameter t, meaning that for each value we give to t we get a polynomial, say in $\mathbb{R}[x]$. When $t = 2$ we get $0x^2 + 3x - 1$, which has degree 1, and when $t \neq 2$ the degree is 2.
- We have not assigned a degree to the zero polynomial yet. Non-zero constants have degree zero, so $\deg(0)$ should be less than that: it is convenient to set $\deg(0) = -\infty$.

Addition and multiplication

$$(a_n x^n + \cdots + a_1 x + a_0) + (b_n x^n + \cdots + b_1 x + b_0) =$$
$$= (a_n + b_n) x^n + \cdots + (a_1 + b_1) x + (a_0 + b_0).$$

$$(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) \cdot (b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0) =$$
$$= a_n b_m x^{n+m} + (a_{n-1} b_m + a_n b_{m-1}) x^{n+m-1} + \cdots$$
$$\cdots + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + (a_0 b_1 + a_1 b_0) x + a_0 b_0.$$

- So the degrees of a sum and of a product of polynomial satisfy

$$\deg\bigl(f(x) + g(x)\bigr) \leq \max\bigl(\deg(f(x)), \deg(g(x))\bigr),$$

and $$\deg\bigl(f(x) \cdot g(x)\bigr) = \deg\bigl(f(x)\bigr) + \deg\bigl(g(x)\bigr).$$

- Setting $\deg(0) = -\infty$ these are valid also for the zero polynomial.

Polynomial division with remainder

- THEOREM. *Let F be a field and let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that*

$$f(x) = g(x)q(x) + r(x),$$

where $\deg\big(r(x)\big) < \deg\big(g(x)\big)$.

- Note $\deg\big(r(x)\big) < \deg\big(g(x)\big)$ includes the case $r(x) = 0$.
- Had we not assigned a degree to 0, the condition on $r(x)$ should be *where either* $r(x) = 0$ *or* $\deg\big(r(x)\big) < \deg\big(g(x)\big)$.
- There is no variant such as remainder with $-b/2 < r \leq b/2$ when dividing integers: polynomial division can only be done in one way.
- PROOF OF EXISTENCE (OF QUOTIENT AND REMAINDER). The main idea of the long division algorithm can provide a proof. □

- EXAMPLE. Divide $f(x) = 2x^4 + x^2 - x + 1$ by $g(x) = 2x - 1$.

$$
\begin{array}{rrrrrrrrrr}
 & x^3 & + & \frac{1}{2}x^2 & + & \frac{3}{4}x & - & \frac{1}{8} & & \\ \cline{2-10}
\multicolumn{1}{r|}{\mathbf{2x} - 1} & \mathbf{2x^4} & + & 0x^3 & + & x^2 & - & x & + & 1 \\
 & 2x^4 & - & x^3 & & & & & & \\ \cline{2-4}
 & & & \mathbf{x^3} & + & x^2 & & & & \\
 & & & x^3 & - & \frac{1}{2}x^2 & & & & \\ \cline{4-6}
 & & & & & \mathbf{\frac{3}{2}x^2} & - & x & & \\
 & & & & & \frac{3}{2}x^2 & - & \frac{3}{4}x & & \\ \cline{6-8}
 & & & & & & - & \mathbf{\frac{1}{4}x} & + & 1 \\
 & & & & & & - & \frac{1}{4}x & + & \frac{1}{8} \\ \cline{7-10}
 & & & & & & & & & \mathbf{\frac{7}{8}}
\end{array}
$$

- Hence $2x^4 + x^2 - x + 1 = (2x - 1) \cdot \left(x^3 + \frac{1}{2}x^2 + \frac{3}{4}x - \frac{1}{8}\right) + \frac{7}{8}$.
- The algorithm stops as soon as we obtain a *remainder* which is zero or has degree less than the degree of $g(x)$.

- We started with integer coefficients but had to use rational numbers in the calculation, and also for the final result: the theorem would fail with $F = \mathbb{Z}$ because that is not a field.
- EXAMPLE. Divide $f(x) = 2x^4 - x^3 + 3x^2 + x - 2$ by $g(x) = x^2 - 2x + 2$.

$$
\begin{array}{r|ccccccccc}
\multicolumn{1}{r}{} & 2x^2 & + & 3x & + & 5 & & & & \\
\cline{2-10}
x^2 - 2x + 2 & 2x^4 & - & x^3 & + & 3x^2 & + & x & - & 2 \\
\multicolumn{1}{r}{} & 2x^4 & - & 4x^3 & + & 4x^2 & & & & \\
\cline{2-6}
\multicolumn{1}{r}{} & & & 3x^3 & - & x^2 & + & x & & \\
\multicolumn{1}{r}{} & & & 3x^3 & - & 6x^2 & + & 6x & & \\
\cline{4-8}
\multicolumn{1}{r}{} & & & & & 5x^2 & - & 5x & - & 2 \\
\multicolumn{1}{r}{} & & & & & 5x^2 & - & 10x & + & 10 \\
\cline{6-10}
\multicolumn{1}{r}{} & & & & & & & 5x & - & 12
\end{array}
$$

- $2x^4 - x^3 + 3x^2 + x - 2 = (x^2 - 2x + 2) \cdot (2x^2 + 3x + 5) + (5x - 12)$.

- PROOF OF UNIQUENESS (OF QUOTIENT AND REMAINDER).
  - Suppose that the division can be done in two ways,
$$f(x) = g(x)q_1(x) + r_1(x) \qquad \text{and} \qquad f(x) = g(x)q_2(x) + r_2(x),$$
    with $\deg(r_1(x)) < \deg(g(x))$ and $r_2(x) < \deg(g(x))$.
  - Then we claim that $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$. In fact,
$$g(x)q_1(x) + r_1(x) = f(x) = g(x)q_2(x) + r_2(x),$$
    and so
$$g(x) \cdot [q_1(x) - q_2(x)] = r_2(x) - r_1(x).$$
  - By the condition on remainders, the RHS has degree $< \deg(g(x))$.
  - The LHS has degree $\deg(g(x)) + \deg[q_1(x) - q_2(x)]$.
  - Hence $q_1(x) - q_2(x)$ has negative degree, but the only negative degree is $-\infty$, hence $q_1(x) - q_2(x) = 0$.
  - This implies $q_1(x) = q_2(x)$, and then also $r_1(x) = r_2(x)$. $\square$