Basic Math - Fourth and Last lesson

Caboara

1 Notations

1. The set of natural numbers (positive integers) is denoted by $\mathbb{N}$. The elements of $\mathbb{N}$ are $0, 1, 2, \cdots$ etc..
2. The set of integer numbers is denoted by $\mathbb{Z}$. The elements of $\mathbb{Z}$ are $0, 1, -1, -2, -2 \cdots$ etc..
3. The set of rationals (numeric fractions) is denoted by $\mathbb{Q}$. The elements of $\mathbb{Q}$ are $-3, 0, 2, \frac{4}{5}$ etc..
4. The set of reals is denoted by $\mathbb{R}$. Elements of R are $-3, 0, 2, \frac{4}{5}, \sqrt{2}, \pi$ etc..
5. Note that all these sets are nested $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$
6. The set of polynomials over $\mathbb{R}$ (with real coefficients) is denoted by $\mathbb{R}[x]$. Elements of $\mathbb{R}[x]$ are $\pi x + 1, x^3 - \frac{2}{5}x^2 + 1, x^2 - \sqrt{2}$ etc..
7. The sets $\mathbb{N}[x], \mathbb{Z}[x], \mathbb{Q}[x]$ are defined similarly.
8. Note that these sets are nested $\mathbb{N}[x] \subset \mathbb{Z}[x] \subset \mathbb{Q}[x] \subset \mathbb{R}[x]$.

Definition 1. *Let $n \in \mathbb{N}$. The set of divisors of n, denoted* $\mathrm{DIV}(n)$*, is the set of all natural numbers that divide n. For example,*

$$\mathrm{DIV}(12) = \{1, 2, 3, 4, 6, 12\}.$$

2 Theorems and Propositions

Proposition 2. *For all $a, b \in \mathbb{R}[x]$, the following hold:*

- $a^2 - b^2 = (a + b)(a - b).$
- $a^3 - b^3 = (a - b)(a^2 + ab + b^2).$
- $a^3 + b^3 = (a + b)(a^2 - ab + b^2).$
- $a^2 + b^2$ *cannot be factored further over* $\mathbb{R}$.

Theorem 3 (Ruffini's Theorem)**.** *Let $f(x) \in \mathbb{R}[x]$ and $a \in \mathbb{R}$ such that $f(a) = 0$ (i.e., a is a root of $f(x)$). Then,*

$$(x - a) \;\mid\; f(x).$$

Proposition 4. *Let $f(x), g(x), h(x) \in \mathbb{R}[x]$ such that $f(x) \mid h(x)$, $g(x) \mid h(x)$, and $f(x), g(x)$ are coprime. Then,*

$$f(x)g(x) \;\mid\; h(x).$$

Theorem 5 (Rational Root Theorem)**.** *Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in \mathbb{Z}[x]$ and $a \in \mathbb{Q}$ such that $f(a) = 0$. Then,*

$$a \in \left\{ \pm\frac{p}{q} \mid p \in \mathrm{DIV}(a_0),\ q \in \mathrm{DIV}(a_d) \right\}.$$

3 Exercises

1. $P(x) = x^5 + x^3 + x^2 + 1 = 0$. Note that $P(-1) = 0$. Use polynomial division.
   - Factorization $x^5 + x^3 + x^2 + 1 = (x^2 + 1)(x^3 + 1) = (x + 1)(x^2 + 1)(x^2 - x + 1)$.
   - The solution is $x = -1$.
2. $P(x) = x^5 - 9x^3 - 8x^2 + 72 = 0$. Note that $P(\pm 3) = P(2) = 0$. Use division.
   - Factorization $x^5 - 9x^3 - 8x^2 + 72 = (x + 3)(x - 3)(x - 2)(x^2 + 2x + 4)$.
   - The solutions are $x = \pm 3, 2$.
3. $P(x) = x^4 - 3x^3 + 2x - 6 = 0$. Note that $P(3) = 0$. Use division.
   - Factorization $x^4 - 3x^3 + 2x - 6 = (x - 3)(x^3 + 2)$.
   - The solutions are $x = 3,\ \pm\sqrt[3]{-2}$.

4 Proposed exercises

Solutions will be given in the next installment of these notes. Regrouping will be more difficult here. Use of the root rule and Ruffini is recommended.

1. For the parameter $a \in \mathbb{R}$, $P(x) = x^3 - ax^2 - 2x + 2a = 0$. Note that $P(a) = 0$. Use division.
   - Factorization $x^3 - ax^2 - 2x + 2a = (x - a)(x^2 - 2)$.
   - The solutions are $x = a,\ \pm\sqrt{2}$.
2. For the parameter $a \in \mathbb{R}$, $P(x) = x^3 - ax^2 - 2x + 2a = 0$. Note that $P(a) = 0$. Use division.
   - Factorization $x^3 - ax^2 - ax + a^2 = (x - a)(x^2 - a)$.
   - The solutions are $x = a$ always, if $a \geq 0$ also $\pm\sqrt{a}$.

3. $x^{32} - 1 = 0$
4. $x^8 - 4 = 0$
5. $x^3 + (1-a)x^2 - (a+6)x + 6a = 0$
6. $2x^3 - 17x^2 + 38x - 15 = 0$
7. $3x^4 - 22x^3 - 2x^2 + 66x - 21 = 0$
8. $x^3 - 17x^2 + 92x - 160 = 0$
9. $x^6 - 12x^4 + 47x^2 - 60 = 0$
10. $x^3 - xa^2 - 2xab - xb^2 - x^2 + a^2 + 2ab + b^2 = 0$
11. $x^3 + 3x^2y + 3xy^2 + y^3 - 2x^2 - 4xy - 2y^2 - x - y + 2 = 0$. Hint: try to detect powers.

5 Greater Common Divisor - $\mathbb{N}$

Definition 6. *If $a, b \in \mathbb{N}$, the greater common divisor of a, b is the biggest $p \in \mathbb{N}$ such that $p|a$ and $p|b$. Since $1|a$ and $1|b$, if there are no other common divisor, $\gcd(a,b) = 1$.*

Remark 7. *If $a, b \in \mathbb{N}$ a divides $b \Leftrightarrow$ exists $c \in \mathbb{N}$ such that $b = c \cdot a$. We write*

$$a|b \Leftrightarrow \exists\ c \in \mathbb{N} \text{ such that } b = c \cdot a$$

Since for every $a \in \mathbb{N}$ $0 = 0 \cdot a$, we have that 0 is divisible by any natural number. Hence, $\gcd(a, 0) = a$

Computing GCD's using factorizations.

Proposition 8. *If we have $a, b \in \mathbb{N}$ and their prime factorization*

$$a = p_1^{\alpha_1} \cdots p_n^{\alpha_n} q_1^{\gamma_1} \cdots q_m^{\gamma_m} \quad \text{and} \quad a = p_1^{\beta_1} \cdots p_n^{\beta_n} s_1^{\theta_1} \cdots s_t^{\theta_t}$$

(the p_i are the common prime factors) then

$$\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_n^{\min(\alpha_1,\beta_1)}$$

We can say that the greatest common divisor of a and b, if their prime factorizations are known, is the product of the common prime factors, taken with the minimum exponent.

Example 9.

1. *Since* $600 = 2^3 \cdot 3 \cdot 5^2$ *and* $252 = 2^2 \cdot 3^2 \cdot 7$ *we have that* $\gcd(600, 252) = 2^2 \cdot 3 = 12$.
2. *Since* $70 = 2 \cdot 5 \cdot 7$ *and* $429 = 3 \cdot 11 \cdot 3$ *we have that* $\gcd(70, 429) = 1$.

The greatest common divisor has the following properties

Proposition 10. *If $a, b, c \in \mathbb{N}$*

1. $\gcd(a, b) = \gcd(b, a)$.
2. $\gcd(a, a) = a$.
3. $\gcd(a, 0) = a$.
4. $\gcd(0, 0)$ *is undefined. Why?*
5. $\gcd(ac, bc) = c \gcd(a, b)$.
6. *If* $a = cb+r$, *with* r *the remainder of the division of* a *by* b *we have* $\gcd(a, b) = \gcd(cb+r, b) = \gcd(r, b) = \gcd(b, r)$.

Computing GCD's using Euclid's Algorithm.

Example 11. *Using the rule* $\boxed{\gcd(a, b) = \gcd(b, r)}$ *with* r *the remainder of* a *divided by* b. *We compute some* gcd *using the* `EuclidVerbose` *procedure of CoCoA.*

1.
```
EuclidVerbose(15,12);
 [15, 12]
 [12, 3]
 [3, 0]
GCD(15,12)=3
3
```

2.
```
EuclidVerbose(2343,432);
 [2343, 432]
 [432, 183]
 [183, 66]
 [66, 51]
 [51, 15]
 [15, 6]
 [6, 3]
 [3, 0]
GCD(2343,432)=3
3
```

3.
```
EuclidVerbose(347,237);
 [347, 237]
 [237, 110]
 [110, 17]
 [17, 8]
 [8, 1]
 [1, 0]
GCD(347,237)=1
1
```

Definition 12. *If $a, b \in \mathbb{N}$ and $\gcd(a,b) = 1$ we say that a, b are* coprime. *Coprime natural numbers have no common divisors other than 1. A prime number p is coprime with every natural number except its multiples, i.e., numbers of the form p^n.*

Remark 13. *We remark that if $c \in \mathbb{N}$ is coprime with $b \in \mathbb{N}$ then $\gcd(ac,b) = \gcd(a,b)$. We can discard coprime factors.*

1. $\gcd(32 \cdot 5, 27) = \gcd(32, 27)$ *since $5, 27$ are coprime.*

6 Greater Common Divisor - Polynomials

Definition 14. *An polynomial $p(x) \in \mathbb{R}[x]$ is* irreducible *if there is no other polynomial $f(x) \in \mathbb{R}[x]$ of degree bigger or equal to 1 that divides $p(x)$. A polynomial is* reducible *if it is not irreducible. itself. Irreducible polynomials play the role of prime numbers.*

Example 15.

1. *All degree one polynomials are irreducible.*
2. *A polynomial $ax^2 + bx + c$ is irreducible if and only if $\Delta = b^2 - 4ac > 0$.*
3. $x^2 + x + 1$ *is irreducible since $\Delta = 1 - 4 < 0$.*
4. $x^2 + 1$ *is irreducible since $\Delta = 0 - 4 < 0.$.*
5. *The polynomial x^2-5x+6 is reducible because $(x-2)|(x^2-5x+6)$. Also $\Delta = 25-24 = 1 > 0$.*
6. *The polynomial $4x^2-12x+9$ is reducible because $(2x-3)|(4x^2-12x+9)$. Also $\Delta = 144-144 = 0$.*
7. *The polynomial $p(x) = x^4-3x^3+5x^2-9x+6$ is reducible since $p(x) = (x-1)(x-2)(x^2+3)$.*
8. *Find if a polynomial of degree ≥ 3 is reducible or not can be quite difficult.*

Remark 16. *All the properties of the GCD over the natural numbers hold for the polynomials. Moreover by convention, the GCD of polynomials is defined not taking into consideration purely numeric factors. Hence, we can take out of the computations any pure number, not only coprime factors.*

$$F(x), G(x) \in \mathbb{R}[x],\ a \in \mathbb{R}, \quad \gcd(F(x), aG(x)) = \gcd(F(x), G(x))$$

We have $\gcd(2x^2, 4x) = x$, and

$$\begin{aligned} \gcd((x-2)(3x-3), x^2-1) &= \gcd(3(x-2)(x-1), x^2-1) \\ &= \gcd((x-2)(x-1), x^2-1) \\ &= \gcd((x-2)(x-1), (x+1)(x-1) \\ &= x-1 \end{aligned}$$

We can compute Polynomial GCD's easily if we know the irreducible factorization, at least of one factor

Example 17. *The polynomials $x-2, x-7, x-1$ are irreducible since they have degree one. The polynomial x^2+2 is irreducible since it has negative Δ.*

$$\gcd((x-2)^2(x^2+2)^3(x-7),(x-2)(x^2+2)^4(x-1)) = (x-2)^{\min(2,1)}(x^2+2)^{\min(3,4)} = (x-2)(x^2+2)^3$$

Example 18. *We have to compute $\gcd(x^4+x-7, x^2-1)$. We define $p(x)=x^4+x-7$ and we note that irreducible factorization $x^2-1=(x+1)(x-1)$, so*

$$\gcd(x^4+x-7, x^2-1) = \gcd(x^4+x-7,(x+1)(x-1))$$

the GCD has to have the common factors, but there are none, since

$$p(1) = -5 \Rightarrow (x-1) \nmid p(x) \quad \textit{and} \quad p(-1) = -7 \Rightarrow (x+1) \nmid p(x)$$

Hence, $\gcd(x^4+x-7, x^2-1) = 1$ *and* $x^4+x-7,\ x^2-1$ *are coprime.*

We can use Euclid's Algorithm for the GCD in the polynomial case, using polynomial divisions.

The computations are done using the `GCDPolyVerbose` command of the CoCoA system. The remainder sequence for $f(x),\ g(x)$ is given by $f(x),\ g(x)$ and the remainders, if suitable regrouping and taking out numeric factors

Example 19.

```
GCD(x^2+x+1,x^2+2)=
We divide x^2+x+1 by x^2+2, the remainder is x - 1
(x^2 + x + 1)=(1)*(x^2 + 2)+(x - 1)

=GCD(x^2+2,x - 1)=
(x^2 + 2)=(x + 1)*(x - 1)+(3)
We divide x^2+2 by x-1, the remainder is 3

=GCD(x - 1,3)=GCD(x - 1,1) (we took out the number 3)

=GCD(x - 1,1)=1 there is no common factor

The remainder sequence is x^2 + x + 1, x^2 + 2, x - 1, 1
```

Example 20.

```
GCD(x^4+x^3-1,x^3+x-2)=
(x^4 + x^3 - 1)=(x + 1)*(x^3 + x - 2)+(-x^2 + x + 1)
We divide x^4+x^3-1 by x^3+x-2 the remainder is -x^2 + x + 1

=GCD(x^3+x-2,-x^2 + x + 1)=
(x^3 + x - 2)=(-x - 1)*(-x^2 + x + 1)+(3x - 1)
We divide x^3+x-2 by -x^2 + x + 1 the remainder is 3x - 1
```

```
=GCD(-x^2 + x + 1,3x - 1)=
(-x^2 + x + 1)=(-1/3x + 2/9)*(3x - 1)+(11/9)
We divide -x^2 + x + 1 by 3x - 1 the remainder is 11/9

=GCD(3x - 1,11/9)=GCD(3x - 1,1)=1 We took out the numeric factor 11/9

The remainder sequence is x^4 + x^3 - 1, x^3 + x - 2, -x^2 + x + 1, 3x - 1, 1
```

Example 21.

```
GCD(x^4 - 6x^3 + 7x^2 + 12x - 18,x^3 + x^2 - 2x - 2)=
(x^4 - 6x^3 + 7x^2 + 12x - 18)=(x - 7)*(x^3 + x^2 - 2x - 2)+(16x^2 - 32)
We divide x^4 - 6x^3 + 7x^2 + 12x - 18 by x^3 + x^2 - 2x - 2,
the remainder is 16x^2 - 32=16(x^2-2)
We take out the number 16, the remainder is now x^2-2

=GCD(x^3 + x^2 - 2x - 2,x^2-2)=
(3x^3 + 2x^2 - 6x - 4)=(-3x - 2)*(-x^2 + 2)+(0)
We divide x^3 + x^2 - 2x - 2 by x^2-2, the remainder is 0

=GCD(x^2-2,0)=x^2-2

The remainder sequence is x^4 - 6x^3 + 7x^2 + 12x - 18, x^3 + x^2 - 2x - 2, x^2 - 2
```