# MMA 数学特論 I

# Algorithms for polynomial systems: elimination & Gröbner bases

# 多項式系のアルゴリズム: グレブナー基底 & 消去法

---

## Lecture II: Univariate polynomials, (polynomials in one variable)

**April, 22th 2010.** Part I: Generalities

Part II: The quotient ring $\Bbbk[X]/\langle P\rangle$

Part III: When $\Bbbk[X]/\langle P\rangle$ is it a field ?

**May, 6th 2010.** Part IV: Algebraic numbers

## Part I: Generalities

### The polynomial algebra $\mathbb{k}[X]$

$P \in \mathbb{k}[X]$ written as: $P = \sum_{i=0}^{n} p_i X^i$, with $p_i \in \mathbb{k}$.

The largest integer $n$ such that $p_n \neq 0$ is called the degree of $P$.

Then, the leading coefficient of $P$ is $p_n$: $\textsc{lc}(P) = p_n$.

Let $Q = \sum_{i=0}^{m} q_i X^i$ be a polynomial of degree $m \leq n$.

Addition: $P + Q = \sum_{i=0}^{m} (q_i + p_i) X^i + \left[ \sum_{i=m+1}^{n} p_i X^i \right]_{\text{appears only if } m<n}$

Multiplication: $PQ = \sum_{i=0}^{m+n} \left( \sum_{k+\ell=i} p_k q_\ell \right) X^i$

$\Leftrightarrow \textsc{lc}(PQ) = p_n q_m = \textsc{lc}(P)\textsc{lc}(Q)$ which is not zero (true over any field).

## The ring $\Bbbk[X]$

The following three points are easy to check:

1. $PQ = QP$ (the multiplication is commutative)
2. $(PQ)R = P(QR)$ (the multiplication is associative)
3. $P(Q + R) = PQ + PR$ (the multiplication is distributive with respect to the addition)

$\Rightarrow \Bbbk[X]$ is a commutative ring.

---

**Definition 1** *A* ring $R$ *is a set endowed with an addition* $+$ *so that* $(R, +)$ *is a commutative group, and a multiplication* $\times$*, with a* unit element $1_A$*, which verifies points 2 and 3 above.*

*If* $\times$ *verifies point 1 as well, then* $R$ *is a* commutative ring*.*

# The degree

**Proposition 1** *For any polynomials $P$ and $Q$ in $\Bbbk[X]$, we have:*

*(i)* $\deg(P+Q) \leq \max\{\deg(P)\,,\, \deg(Q)\}$, *with equality if* $\deg(P) \neq \deg(Q)$.
*(true over any ring, not only fields $\Bbbk$).*

*(ii)* $\deg(PQ) = \deg(P) + \deg(Q)$ *(not true over any ring, but true over any* integral domain $\rightarrow$ *Definition 7)*

PROOF:Exercise. □

Example: $P = X^2 + X$ and $Q = -X^2 + 1$, then $\deg(P+Q) < 2$.

Consequence: Let $L \in \mathbb{N}^\star$ and let $\Bbbk[X]_{<L} = \{P \in \Bbbk[X] \mid \deg(P) < L\}$.

This a $\Bbbk$-vector space of dimension $L$, with monomial basis
$\{1, X, X^2, \ldots, X^{L-1}\}$ (*Comment:* there are many other bases of $\Bbbk[X]_{<L}$ !).

# Lagrange bases of $\Bbbk[X]_{<L}$

Nodes: Let $a_1, \ldots, a_L$ be $L$ distinct points in $\Bbbk$ (assume $L < |\Bbbk|$, if $\Bbbk$ is finite).

Idempotents: For $1 \leq i \leq L$, let $\ell_i(X) := \prod_{j \neq i} \frac{X - a_j}{a_i - a_j}$.

- $\ell_i(a_j) = 0$ if $j \neq i$, and $\ell_i(a_i) = 1$.
- $\deg(\ell_i) = L - 1$

Lagrange interpolation formula: For any $P \in \Bbbk[X]_{<L}$, we have
$P(X) = \sum_{i=1}^{L} P(a_i)\ell_i(X)$. Indeed, let $Q(X) = P(X) - \sum_{i=1}^{L} P(a_i)\ell_i(X)$:

$$
\begin{aligned}
Q(a_i) &= P(a_i) - P(a_1)\ell_1(a_i) - P(a_2)\ell_2(a_i) - \cdots - P(a_i)\ell_i(a_i) - \cdots - P(a_L)\ell_L(a_i) \\
&= P(a_i) - \quad 0 \quad - \quad 0 \quad - \cdots - P(a_i)1 \quad - \cdots - \quad 0 \\
&= 0.
\end{aligned}
$$

$\Rightarrow Q$ is of degree $L - 1$ and has $L$ roots, hence $Q = 0$ (Corollary 1, Lect. I).

Consequences: $1 = \ell_1(X) + \ell_2(X) + \cdots + \ell_L(X)$.

$\{\ell_1(X), \ldots, \ell_L(X)\}$ generates $\Bbbk[X]_{<L}$ as a vector space, so it is a basis.

# The graded commutative algebra $\mathbb{k}[X]$

Consequence: ... The multiplication in $\mathbb{k}[X]$ induces a $\mathbb{k}$-bilinear map of $\mathbb{k}[X]$:

$$\begin{array}{rcccl} Mult & : & \mathbb{k}[X]_{<L_1} \times \mathbb{k}[X]_{<L_2} & \longrightarrow & \mathbb{k}[X]_{<L_1+L_2} \\ & & (A, B) & \longmapsto & AB \end{array}$$

We say that $\mathbb{k}[X]$ is a graded ring.

Also $\mathbb{k}[X]$ is a $\mathbb{k}$-vector space (of infinite dimension...) $\Rightarrow$ it is an algebra over $\mathbb{k}$.

$\Rightarrow$ Finally, $\mathbb{k}[X]$ is a ring, a $\mathbb{k}$-vector space, graded, commutative: it is a graded commutative algebra over $\mathbb{k}$.

---

**Definition 2** *An* algebra *$A$ over a field $k$ is a ring that is a $k$-vector space.*

## Part II: The quotient ring $\Bbbk[X]/\langle P\rangle$

### The remainder map

Let $P \in \Bbbk[X]$ be a non-constant polynomial of degree $L \geq 1$.

For any $A \in \Bbbk[X]$, let $A = BP + R$ be the Euclidean division of $A$ by $P$.

The map $\phi_P$ is well-defined, because the remainder $R$ is uniquely determined by $A$ and $P$.

$$\begin{array}{rcccl} \phi_P & : & \Bbbk[X] & \longrightarrow & \Bbbk[X]_{<L} \\ & & A & \longmapsto & R, \end{array}$$

Easy to check: For any $A_1, A_2 \in \Bbbk[X]$ we have:
$\phi_P(A_1 + A_2) = \phi_P(A_1) + \phi_P(A_2)$.

For any $\lambda \in \Bbbk$: $\phi_P(\lambda A_1) = \lambda\phi_P(A_1)$.

$\Rightarrow$ $\phi_P$ is a linear map between the $\Bbbk$-vector spaces $\Bbbk[X]$ and $\Bbbk[X]_{<L}$.

# Kernel of the remainder map

$$\begin{aligned}\ker \phi_P &= \{A \in \Bbbk[X] \mid \phi_P(A) = 0\} \\ &= \{A \in \Bbbk[X] \mid P \mid A, \quad \text{“}P \text{ divides } A\text{”}\}.\end{aligned}$$

Hence $\ker \phi_P = \langle P \rangle$ (the principal ideal generated by $P$).

Notation: For $a \in \Bbbk[X]$ let $a + \langle P \rangle = \{a + QP \mid Q \in \Bbbk[X]\} \subset \Bbbk[X]$.

(*Comment:* sometimes denoted $a \bmod P$, or even $a\langle P \rangle \ldots$)

---

**Definition 3** *An ideal $I$ of a commutative ring $A$ is a subset which verifies:*

1. *$I$ is a subgroup of $A$ for the addition.*
2. *for all $a \in A$ and $b \in I$, we have $ab \in A$*

*An ideal $I$ is said to be principal if $I = \langle b \rangle$ (where $\langle b \rangle := \{ab \mid a \in A\}$).*

# A quotient algebra

Let $\mathbb{k}[X]/\langle P\rangle := \{a + \langle P\rangle \mid a \in \mathbb{k}[X]\}$.

**Lemma 1** *$\mathbb{k}[X]/\langle P\rangle$ is a $\mathbb{k}$-algebra (a $\mathbb{k}$-vector space and a ring).*

PROOF:Let $\langle P\rangle \in \mathbb{k}[X]/\langle P\rangle$ be the zero element.

Addition: $(a + \langle P\rangle) + (b + \langle P\rangle) := (a + b) + \langle P\rangle$

Multiplication: $(a + \langle P\rangle).(b + \langle P\rangle) := ab + \langle P\rangle$. (indeed: $(a + \langle P\rangle).(b + \langle P\rangle) = ab + (a + b)\langle P\rangle + \langle P^2\rangle$, but $(a + b)\langle P\rangle + \langle P^2\rangle \subset \langle P\rangle$).

Easy to check: with this addition and multiplication, $\mathbb{k}[X]/\langle P\rangle$ is a ring (Cf. Definition 1)

Finally, for $\lambda \in \mathbb{k}^\star$, we have: $\lambda(a + \langle P\rangle) = \lambda a + \langle P\rangle$, because $\langle \lambda P\rangle = \langle P\rangle$.

This defines on $\mathbb{k}[X]/\langle P\rangle$ a structure of vector space over $\mathbb{k}$.

By Definition 2 this shows that $\mathbb{k}[X]/\langle P\rangle$ is an algebra. $\square$

# An isomorphism

For two polynomials $a, b \in \Bbbk[X]$, if $a - b \in \langle P \rangle = \ker \phi_P$ then:

$\phi_P(a-b) = 0 \Rightarrow \phi_P(a) = \phi_P(b) \Rightarrow \forall b \in a + \langle P \rangle,\ \phi_P(b) = \phi_P(a)$.

Then $\bar{\phi}_P(a + \langle P \rangle) := \phi_P(a)$ is well-defined.

$$\begin{array}{ccccc} \Bbbk[X] & \xrightarrow{\bmod P} & \Bbbk[X]/\langle P \rangle & \xrightarrow{\bar{\phi}_P} & \Bbbk[X]_{<L} \\ a & \mapsto & a + \langle P \rangle & \mapsto & \bar{\phi}_P(a + \langle P \rangle). \end{array}$$

By definition : $\phi_P = \bar{\phi}_P \circ \bmod P$ .

$\Rightarrow \ker \bar{\phi}_P = \langle P \rangle$ which is zero in $\Bbbk[X]/\langle P \rangle$.

$\Rightarrow \bar{\phi}_P$ is an isomorphism of vector spaces between $\Bbbk[X]/\langle P \rangle$ and $\Bbbk[X]_{<L}$.

$\Rightarrow \dim_{\Bbbk} \Bbbk[X]/\langle P \rangle = L$.

Comment: $\Bbbk[X]_{<L}$ is not a subring of $\Bbbk[X]$, because there exists $P_1, P_2 \in \Bbbk[X]_{<L}$, such that $\deg(P_1 P_2) \geq L$ (so that $P_1 P_2 \notin \Bbbk[X]_{<L}$). But we can transport the multiplication of $\Bbbk[X]/\langle P \rangle$ to $\Bbbk[X]_{<L}$ by this linear isomorphism:

$P_1 \cdot P_2 := \bar{\phi}_P(P_1 P_2)$. Then, $\bar{\phi}_P$ is a ring homomorphism, and also an isomorphism.

# Abstraction to general rings

Let $A$ be a commutative ring and $I$ an ideal of $A$.

The *quotient* ring $A/I$ is a ring defined in the following way:

Addition: $(a+I)+(b+I)=(a+b)+I$.

Multiplication: $(a+I)(b+I)=ab+(a+b)I+I^2\subset(ab)+I$.

Let $B$ be another ring, and $\phi : A \to B$ a ring homomorphism:

1. $\phi(0)=0$, $\phi(1_A)=1_B$ and for all $a_1,a_2\in A$:
2. $\phi(a_1+a_2)=\phi(a_1)+\phi(a_2)$ and $\phi(a_1a_2)=\phi(a_1)\phi(a_2)$,

First isomorphism theorem: As before, $I:=\ker\phi$ is an ideal of $A$, and $\forall a'\in a+I$, $\phi(a')=\phi(a)$.

The map $\bar\phi(a+I):=\phi(a)$ is well-defined and verifies, $\phi=\bar\phi\circ\operatorname{mod} I$:

$$A\xrightarrow{\text{mod } I}A/I\xrightarrow{\bar\phi}B,\quad \text{and } \bar\phi \text{ is one-one}$$

# Another very similar ring: $\mathbb{Z}$ (1/2)

$\mathbb{Z}$ and $\Bbbk[X]$ are 2 rings with an Euclidean division: they are Euclidean rings.

Let $n \in \mathbb{N}$ and let $\begin{array}{rcl} \phi_n : \mathbb{Z} & \rightarrow & \{0, 1, \ldots, n-1\}, \\ r & \mapsto & r \bmod n \text{ (euclidean remainder of } r \text{ by } n). \end{array}$

As usual: $\phi_n(x+y) = \phi_n(\phi_n(x) + \phi_n(y)) = x + y \bmod n$.

$\phi_n(xy) = \phi_n(\phi_n(x)\phi_n(y)) = xy \bmod n$.

/!\ $\{0, \ldots, n-1\}$ has no structure: no addition, multiplication...

We transport the addition and multiplication of $\mathbb{Z}$ to $\{0, \ldots, n-1\}$ by the map $\phi_n$ : $\phi_n$ becomes then a ring homomorphism that is onto.

---

**Definition 4** *A principal ideal domain (PID for short) is an integral domain in which each ideal is principal.*

**Proposition 2** *Any Euclidean ring is a PID (but some PID are not Euclidean).*

# Another very similar ring: $\mathbb{Z}$ (2/2)

Kernel of the map $\phi_n$: $\ker \phi_n = \{r \in \mathbb{Z} \mid n|r \text{ “}r\text{ divides }n\text{” } \} = n\mathbb{Z}$.

This is an ideal of $\mathbb{Z}$. The quotient ring is denoted $\mathbb{Z}/n\mathbb{Z}$.

An element of $\mathbb{Z}/n\mathbb{Z}$ is denoted $a + n\mathbb{Z}$ $(= \{a + rn \mid r \in \mathbb{Z}\} \subset \mathbb{Z})$.

The addition and multiplication of $\mathbb{Z}/n\mathbb{Z}$ are defined naturally.

If $a' \in a + n\mathbb{Z}$, then $\phi_n(a') = \phi_n(a)$, so the map

$$\begin{aligned} \bar{\phi}_n : \mathbb{Z}/n\mathbb{Z} &\rightarrow \{0, \ldots, n-1\}, \\ a + n\mathbb{Z} &\mapsto \phi_n(a) \end{aligned}$$

is well-defined.

The first isomorphism theorem is written in this case:

$\mathbb{Z} \xrightarrow{\text{mod } n} \mathbb{Z}/n\mathbb{Z} \xrightarrow{\bar{\phi}_n} \{0, \ldots, n-1\}$, with $\phi_n = \bar{\phi}_n \circ \text{mod} n$, and $\bar{\phi}_n$ is one-one

## Part III: When $\Bbbk[X]/\langle P\rangle$ is it a field ?

### Bézout identity

Let $a$ and $b$ be two polynomials of $\Bbbk[X]$; denote $\mathsf{gcd}(a,b) = g$.

This means: $\langle a, b\rangle = \langle g\rangle$, so there exists, $u, v \in \Bbbk[X]$ such that

$$au + bv = g \qquad \textit{(Bézout identity)}$$

Euclid's Lemma: *Let $p$ and $x$ be 2 relatively prime ( $\iff \mathsf{gcd}(p,x) = 1$) polynomials in $\Bbbk[X]$, and $y$ another one. Assume that: $p|xy$ ($p$ divides $xy$). Then $p|y$ ($p$ divides $y$).*

PROOF:The Bézout identity of $p$ and $x$ is here : $up + vx = 1$ for 2 polynomials $u, v \in \Bbbk[X]$.

So $upy + vxy = y$ and since $p|xy$, there exists $p'$ such that $pp' = xy$:

$\Rightarrow upy + vpp' = y \Rightarrow p(uy + vp') = y$, so $p|y$. $\square$

# Prime ideal and irreducible element

**Definition 5** *A polynomial $P \in \Bbbk[X]$ is* irreducible *if it is non-constant ($\iff \deg(P) > 0$), and if we have:*

$$P = P_1 P_2, \text{ then } P_1 \text{ or } P_2 \in \Bbbk \ (\iff \deg(P_1) \text{ or } \deg(P_2) = 0).$$

Comment: If $P$ is an irreducible polynomial, then $P$ has no root in $\Bbbk$ (indeed if $\alpha \in \Bbbk$ is such a root, then $X - \alpha$ is a factor in $\Bbbk[X]$ of $P$, contradiction).

The converse is false: $X^4 - X^2 + 2$ has no root in $\Bbbk$, but factorizes into $(X^2+1)(X^2-2)$.

**Proposition 3** *If $P$ is an irreducible polynomial, then the ideal it generates $\langle P \rangle$ in $\Bbbk[X]$, is a* prime ideal.

---

**Definition 6** *An ideal $I$ of a ring $A$ is* prime *if for all $x, y \in A$ such that $xy \in I$, then $x \in I$ or $y \in I$.*

# Field $\Bbbk[X]/\langle P\rangle$

PROOF:(of Proposition 3) Let $x, y \in \Bbbk[X]$ such that $xy \in \langle P\rangle$. This is equivalent to $p|xy$. By Euclid's Lemma, $p|x$ or $p|y$; so $x$ or $y \in \langle P\rangle$. $\square$

This implies: if $P$ is irreducible, then $\Bbbk[X]/\langle P\rangle$ is an integral domain. There is actually a stronger result:

**Proposition 4** *If $P$ is an irreducible polynomial, then $\Bbbk[X]/\langle P\rangle$ is a* field

PROOF:Given $a + \langle P\rangle \neq 0$ in $\Bbbk[X]/\langle P\rangle$ ($\iff a \notin \langle P\rangle$), what is its inverse ?
(1) If $a \in \Bbbk^\star$, then $(a + \langle P\rangle)(\frac{1}{a} + \langle P\rangle) = 1 + \langle P\rangle$.
(2) If $a \notin \Bbbk$, ($\iff \deg(a) > 0$), then $a$ and $P$ are relatively prime (since $P$ is supposed irreducible), and the Bézout identity holds: $au + Pv = 1$. It comes: $(a + \langle P\rangle)(u + \langle P\rangle) = 1 + \langle P\rangle$. $\square$

---

**Definition 7** *A ring $A$ is an* integral domain *if $xy = 0 \Rightarrow x = 0$ or $y = 0$.*

**Lemma 2** *If $I$ is a prime ideal, then $A/I$ is an integral domain.*

# Computing Bézout identity

## Extended Euclidean Algorithm

\# Inputs: $f, g \in \mathbb{k}[X]$ with $f \neq 0$ and $\deg(f) \geq \deg(g)$

\# Outputs: $\ell \in \mathbb{N}$, $r_\ell, s_\ell, t_\ell \in \mathbb{k}[X]$, with $r_\ell = \mathsf{gcd}(f, g)$ and $r_\ell = f s_\ell + g t_\ell$.

$r_0 \leftarrow f$, $s_0 \leftarrow 1$, $t_0 \leftarrow 0$

$r_1 \leftarrow g$, $s_1 \leftarrow 0$, $t_1 \leftarrow 1$

$i \leftarrow 1$

`while` $(r_i \neq 0)$ `do`

    $(q_i, r_{i+1}) \leftarrow$ `EuclideanDivision`$(r_{i-1}, r_i)$ *//so that:* $r_{i-1} = q_i r_i + r_{i+1}$

    $s_{i+1} \leftarrow s_{i-1} - q_i s_i$

    $t_{i+1} \leftarrow t_{i-1} - q_i t_i$

    $i \leftarrow i + 1$

`end while`

$\ell \leftarrow i - 1$

`return` $\ell$, $r_\ell, s_\ell, t_\ell$.

# Termination

Does the algorithm terminate ? Yes.

We must show that the `while` loop at Step 4 exits after a finite number of iterations. For all $i = 1, 2, \ldots$ by Step 5, $r_{i-1} = q_i r_i + r_{i+1}$, with $r_{i-1} \neq 0$ and $\deg(r_{i-1}) < \deg(r_i)$ or $r_{i-1} = 0$.

Starting with $r_0 = f$, and $r_1 = g$, the sequence $(\deg(r_i))_{i \geq 0}$ is strictly decreasing, and then there exists $i \geq 1$ such that $r_i = 0$. Then the `while` loop does a finite number of iterations.

Actually, this shows that the number of iterations is at most $\deg(r_1) = \deg(g)$.

---

Comment: If we replace $\Bbbk[X]$ by $\mathbb{Z}$, and $\deg(\,.\,)$ by the absolute value $|\,.\,|$, the algorithm and the proof of termination are the same.

# Correctness

Is the algorithm correct ? Or is $r_\ell = fs_\ell + gt_\ell$ the Bézout identity ?

For $i = 0, \ldots, \ell$, the equality $r_i = fs_i + gt_i$ $(*)_i$ holds.

Proof by induction. By the initialization step, $r_0 = f$ and $s_0 f + t_0 g = f$. Then if we assume Equality $(*)_j$ true for $j = 0, \ldots, i$ then by Steps 5,6 and 7:

$$\begin{aligned} r_{i+1} &= r_{i-1} - r_i q_i = (s_{i-1} f + t_{i-1} g) - (s_i f + t_i g) q_i \\ &= (s_{i-1} - q_i s_i) f + (t_{i-1} - q_i t_i) g = s_{i+1} f + t_{i+1} g, \end{aligned}$$

which is $(*)_{i+1}$.

Finally, if $r_i = 0$, then we have $r_{i-1} = \mathsf{gcd}(f, g)$ (this is the standard Euclidean algorithm) and Step 9 denotes $r_\ell = \mathsf{gcd}(f, g)$. So $r_\ell = fs_\ell + gt_\ell$ □

---

Comment: This proof is correct if we exchange $\Bbbk[X]$ by $\mathbb{Z}$ (or any Euclidean ring).

# Example over $\mathbb{Z}$

$f = 126$ and $g = 35$.

| $i$ | $q_i$ | $r_i$ | $s_i$ | $t_i$ | $r_i = s_i f + t_i g$ | $r_{i-1} = q_i r_i + r_{i+1}$ |
|---|---|---|---|---|---|---|
| 0 | | 126 | 1 | 0 | $126 = 1.126 + 0.35$ | |
| 1 | 3 | 35 | 0 | 1 | $35 = 0.126 + 1.35$ | $126 = 3.35 + 21$ |
| 2 | 1 | 21 | 1 | $-3$ | $21 = 1.126 - 3.35$ | $35 = 1.21 + 14$ |
| 3 | 1 | 14 | $-1$ | 4 | $14 = -1.126 + 4.35$ | $21 = 1.14 + 7$ |
| 4 | 2 | 7 | 2 | $-7$ | $7 = 2.126 - 7.35$ | $14 = 2.7 + 0$ |
| 5 | | 0 | $-5$ | 18 | $0 = -5.126 + 18.35$ | |

We have $r_5 = 0$ so $\ell = 4$ and $\mathsf{gcd}(f, g) = r_4 = 7$ and the Bézout identity is:

$$7 = 2.126 - 7.35$$

# Example over $\mathbb{k}[X]$

$f = 18X^3 - 42X^2 + 30X - 6$ and $g = -12X^2 + 10X - 2$

| $i$ | $q_i$ | $r_i$ | $s_i$ | $t_i$ |
|---|---|---|---|---|
| 0 | | $18X^3 - 42X^2 + 30X - 6$ | 1 | 0 |
| 1 | $-\frac{3}{2}X + \frac{9}{4}$ | $-12X^2 + 10X - 2$ | 0 | 1 |
| 2 | $-\frac{8}{3}X + \frac{4}{3}$ | $\frac{9}{2}X - \frac{3}{2}$ | 1 | $\frac{3}{2}X - \frac{9}{4}$ |
| 3 | | 0 | $\frac{8}{3}X - \frac{4}{3}$ | $4X^2 - 8X + 4$ |

Here $r_3 = 0$ so $\ell = 2$ and $\mathsf{gcd}(f, g) = r_\ell = r_2 = \frac{9}{2}X - \frac{3}{2}$. The Bézout identity:

$$\frac{9}{2}X - \frac{3}{2} = 1.(18X^3 - 42X^2 + 30X - 6) + \left(\frac{3}{2}X - \frac{9}{4}\right)(-12X^2 + 10X - 2)$$

# Application of the EEA, 1

Linear Diophantine equations : What are the $x, y \in \mathbb{Z}$ such that $6x - 8y = 1$ ?
$\mathsf{gcd}(6, 8) = 2 \Rightarrow \langle 8, 6 \rangle = \langle 2 \rangle$. But $1 \notin \langle 2 \rangle$, so there is no solutions in $\mathbb{Z} \times \mathbb{Z}$.

What about $6x - 8y = 4$ ? We can divide by the gcd : $3x - 4y = 2$

This time, $\mathsf{gcd}(3, 4) = 1$, so $2 \in \langle 1 \rangle = \mathbb{Z}$ and there are some solutions.

Compute the Bézout identity by the **E**xtended **E**uclidean **A**lgorithm (EEA):

$$3.(-1) + (-4).(-1) = 1 \quad \Rightarrow \quad 3.(-2) + (-4).(-2) = 2.$$

$\Rightarrow$ this gives one solution $(x, y) = (-2, -2)$.

All solutions are $(x, y) = (-2 + 4a, -2 + 3a), a \in \mathbb{Z}$.

# Application of the EEA, 2

Chinese remaindering theorem : If $n, m \in \mathbb{Z}$ are coprime $\langle n, m\rangle = \langle 1\rangle$

There is an isomorphism between the two following rings:

$$\begin{array}{rcl} \mathbb{Z}/mn\mathbb{Z} & \simeq & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ a \bmod mn & \mapsto & a \bmod n \ , \ a \bmod m \\ (bun + avm) \bmod mn & \leftarrow & a \bmod n \ , \ b \bmod m \end{array}$$

Bézout identity:

$un + vm = 1$

---

Similarly, given 2 coprime polynomials $A, B \in \mathbb{k}[X]$ $\langle A, B\rangle = \langle 1\rangle$

There is an isomorphism between the two following rings:

$$\begin{array}{rcl} \mathbb{k}[X]/\langle AB\rangle & \simeq & \mathbb{k}[X]/\langle A\rangle \times \mathbb{k}[X]/\langle B\rangle \\ P \bmod AB & \mapsto & P \bmod A \ , \ P \bmod B \\ (QUA + PVB) \bmod AB & \leftarrow & P \bmod A \ , \ Q \bmod B \end{array}$$

Bézout identity:

$UP + VQ = 1$

# Part IV: Algebraic numbers

## Back to the rationals: $\Bbbk = \mathbb{Q}$

Let $\alpha \in \mathbb{C}$, and let $\mathbb{Q}[\alpha] := \{P(\alpha) \mid P \in \mathbb{Q}[X]\}$. This is a subring of $\mathbb{C}$.

Consider $\phi_\alpha : \mathbb{Q}[X] \to \mathbb{Q}[\alpha],\ P(X) \mapsto P(\alpha)$ .

This a ring homomorphism, that is onto by definition of $\mathbb{Q}[\alpha]$

Let $\ker \phi_\alpha := \{P \in \mathbb{Q}[X] | P(\alpha) = 0\}$ be its kernel.

1st case, $\ker \phi_\alpha = \{0\}$ : then $\alpha$ is a transcendental number.

2nd case, $\ker \phi_\alpha \neq \{0\}$, then $\alpha$ is an algebraic number.

By the first isomorphism theorem $\mathbb{Q}[X]/\ker \phi_\alpha \simeq \mathbb{Q}[\alpha]$ as rings.

Since $\mathbb{Q}[\alpha]$ is an integral domain, then $\ker \phi_\alpha$ must be a prime ideal (Lemma 2).

Assume that $\alpha$ is algebraic. Since $\ker \phi_\alpha \neq \{0\}$, there exists an unique irreducible monic polynomial $P$ such that $\langle P \rangle = \ker \phi_\alpha$.

**Definition 8** *$P$ is called the* minimal polynomial *of $\alpha$.*

# The field embedding problem

$\langle P \rangle$ generates the ideal of vanishing polynomial at $\alpha$.

$\mathbb{Q}[X]/\langle P \rangle$ is a field $\Rightarrow$ the ring $\mathbb{Q}[\alpha]$ also, denoted often $\mathbb{Q}(\alpha)$.

Let $\beta$ be another root of $P$ ($\alpha$ and $\beta$ are conjugate).

Then $\mathbb{Q}[\beta]$ is a field isomorphic to $\mathbb{Q}[X]/\langle P \rangle$.

An embedding $\sigma : \mathbb{Q}[X]/\langle P \rangle \hookrightarrow \mathbb{C}$ is an injective homomorphism, that induces the identity on $\mathbb{Q}$ ($\sigma(x) = x$ for all $x \in \mathbb{Q}$).

For each root $\alpha_1, \ldots, \alpha_n$ of $P$, there is an embedding $\sigma_i$ of $\mathbb{Q}[X]/\langle P \rangle$ whose image is $\mathbb{Q}(\alpha_i) \subset \mathbb{C}$.

Embedding problem: Among the fields $\mathbb{Q}(\alpha_i)$, $i = 1, \ldots, n$, which fields $\mathbb{Q}[X]/\langle P \rangle$ is it representing ? ( $\iff$ which embedding $\sigma_1, \ldots, \sigma_n$ choosing ?)

No answer, if necessary, numerical approximations of the roots of $P$ can be done then it is satisfactory.

# Computation in $\mathbb{Q}(\alpha)$ (1/2)

Because $\{1, X, \ldots, X^{n-1}\}$ is a basis of the $\mathbb{Q}$-vector space $\mathbb{Q}[X]/\langle P \rangle$, and because $\mathbb{Q}[X]/\langle P \rangle \to \mathbb{Q}[\alpha]$, $X \mapsto \alpha$ is an isomorphism, we deduce that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis of $\mathbb{Q}(\alpha)$.

To compute in $\mathbb{Q}(\alpha)$ we compute in $\mathbb{Q}[X]/\langle P \rangle$

Let $\beta$, $\gamma \in \mathbb{Q}(\alpha)$.

$\beta = \beta_0.1 + \beta_1.\alpha + \beta_2\alpha^2 + \cdots + \beta_{n-1}\alpha^{n-1}$, with $\beta_i \in \mathbb{Q}$.

$\gamma = \gamma_0.1 + \gamma_1.\alpha + \gamma_2\alpha^2 + \cdots + \gamma_{n-1}\alpha^{n-1}$, with $\gamma_i \in \mathbb{Q}$.

Let $P_\beta(X) = \sum_{i=0}^{n-1} \beta_i X^i \in \mathbb{Q}[X]$ and $P_\gamma(X) = \sum_{i=0}^{n-1} \gamma_i X^i \in \mathbb{Q}[X]$.

We have $P_\beta(\alpha) = \beta$ and $P_\gamma(\alpha) = \gamma$.

Addition: $\beta + \gamma$ is equal to $P_\beta(\alpha) + P_\gamma(\alpha)$, so $P_{\beta+\gamma} = P_\beta + P_\gamma$.

Multiplication: $\beta \,.\, \gamma$ is equal to $P_\beta(\alpha) \,.\, P_\gamma(\alpha)$, so $P_{\beta\,.\,\gamma} = P_\beta \,.\, P_\gamma \bmod P$.

## Computation in $\mathbb{Q}(\alpha)$ (2/2)

Division: Assume that $\beta \neq 0$. How to compute $\beta^{-1}$ ?

$\iff$ How to compute $(P_\beta \bmod P)^{-1}$ in the field $\mathbb{Q}[X]/\langle P \rangle$ ?

By Proposition 4, we compute the Bézout identity $uP_\beta + vP = 1$ using the EEA.

And $(P_\beta \bmod P)^{-1} = u \bmod P$ in $\mathbb{Q}[X]/\langle P \rangle$.

So $P_{\beta^{-1}} = u \Rightarrow \beta^{-1} = u(\alpha) = P_{\beta^{-1}}(\alpha)$.

# Effective primitive element theorem (1/2)

Let $\Bbbk$ be a finite extension of $\mathbb{Q}$, and let $n$ the degree $[\Bbbk : \mathbb{Q}]$ of the extension.

**Theorem 1** *There exists exactly $n$ distinct embeddings of $\Bbbk$.*

PROOF: *(No proof, admitted. It is not the purpose of this class.)*

**Corollary 1 (Theorem of the primitive element)** *There exists $\alpha \in \mathbb{C}$ such that $\Bbbk = \mathbb{Q}(\alpha)$. Such an $\alpha$ is called a primitive element of $\Bbbk$ over $\mathbb{Q}$.*

PROOF: *(On the blackboard...)*

---

**Definition 9** *A field $\mathbb{L}$ is an extension of a field $\mathbb{K}$ if $\mathbb{K} \subset \mathbb{L}$. The field $\mathbb{L}$ is then a $\mathbb{K}$-vector space, and we say that $\mathbb{L}|\mathbb{K}$ is a field extension.*

*If the dimension of $\mathbb{L}$ over $\mathbb{K}$ is finite, then the extension $\mathbb{L}|\mathbb{K}$ is said finite. This dimension is called the degree of the extension $\mathbb{L}|\mathbb{K}$, denoted $[\mathbb{L} : \mathbb{K}]$.*

# Effective primitive element theorem (2/2)

How to compute a primitive element $\alpha$ ?

Answer: There are a lot of possibilities **!** $\Rightarrow$ choose one at random...

In practice, $\mathbb{k}$ is given by some algebraic elements $\alpha_1, \ldots, \alpha_t$ so that $\mathbb{k} = \mathbb{Q}(\alpha_1, \ldots, \alpha_t)$. We assume that

Today, we assume $t = 2$, so $\mathbb{k} = \mathbb{Q}(\alpha_1, \alpha_2)$, and we know the degree $[\mathbb{k} : \mathbb{Q}] := n$

**Proposition 5** *Let $0 < \epsilon < 1$ be fixed. Let $M \in \mathbb{N}$, verifying $M \geq \frac{n(n-1)}{4\epsilon}$.*

*Let $c \in [-M; M]$ be an integer chosen at random.*

*Then $\alpha_1 + c\alpha_2$ is* not *a primitive element for $\mathbb{k}$ ($\iff \mathbb{Q}(\alpha_1 + c\alpha_2) \subsetneq \mathbb{k}$) with probability $\leq \epsilon$.*

PROOF: *(On the blackboard...)* □