MODEL – Basic algebraic structures

September 29, 2017

This course is taught by:

- Mohab safey El Din, `Mohab.Safey@lip6.fr`
- Jeremy Berthomieu, `Jeremy.Berthomieu@lip6.fr`

The evaluation is done through:

- short exams (at least 5 during the semester), evaluating how you learnt the course ;
- one mid-term exam evaluating your ablity to manipulate the concepts taught during the first half of the semester ;
- one final exam evaluating your ability to manipulate the concepts taught during the whole semester (but with an emphasis on the second half).

All these items count for 1/3 of the final grade.

Objectives of the course and outline. The course provides an introduction to fundamental and basic computing methodologies used in many areas of computer science (cryptography, high-performance computing, big data, operational research, imagery, etc.). These methods rely either on *exact* or *approximate* computation.

The first half of the course focuses on exact computation. The plan is as follows:

1. basic mathematical notions which are needed at the Master degree level ;
2. arithmetic algorithms on numbers, polynomials, and matrices ;
3. Euclide's algorithm and its applications ;
4. Algorithms in linear algebra and complexity equivalences ;
5. Algorithms for solving bivariate systems.

Groups.

Definition 1 (Group)**.** *Let G be a set equipped with the binary operation $\star$. One says that $(G, \star)$ is a group if the following hold:*

1. *the operation $\star$ is associative (i.e. $\boldsymbol{x} \star (\boldsymbol{y} \star \boldsymbol{z}) = (\boldsymbol{x} \star \boldsymbol{y}) \star \boldsymbol{z}$) ;*
2. *there exists $\boldsymbol{e} \in G$ (called identity element) such that for all $\boldsymbol{x} \in G$, $\boldsymbol{x} \star \boldsymbol{e} = \boldsymbol{e} \star \boldsymbol{x} = \boldsymbol{x}$;*
3. *for all $\boldsymbol{x} \in G$, there exists $\boldsymbol{y} \in G$ (called invert of $\boldsymbol{x}$) such that $\boldsymbol{x} \star \boldsymbol{y} = \boldsymbol{e}$. Usually, such an element $\boldsymbol{y}$ is denoted by $\boldsymbol{x}^{-1}$.*

A group is said to be abelian (or commutative) if the binary operation is commutative. Also, a group is said to be finite when its cardinality is finite.

Proposition 2. *Let $(G,.)$ be a group and, a and b be in G. Then $(a.b)^{-1} = b^{-1}.a^{-1}$.*

Proof. It suffices to check that $(a.b).(b^{-1}.a^{-1}) = e_G$ (where e_G is the identity element of G). This is immediate

$$(a.b)^{-1}.b^{-1}.a^{-1} = a.(b.b^{-1}).a^{-1} = a.e_G.a^{-1} = a.a^{-1} = 1.$$

□

Definition 3 (Group homomorphism)**.** *Let $(G,\star)$ and $(G',.)$ be two groups. A map $f : (G,\star) \to (G',.)$ is a group homomorphism if for any couple $(a,b) \in G \times G$, $f(a \star b) = f(a).f(b)$.*

Moreover, when f is a bijection, then f is said to be a group isomorphism ; besides G and G' are said to be isomorphic.

Rings.

Definition 4 (Ring)**.** *Let R be a set equipped with two binary operations $+$ and $\times$. One says that $(R,+,\times)$ is a ring if the following holds:*

1. *$(R,+)$ is an abelian group ;*
2. *$\times$ is an associative binary operation ;*
3. *$\times$ is distributive with respect to $+$.*

- Unitary rings are those rings which contain an identity element for $\times$ – this one is usually denoted by 1_R ;
- A ring is said to be commutative when $\times$ is commutative ;
- A ring is said to be integral when it is commutative and when for all $(\boldsymbol{x},\boldsymbol{y}) \in R \times R$, $\boldsymbol{x} \times \boldsymbol{y} = 0$ implies $\boldsymbol{x} = 0$ or $\boldsymbol{y} = 0$.

  When this occurs, one says that R does not admit a zero divisor.

Definition 5 (Ring homomorphisms)**.** *Let $(R,+,\times)$ and $(S,\star,\circ)$ be two rings. One says that a map $\phi : R \to S$ is a ring homomorphism if for all $(a_1,a_2) \in R \times S$, the following holds:*

- $\phi(a_1 + a_2) = \phi(a_1) \star \phi(a_2)$;
- $\phi(a_1 \times a_2) = \phi(a_1) \circ \phi(a_2)$.

The set $\ker \phi = \{a \in R \mid \phi(a) = 0_S\}$ is called the kernel of ϕ. When a ring homomorphism is bijective, one says that it is a ring isomorphism and both rings R and S are isomorphic to each other.

Observe that not all rings are ordered. This yields some difficulty for defining a (Euclidean) division over rings. To bypass this difficulty, one introduces a function which embeds the considered ring in $\mathbb{N}$.

Definition 6 (Euclidean division)**.** *Let $(R,+,.)$ be a ring. One says that R is equipped with a Euclidean division if there exists a map $h : R - \{0\}$ in $\mathbb{N}$ such that for all (a,b) in $R - \{0\}$ the following holds:*

- *$h(a.b) \geq h(a)$;*
- *there exists a couple $(q,r) \in R \times R$ such that $a = b.q + r$ with either $r = 0$ or $h(r) < h(b)$.*

Using the above notations, q is said to be the quotient and r is said to be the remainder of the Euclidean division.

Definition 7. *A ring R is said to be Euclidean if it is integral and is equipped with a Euclidean division.*

Fields.

Definition 8 (Field)**.** *Let $\mathbb{K}$ be a set equipped with two binary operations $+$ and $\times$. On says that $(\mathbb{K}, +, \times)$ is a field if the following holds:*

1. *$(\mathbb{K}, +, \times)$ is a unitary commutative ring ;*
2. *the identity elements of $+$ and $\times$ (denoted respectively $0_{\mathbb{K}}$ and $1_{\mathbb{K}}$) do not coincide ;*
3. *$(\mathbb{K}^\star, \times)$ is a group (where $\mathbb{K}^\star = \mathbb{K} - \{0\}$).*

A field is said to be finite when its cardinality is finite.

Theorem 9. *Any field is an integral ring. Any finite integral ring is a field.*

Definition 10 (Subfield)**.** *A subset $\mathbb{L}$ of a field $(\mathbb{K}, +, \times)$ is a subfield of $\mathbb{K}$ if the following holds:*

- $1_{\mathbb{K}} \in \mathbb{L}$
- *$(\mathbb{L}, +)$ is a subgroup of $\mathbb{K}$*
- *$(\mathbb{L} - \{0_{\mathbb{K}}\}, \times)$ is a subgroup of $\mathbb{K} - \{0\}$.*

Proposition 11. *Let $(\mathbb{K}, +, \times)$ be a field and $(\mathbb{L}+, \times)$ be a subfield of $\mathbb{K}$. Then, $\mathbb{K}$ is a $\mathbb{L}$-vector space.*

Vector spaces.

Definition 12 (Vector space)**.** *A set $(E_{\mathbb{K}}, +, .)$ is a vector space over a field $(\mathbb{K}, \oplus, \star)$ (also called $\mathbb{K}$-vector space) if the following holds, for all $\alpha \in \mathbb{K}$, and $(\boldsymbol{u}, \boldsymbol{v}) \in E \times E$:*

- *vector addition satisfies the standard axioms of addition in a number system (commutativity, associativity, identity element, inversion);*
- $\alpha.(\boldsymbol{u} + \boldsymbol{v}) = \alpha.\boldsymbol{u} + \alpha.\boldsymbol{v}$;
- $(\alpha + \beta).\boldsymbol{v} = \alpha.\boldsymbol{v} + \beta.\boldsymbol{v}$;
- $(\alpha \star \beta).\boldsymbol{v} = \alpha.(\beta.\boldsymbol{v})$;
- $1_{\mathbb{K}}\boldsymbol{v} = \boldsymbol{v}$.

Elements of the field $\mathbb{K}$ will be called scalars.

Definition 13. *Let E be a $\mathbb{K}$-vector space. One says that elements $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell$ are linearly dependent if there exist $\alpha_1, \ldots, \alpha_\ell$ in $\mathbb{K}$, not all zero, which satisfy*

$$\alpha_1\boldsymbol{v}_1 + \cdots + \alpha_\ell\boldsymbol{v}_\ell = 0.$$

Vectors of the above form are called linear combinations of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell$.

Lemma 14. *We reuse the notations introduced above. The vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell$ in E are linearly dependent if either $\boldsymbol{v}_1 = \boldsymbol{0}$ or for some r, $\boldsymbol{v}_r =$ is a linear combination of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{r-1}$.*

Definition 15. *The vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ span the $\mathbb{K}$-vector space E if for any $\boldsymbol{v} \in E$, there exist $\alpha_1, \ldots, \alpha_n$ in $\mathbb{K}$ such that*

$$\boldsymbol{v} = \alpha_1\boldsymbol{v}_1 + \cdots + \alpha_n\boldsymbol{v}_n.$$

They form a basis of E if they are linearly independent. The cardinality of a basis of E is called the dimension of the vector space E. A vector space with a finite basis is called finite dimensional.