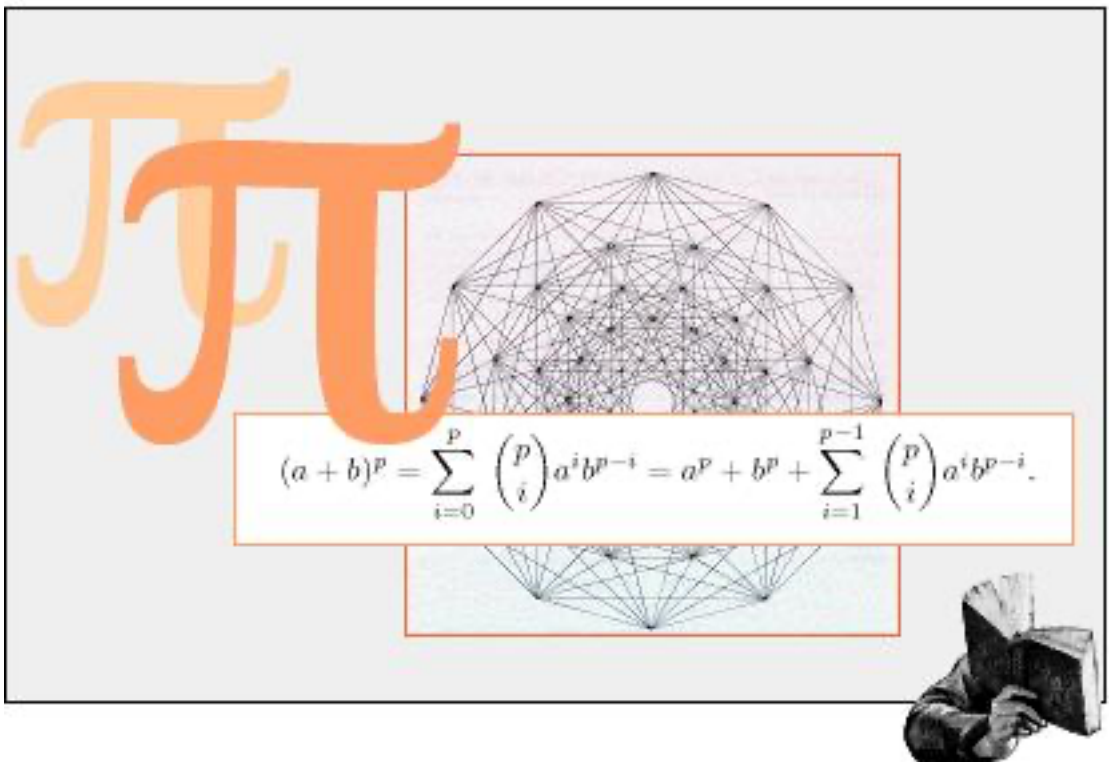
Università di Trieste
Corso di Laurea in Informatica

Note del corso di
Strutture Algebriche

Michela Brundu



anno accademico 2007/08

Note del corso di Strutture algebriche

Michela Brundu

Indice

Chapter 1
Topics in Groups Theory

Definition 1.1. A set G together with an operation $\mu : G \times G \longrightarrow G$ is called a *group* if

i) μ is associative (i.e. $\mu(\mu(x,y),z) = \mu(x,\mu(y,z))$, for every $x,y,z \in G$);

ii) there exists an element e of G, called *neutral element*, such that $\mu(e,x) = \mu(x,e) = x$, for every $x \in G$;

iii) for every $x \in G$, there exists an element $x' \in G$, called *inverse* of x, such that $\mu(x,x') = \mu(x',x) = e$.

If, in addition, the following property holds:

iv) $\mu(x,y) = \mu(y,x)$, for every $x,y \in G$,

we say that G is a *commutative* or *abelian* group.

Notation. Usually we denote $\mu(x,y)$ by xy (or $x \cdot y$) or by $x+y$, and we say that G is, respectively, a *multiplicative* or an *additive* group. Note that the additive notation '+' is normally used for abelian groups. In a multiplicative group (respectively additive), the neutral element is usually denoted by 1_G or simply by 1 (resp. 0_G or 0) and the inverse of an element x by x^{-1} (resp. by $-x$).

Example 1.1.1. Here are some examples of groups (the notations here given, which are almost standard, will be used during all the notes).
$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ are the groups of, respectively, *integer numbers, rational numbers, real numbers, complex numbers*, w.r.t. the addition;
$\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$, which are the groups of, respectively, not-zero rational, not-zero real and not-zero complex numbers w.r.t. the product;
the set $(\mathbb{R}^n,+)$ of n-uples of real numbers w.r.t. the addition;
the set $(M_{m,n}(\mathbb{R}),+)$ of the $m \times n$ real matrices w.r.t. the usual addition of matrices; the set $(GL_n(\mathbb{R}),\cdot)$ of invertible matrices of order n w.r.t. the product of matrices.
Some other examples of groups are:
the set $G := \{f : A \longrightarrow A \mid f \text{ is bijective}\}$ w.r.t. the composition of maps, where A is any set;
the set $\{f : \mathbb{R} \longrightarrow \mathbb{R}\}$, with the addition defined pointwise;
the set $S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$, w.r.t. the product of $\mathbb{C}$; the set $\{z \in \mathbb{C} \mid z^n = 1\}$, again w.r.t. the product of $\mathbb{C}$ (n is any natural number).
Another class of groups is that given by the symmetries of some geometric figures. For instance, if X is a square, then the set of symmetries of X is a group of eight elements (denoted by D_8).

Definition 1.2. A *subgroup* of G is a subset H of G which itself forms a group with respect to the operation defining G; we will write $H \leq G$ (or $H < G$, if the subgroup H is proper, i.e. a proper subset of G).

Remark 1.3. It is easy to verify that a non-empty subset H of G is a subgroup if and only if $xy^{-1} \in H$ for every $x,y \in H$.

Example 1.3.1. The following are examples of subgroups:
$(\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C},+)$.

$\{z \in \mathbb{C} \mid z^n = 1\} \leq S^1 \leq \mathbb{C}^\times$.
If $n \in \mathbb{Z}$ is any element, we shall denote by (n) the set $\{mn \mid m \in \mathbb{Z}\}$; then (n) is a subgroup of $(\mathbb{Z}, +)$.

Proposition 1.4. *Given two subgroups H and J of G, then $H \cap J$ is a subgroup of G. More generally, if H_i, $i \in I$, is a family of subgroups of G, then $\bigcap_{i\in I} H_i$ is a subgroup of G.*

Proof. Let $x, y \in H \cap J$; then, since both H and J are subgroups, $xy^{-1} \in H$ and $xy^{-1} \in J$. So $xy^{-1} \in H \cap J$. Analogously for the case of any family of subgroups. □

Definition 1.5. The smallest subgroup of a group G containing two given subgroups H and J of G is called *product* of H and J and it is denoted by HJ.

Definition 1.6. If for G we use the additive notation, hence if $(G, +)$ is an abelian group and H, J are subgroups of G, then the smallest subgroup of G which contains H and J is denoted by $H + J$ and called *sum* of H and J.

Example 1.6.1. For example, take $(2), (3) \subseteq \mathbb{Z}$, then the subgroup $(2) + (3)$ is $\mathbb{Z}$, while the subgroup $(4) + (6)$ is (2).

Definition 1.7. Let G be a group, H be a subgroup and $g \in G$; we call, respectively, *left coset* and *right coset* of H with respect to g the two subsets:

$$gH = \{gh \mid h \in H\} \qquad Hg = \{hg \mid h \in H\}.$$

If the number of left (right) cosets of a subgroup H of G is finite, we say that H is of *finite index*. Such a number is called *index* of H in G and it is denoted by $[G : H]$.
If gH is a coset, g is called *representative* of gH.

Note that two representatives of the same coset are equal up to an element of H; i.e. $gH = fH$ if and only if there exists some $h \in H$ such that $g = fh$.

Definition 1.8. A subgroup H of G is a *normal subgroup* if $gH = Hg$ for every $g \in G$; we will write $H \triangleleft G$.

Example 1.8.1. Let $D_n := \{aI_n \mid a \in \mathbb{R}, a \neq 0\}$ (I_n is the $n \times n$ identity matrix). Then D_n is a normal subgroup of $GL_n(\mathbb{R})$.

Proposition 1.9. *Let G be a group and $H \leq G$. The following facts are equivalent:*
i) $H \triangleleft G$;
ii) $gHg^{-1} \subseteq H$ for all $g \in G$ (where $gHg^{-1} := \{ghg^{-1} \mid h \in H\}$);
iii) $gHg^{-1} = H$ for all $g \in G$.

Proof. i) ⇒ ii). If $x \in gHg^{-1}$, then $x = ghg^{-1}$, for a suitable $h \in H$. But $gh = h'g$ by assumption, so $x = h' \in H$.
The other parts of the proof are analogous. □

Remark 1.10. If H is a normal subgroup of G, let us consider the set $\{gH \mid g \in G\}$. In this set we define a multiplication by: $g_1H \cdot g_2H := (g_1g_2)H$. This operation is well-defined, because H is normal. In fact if $g_1H = f_1H$, then $g_1 = f_1h$, for some $h \in H$. We

want to show that $g_1H \cdot g_2H = f_1H \cdot g_2H$, i.e. that $(g_1g_2)H = (f_1g_2)H$ or, equivalently, that $g_1g_2 = f_1g_2k$, for some $k \in H$. By assumption $g_1g_2 = f_1hg_2$ and $hg_2 = g_2k$, for a suitable $k \in H$, since H is normal. So we are done.
Moreover, it is easy to verify that the coset $1_GH = H$ is the neutral element in the set $\{gH \mid g \in G\}$ with respect the above product. Finally note that, for any $g \in G$, it holds: $(gH)^{-1} = g^{-1}H$.
The given set $\{gH \mid g \in G\}$ becomes in this way a group.

Definition 1.11. If H is a normal subgroup of G, the group $\{gH \mid g \in G\}$, endowed with the product defined above, is called *quotient group* of G by H and is denoted by G/H.

Review 1.12. Let us briefly remind the basic notions about equivalence relations.
Let X be a given set. A *relation* $\mathcal{R}$ on X is a subset of the Cartesian product of X with itself, $X \times X$. Hence any particular element, $x \in X$ *has the relation* $\mathcal{R}$ with any element $y \in X$ if and only if $(x, y) \in \mathcal{R}$.
Equivalence relation is a special case of relation. Let X be a set and let $x, y, z \in X$. An *equivalence relation* $\sim$ on X is a relation such that:

- Reflexive Property: $x \sim x$, for all $x \in X$.
- Symmetric Property: if $x \sim y$, then $y \sim x$.
- Transitive Property: if $x \sim y$ and $y \sim z$, then $x \sim z$.

Here $x \sim y$ means that (x, y) is an element of the equivalence relation $\sim$.
In the language of sets, one can rewrite the three properties of equivalence relation as follows:

- Reflexive Property: $(x, x) \in \sim$, for all $x \in X$.
- Symmetric Property: if $(x, y) \in \sim$, then $(y, x) \in \sim$.
- Transitive Property: if $(x, y), (y, z) \in \sim$, then $(x, z) \in \sim$.

Example 1.12.1. There are two obvious equivalence relations on a set X that follow easily from the definition: the relation of equality and the Cartesian product. The relation of equality is defined by $x \sim y$ if and only if $x = y$ in X. This relation is sometimes called the *trivial equivalence relation.* This relation is also the smallest possible equivalence relation on X since every other equivalence relation must contain this one as a subset.
Another equivalence relation, the Cartesian product $X \times X$, is the largest relation on X. That $X \times X$ is the largest relation follows from the definition of relation on X.
Finally, *clockwork arithmetic* provides another example of a simple equivalence relation.

Definition 1.13. Let X be a set and $\sim$ be an equivalence relation on X. Let x be an element of X. The *equivalence class* of x is the subset of X that contains all elements that are equivalent to x under $\sim$. In symbols, the equivalence class of x is

$$[x] := \{y \in X \mid x \sim y\}.$$

Let us remark that the equivalence class representative is, in general, not unique. If both x and y are in the same equivalence class, then which element should represent the equivalence class, x or y? The answer is either one. To prove that the element that represents an equivalence class does not matter, one easily shows that the equivalence class

$[x]$ and the equivalence class $[y]$ coincide for $x \sim y$.
A *Partition Theorem* holds: let X be a non-empty set and $\sim$ be an equivalence relation on X. The equivalence classes of $\sim$ form a partition (a disjoint collection of non-empty subsets whose union is the whole set) of X.
A converse of this partition theorem also holds.

Definition 1.14. Let X be a non-empty set and $\sim$ be an equivalence relation on X. Then the set consisting of all the equivalence classes of $\sim$ is called *quotient set* of X modulo $\sim$. In symbols:

$$X/\sim := \{[x] \,|\, x \in X\}.$$

Let us come back to quotient groups.

Remark 1.15. Let H be a normal subgroup of a group G; then H defines the following relation: $x \sim y \Leftrightarrow \ xy^{-1} \in H$, which is easily seen to be an equivalence relation on G. Moreover the quotient set $G/\sim$ turns out to be G/H, since $[g] = \{x \in G \mid x \sim g\} = \{x \mid xg^{-1} \in H\} = Hg = gH$.

Example 1.15.1. If $n \in \mathbb{Z}$, then, since $\mathbb{Z}$ is abelian, (n) is a normal subgroup of it. The quotient $\mathbb{Z}/(n)$ is denoted by $\mathbb{Z}_n$. According to 1.15, two elements $a, b \in \mathbb{Z}$ are equivalent (hence are the same element in $\mathbb{Z}_n$) if and only if $a - b$ is divisible by n. Namely:

$$a \sim b \Leftrightarrow a - b \in (n) \Leftrightarrow a - b = nh.$$

Therefore, again from 1.15, the coset of a is the set of elements equivalent to a (denoted by $[a]$) is

$$\begin{aligned}[a] &= \{b \in \mathbb{Z} \,|\, a \sim b\} = \\ &= \{b \in \mathbb{Z} \,|\, b = a + nh, \text{where } h \in \mathbb{Z}\} = \\ &= \{\ldots, -2n + a, -n + a, 0 + a, n + a, 2n + a, \ldots\}.\end{aligned}$$

It is clear that, if $b \in \mathbb{Z}$ is any integer and we divide b by n, then $b = nh + a$, where a is the remainder of the division, so $0 \leq a \leq n - 1$. Therefore, from the above computation, it follows that $[b] = [a]$.
In this way we prove that $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$. In particular, $\mathbb{Z}_n$ is a finite group of n elements.

Example 1.15.2. Let G be the subgroup of $\mathbb{R}^\times$ given by all the positive real numbers. It is easy to verify that $\mathbb{C}^\times/G$ can be identified with the group S^1 defined above. In fact, two elements $a + \mathrm{i}b, c + \mathrm{i}d$ of $\mathbb{C}^\times$ are equivalent w.r.t. G if there exists $\lambda \in G$ s.t. $a + \mathrm{i}b = \lambda(c + \mathrm{i}d)$; in particular any element $a + \mathrm{i}b$ is equivalent to $(a + \mathrm{i}b)/\sqrt{a^2 + b^2} \in S^1$.

Definition 1.16. Let G and G' be two groups; a map $f : G \longrightarrow G'$ is a *group homomorphism* if $f(g_1 g_2) = f(g_1) f(g_2)$, for every $g_1, g_2 \in G$. (Note that $f(1_G) = 1_{G'}$ and that $f(g^{-1}) = f(g)^{-1}$).
A group homomorphism which is injective, surjective or bijective is called, respectively, a *group monomorphism, epimorphism, isomorphism.* To mean that there exists an isomorphism between G and G' we shall write $G \cong G'$.

A group homomorphism from a group to itself is called an *endomorphism*; if it is also bijective, it is called an *automorphism.*

Examples 1.16.1. If H, G are groups, s.t. $H \leq G$, then the inclusion map $i : H \longrightarrow G$ is a group homomorphism.
Let us try to find all the group homomorphisms $f : \mathbb{Z} \longrightarrow \mathbb{Z}$. Set $m := f(1)$. If n is any positive integer, then $f(n) = f(1+\cdots+1) = f(1)+\cdots+f(1) = nm$, and if n is any negative integer (so $-n$ is positive), then $f(n) = -f(-n) = -f(1 + \cdots + 1) = -(-nm) = nm$. Therefore we proved that, if $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ is any homomorphism, then there exists an $m \in \mathbb{Z}$ s.t. $f(n) = nm$ for any $n \in \mathbb{Z}$. Conversely, if $m \in \mathbb{Z}$, then it is easy to see that the map $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by $f(n) = nm$ is a group homomorphism.
Let $\phi : \mathbb{C}^\times \longrightarrow S^1$ be defined by: $\phi(a + \mathrm{i}b) := (a + \mathrm{i}b)/\sqrt{a^2 + b^2}$. It is easy to see that ϕ is a group homomorphism.
Let $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$ be the determinant map. It is well known that $\det(AB) = \det(A)\det(B)$ (Binet theorem), hence det is a homomorphism.
Let $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ be defined by

$$f(a, b) := \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

The map f gives a rotation in the plane $\mathbb{R}^2$ of an angle ϕ and is a group homomorphism.

Definition 1.17. Let $f : G \longrightarrow G'$ be a group homomorphism; the set $\{g \in G \mid f(g) = 1_{G'}\}$ is called the *kernel* of f and it is denoted by $\ker(f)$. The image of f will be denoted by $\mathrm{Im}\,(f)$ (it is the set $\{f(g) \mid g \in G\}$).

Example 1.17.1. Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ be the homomorphism $f(n) := mn$ for a fixed $m \in \mathbb{Z}$. Then $\mathrm{Im}\, f = (m)$ and $\ker f = (0)$, if $m \neq 0$.
If $\mathbb{C}^\times \longrightarrow S^1$ is defined as in 1.16.1, then $\ker(f) = \{a \in \mathbb{R} \mid a > 0\}$, i.e. it is the group G of 1.15.2.
If det is the map considered in 1.16.1, then ker(det) is denoted by $SL_n(\mathbb{R})$, and is called the *special linear group.*

Theorem 1.18. *If $f : G \longrightarrow G'$ is a group homomorphism, then:*
i) $\ker(f)$ *and* $\mathrm{Im}\,(f)$ *are subgroups of G and G', respectively;*
ii) $\ker(f)$ *is a normal subgroup of G;*
iii) f is injective if and only if $\ker(f) = 1$.

Proof. i) Let $x, y \in \ker(f)$; then $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = 1_G$; therefore $xy^{-1} \in \ker(f)$. Let now $z, t \in \mathrm{Im}\,(f)$; hence there exist $x, y \in G$ such that $z = f(x)$ and $t = f(y)$. Consider $xy^{-1} \in G$; $f(xy^{-1}) = f(x)f(y)^{-1} = zt^{-1}$; so $zt^{-1} \in \mathrm{Im}\,(f)$.
ii) Let us take $g \in G$ and $h \in \ker(f)$. Then $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = 1_{G'}$; hence $ghg^{-1} \in \ker(f)$, for all $g \in G$.
iii) Assume f is injective; then take $h \in \ker(f) : f(h) = 1_{G'} = f(1_G)$, so $h = 1_G$.
Conversely, let $\ker(f) = \{1_G\}$ and assume there exist $x, y \in G$ such that $f(x) = f(y)$.
Then $f(x)f(y)^{-1} = 1_{G'}$, so $f(xy^{-1}) = 1_{G'}$, i.e. $xy^{-1} \in \ker(f) = \{1_G\}$; therefore $x = y$.
□

Definition 1.19. If $H \leq G$ and $g \in G$, then the subgroup $g^{-1}Hg$ is said *conjugate* to H w.r.t. g.

Note that, by 1.9, that H has no conjugate subgroup (shortly: H is self-conjugate) if and only if it is normal.

Remark 1.20. Let $H \lhd G$; then the map $\pi : G \longrightarrow G/H$ defined by $\pi(g) = gH$ is a surjective homomorphism (called *canonical homomorphism* or *canonical projection* of G onto G/H) and $\ker(\pi) = H$.

Theorem 1.21. *(Fundamental theorem) Let $f : G \longrightarrow G'$ be a group homomorphism, $K = \ker(f)$ and $\pi : G \longrightarrow G/K$ be the canonical projection. Then there exists an injective homomorphism $h : G/K \longrightarrow G'$ such that $f = h \circ \pi$. In particular,* $\mathrm{Im}\,(f) \cong G/K$.

Proof. Let us define $h : G/K \longrightarrow G'$ by $h(gK) := f(g)$. We have to show that h is well defined, i.e. if $g_1K = g_2K$ then $f(g_1) = f(g_2)$. Since $K \lhd G$, from $g_1K = g_2K$ one has $g_2^{-1}g_1 \in K = \ker(f)$; so $f(g_2^{-1}g_1) = 1_{G'}$ i.e. $f(g_1) = f(g_2)$.
Moreover h is a homomorphism by definition, since f is a homomorphism.
Assume, finally, that $h(gK) = 1_{G'}$; this means that $f(g) = 1_{G'}$, so $g \in K$; this implies $gK = K = 1_{G/K}$. By definition $h(\pi(g)) = h(gK) = f(g)$. So, from $f = h \circ \pi$ and from the surjectivity of π, it follows that $\mathrm{Im}\,(f) = \mathrm{Im}\,(h) \cong G/K$, since h is injective. □

Definition 1.22. Let G be a group and $g_1, \ldots, g_n$ be elements of G. We call *subgroup generated by* $g_1, \ldots, g_n$, and we denote it by $\langle g_1, \ldots, g_n \rangle$, the smallest subgroup containing those elements, i.e. $\langle g_1, \ldots, g_n \rangle := \{x_1 \cdots x_p \mid x_i \in \{g_1, \ldots, g_n, g_1^{-1}, \ldots g_n^{-1}\}, p \in \mathbb{N}\}$.
In particular, $\langle g \rangle = \{g^p, p \in \mathbb{Z}\}$ is called *cyclic subgroup generated by* g.
If $G = \langle g \rangle$ for some $g \in G$, we say that G is a *cyclic group*.

Example 1.22.1. Let $a \in \mathbb{C}^\times$ s.t. $|a| = 1$. Using the trigonometric notation, let $a = \cos\phi + \mathrm{i}\sin\phi$. Then

$$\langle a \rangle \cong \begin{cases} \mathbb{Z}_n \text{ if } 2\pi/\phi = m/n \in \mathbb{Q} \ (m, n \text{ coprime}, \ n > 0) \\ \mathbb{Z} \quad \text{if } 2\pi/\phi \notin \mathbb{Q}. \end{cases}$$

Definition 1.23. The *order* of a group G is the number of its elements and it is denoted by $|G|$; G is *finite* if it has finite order. If $g \in G$, the *order* of g is $|\langle g \rangle|$, simply denoted by $|g|$.

Remark 1.24. Every subgroup of a cyclic group is cyclic; every quotient of a cyclic group is cyclic. In particular, if $G \leq \mathbb{Z}$ is a subgroup of $\mathbb{Z}$, then it is cyclic, hence it is of the form (n) for a suitable $n \in \mathbb{Z}$.
Moreover, if G is a cyclic group, then two possibilities can arise: either it is finite of order n and so isomorphic to $\mathbb{Z}_n$, or it is infinite and so it is isomorphic to $\mathbb{Z}$. To see this, suppose that $G =< g >$ and consider the following map:

$$f : \mathbb{Z} \longrightarrow G$$

defined by $a \mapsto g^a$. Clearly f is an epimorphism and

$$\ker(f) = \begin{cases} (0) \\ (n) \end{cases}$$

If $\ker(f) = (0)$, then $G \cong \mathbb{Z}$; if $\ker(f) = (n)$, then $G \cong \mathbb{Z}_n$ (see thm. 1.21).

Example 1.24.1 It is easy to verify that the set of the roots of $x^n - 1$ is an (abelian) subgroup of $\mathbb{C}^\times$ (see 1.1.1). It is well-known that these roots are distinct; for instance, using the trigonometric notation, those roots have the form

$$\varepsilon_k = \cos(2(k-1)\pi/n) + \mathrm{i}\sin(2(k-1)\pi/n)$$

for $k = 1, \ldots, n$.
So the (multiplicative) group $\{\varepsilon_1 = 1, \ldots, \varepsilon_n\}$ of nth roots of unity has order n; it is usually denoted by C_n.
Since $\varepsilon_k = \varepsilon_2^{k-1}$, for all k, then C_n is cyclic; therefore $C_n \cong \mathbb{Z}_n$. A generator of C_n is called a *primitive* nth root of unity.

Theorem 1.25. *(Lagrange) Let G be a finite group and $H \leq G$; then $|H|$ divides $|G|$.*

Proof. Just note that G can be partitioned as the union of a (finite) number of disjoint cosets gH, each containing $|H|$ elements. □

Corollary 1.26. *Let G be a finite group and $H \triangleleft G$; then $|G|/|H| = |G/H|$.*

Proof. The thesis follows from the proof of 1.25, noting that the number of the cosets gH is $|G/H|$ by definition. □

Example 1.26.1. As an example of Lagrange theorem, let us consider the group $G := \mathbb{Z}_{15}$ and its subgroup $H := \{0, 5, 10\}$. Then (note that here we use the additive notation): $0 + H = 5 + H = 10 + H = \{0, 5, 10\}$, $1 + H = 6 + H = 11 + H = \{1, 6, 11\}$, $2 + H = 7 + H = 12 + H = \{2, 7, 12\}$, $3 + H = 8 + H = 13 + H = \{3, 8, 13\}$, $4 + H = 9 + H = 14 + H = \{4, 9, 14\}$, hence the elements of G are divided into five classes of three elements each, as expected.

A natural question arises about the existence and the number of "substantially different" groups of a given order. More precisely, if $n \in \mathbb{N}$, we can consider the family of groups of order n. If this family is non empty, we can consider the following equivalence relation on it: two groups of order n, say G and H, are equivalent if there exists a group isomorphism from G to H. We call *type* of G the equivalence class of G.

Definition 1.27. For each positive integer n, let us denote by $\nu(n)$ the number of different types of groups of order n.

Remark 1.28. For each positive integer n, there exists at least one group of order n (i.e. $\nu(n) \geq 1$, for all n). In fact it is enough to consider, for each n, the additive group $\mathbb{Z}_n$.

Proposition 1.29. *For each prime number p, $\nu(p) = 1$.*

Proof. Let G be a group of order p prime. Take any element $g \in G$, $g \neq 1$. Then, as a consequence of Lagrange theorem, the subgroup $\langle g \rangle$ of G must be G, hence G is cyclic and we already observed that all the cyclic groups of fixed order are isomorphic (see 1.24). □

Corollary 1.30. *If $|G|$ is a prime number p, then $G \cong \mathbb{Z}_p$; in particular G is abelian since cyclic.* □

Chapter 2
Topics in Rings Theory

Definition 2.1. A *ring* is a non-empty set R together with two binary operations $+$, $\cdot$ and two distinguished elements $0_R, 1_R$ (or simply $0, 1$) in R such that $(R, +)$ is an abelian group (0 is its neutral element), the product $\cdot$ is associative (i.e. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$)), 1 is its neutral element, and the following distributive laws

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

hold for all $a, b, c \in R$.
A ring R is *commutative* if $ab = ba$ for all $a, b \in R$.

If $S \subseteq R$, then S is a *subring* of R if $1, 0 \in S$ and $+, \cdot$ induce a ring structure on S. Clearly the intersection of any set of subrings of R is a subring of R; hence if A is a subset of R, one can define the *subring generated* by A to be the intersection of all subrings of R which contain A. This is characterized by the properties: it is a subring, it contains A, and it is contained in every subring containing A.
In the sequel, we shall usually omit the symbol '$\cdot$' for the product.

Examples 2.1.1. 1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all rings. Moreover $\mathbb{Z}$ is a subring of $\mathbb{Q}$ which is a subring of $\mathbb{R}$, which is a subring of $\mathbb{C}$.
2) All the groups $\mathbb{Z}_n$ (defined in Ch.I, 1.15.1) are rings. The product is the product induced by $\mathbb{Z}$. More precisely, for $[a], [b] \in \mathbb{Z}_n$, we set $[a] \cdot [b] := [a \cdot b]$.
3) If A is any set, let $\Gamma := \{f : A \longrightarrow \mathbb{R}\}$. Then we can define in Γ the sum and the product pointwise, and with these operations Γ becomes a ring (0_Γ and 1_Γ are the functions which send every element of A to $0_\mathbb{R}$ and to $1_\mathbb{R}$, respectively).
4) Let $\mathbb{Z}[\sqrt{2}]$ be the set of the real numbers of the form: $m + \sqrt{2}n$ $(m, n \in \mathbb{Z})$. Then $\mathbb{Z}[\sqrt{2}]$ is a subring of $\mathbb{R}$.
5) Let $R = M_{n,n}(\mathbb{R})$ be the set of all $n \times n$ matrices over $\mathbb{R}$. Then $(R, +)$ is an abelian group (see Ch.I, 1.1.1) and with the multiplication row by column it becomes a ring.
All the previous examples are commutative rings, except 5).

Let R be any ring. Here we list some properties, which are an easy consequence of the axioms of rings. For instance, it holds: $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$. If $a \in R$, then $a \cdot 0 = 0 \cdot a = 0$. If $n \in \mathbb{Z}$, then by na we mean $a + a + \cdots + a$ (n times, if n is positive), or $-a - a - \cdots - a$ ($-n$ times, if n is negative). Then it holds:

$$n(a + b) = na + nb;$$
$$(n + m)a = na + ma;$$
$$(nm)a = n(ma);$$
$$(nm)(ab) = (na)(mb)$$

for all $m, n \in \mathbb{Z}$ and all $a, b \in R$.

Definition 2.2. A ring is called a *domain* (or an *integral domain*) if the condition

$$a, b \in R, \quad ab = 0 \quad \Rightarrow \quad a = 0 \text{ or } b = 0,$$

holds.
Note that in a domain the cancellation law holds, i.e. if $ab = ac$ and $a \neq 0$, then $b = c$ (analogously $ba = ca,\ a \neq 0 \ \Rightarrow\ b = c$).

Examples 2.2.1. The rings in 1) of 2.1.1 are domains; while $\mathbb{Z}_n$ is a domain if and only if n is prime. The rings considered in 3) and 5) in general are not domains.

Definition 2.3. If R is a ring, an element $a \in R$ is a *zero-divisor* if there exists an element $b \in R$, $b \neq 0$ such that $ab = 0$.

For example, in $\mathbb{Z}_6$ the element $[2]$ is a zero-divisor, since $2 \cdot 3 = 6 \equiv 0$ in $\mathbb{Z}_6$.

Remark 2.4. A ring is a domain if and only if the only zero-divisor is the element 0.

Definition 2.5. An element $a \in R$ is called *invertible* or a *unit* if there exists $b \in R$ such that $ab = ba = 1_R$. It is obvious that the set of units of R is a multiplicative group w.r.t. the product defined in R, called *group of units* of R.

Example 2.5.1.
(a) The group of units of $\mathbb{Z}$ is $\{1, -1\}$.
(b) The group of units of $M_{n,n}(\mathbb{R})$ is $GL_n(\mathbb{R})$.
(c) The group of units of $\mathbb{Z}_n$ is $\{[m] \,|\, m, n \text{ coprime}\}$.
Proof. First let us prove that the following properties are equivalent for any element $[m] \in \mathbb{Z}_n$:
(i) the element $[m]$ is invertible (i.e. it is a unit);
(ii) the element $[m]$ is not a zero–divisor;
(iii) m and n are coprime.

$(i) \Rightarrow (ii)$ It holds in any ring R; namely, assume that $x \in R$ is invertible and that there exists $y \in R, y \neq 0$ such that $x \cdot y = 0$. Then $x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0$, hence $y = 0$, against the assumption.
$(ii) \Rightarrow (iii)$ Assume that $[m]$ is not a zero–divisor, but m and n have a common non–trivial factor: for instance, let $m = h \cdot d$ and $n = k \cdot d$, where d is not a unit in $\mathbb{Z}$, i.e. $d \neq \pm 1$. Therefore $[k] \neq [0]$ in $\mathbb{Z}_n$, but $[m] \cdot [k] = [m \cdot k] = [h \cdot d \cdot k] = [h \cdot n] = [0]$ in $\mathbb{Z}_n$. This implies that $[m]$ is a zero–divisor and this contraddicts the assumption.
$(iii) \Rightarrow (i)$ Assume that m and n are coprime and consider the set

$$X := \{[m]^p \mid p \in \mathbb{N}\}.$$

Since $X \subseteq \mathbb{Z}_n$, then X is a finite set. Therefore there exist $p, q \in \mathbb{N}$ such that $p \neq q$ and $[m]^p = [m]^q$; for instance $p > q$. Therefore $m^p - m^q = k \cdot n$ for some $k \in \mathbb{Z}$. This means that $m^q(m^{p-q} - 1) = k \cdot n$. Since m and n are coprime, then necessarily $m^{p-q} - 1 \in (n)$, i.e. $[m]^{p-q} = [1]$ in $\mathbb{Z}_n$. Since $p - q > 0$, we can write the last equality as

$$[m]^{p-q-1} \cdot [m] = [1]$$

and this means that $[m]$ is invertible.

The equivalence $(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$ shows that the group of units of $\mathbb{Z}_n$ is as in the statement.

Definition 2.6. A ring R is a *division ring* (also a *skew field*) if every non-zero element is a unit, i.e. if $(R \setminus \{0\}, \cdot)$ is the group of units. A commutative division ring is called a *field.*

Examples 2.6.1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields; $\mathbb{Z}_n$ is a field if and only if n is prime (hence $\mathbb{Z}_n$ is a domain if and only if it is a field). More generally, a finite domain R is a field, in fact if $a \in R$, $a \neq 0$, then the set $\{a^n \mid n \in \mathbb{N}\}$ is finite, so there exist $m, n \in \mathbb{N}$, $m \neq n$, such that $a^n = a^m$, so there exists $r \in \mathbb{N}$ such that $a^r = 1$, therefore $a(a^{r-1}) = 1$.

Remark 2.7. A division ring is a domain; in fact if $ab = 0$ and $a \neq 0$, then there exists the (two-sided) inverse a^{-1} of a. So $a^{-1}ab = 0$ which gives $b = 0$. The converse, in general, is not true: $\mathbb{Z}$ is a domain, but not a field.

Definition 2.8. Let R be a ring and $a, b \in R$. We say that b is a *factor* or *divisor* of a if there exists $c \in R$ such that $a = bc$ or $a = cb$. In this case we shall write $b|a$ (b divides a) and a is called a *multiple* of b.

Remark 2.9. Units are factors of every element, since $a = u(u^{-1}a)$ for any $a \in R$, for any unit u.

Definition 2.10. Let $a, b \in R$; if $b|a$ and $a|b$, then a and b are *associates* and we shall write $a \sim b$ (in this case a and b differ by a unit factor).
If $b \,|\, a$ but $a \not| b$ (a is not a factor of b) then we say that b is a *proper factor* of a.

Definition 2.11. An element $a \in R$ is said to be *irreducible* if a is not a unit and a has no proper factors other than units (i.e. if $a = bc$ then either b or c is a unit).

Example 2.11.1. In $\mathbb{Z}$ an element is irreducible if and only if it is a prime number (different from 1 and -1). Therefore a factorization of an integer number n into prime factors is a factorization into irreducible factors. Moreover the expression

$$n = p_1 \cdots p_s$$

where the p_i's are prime numbers, is essentially unique, since two factorizations of n differ, at most, by a permutation of the prime factors and by the sign of each factor. E.g. $6 = 2 \cdot 3 = 3 \cdot 2 = (-2) \cdot (-3) = \dots$.

In general we have the following:

Definition 2.12. Let R be a ring and $a \in R$ be any element. The expression

$$a = p_1 \cdots p_s$$

is an *essentially unique factorization* of a *into irreducible elements* p_i's if for any other factorization

$$a = q_1 \cdots q_t$$

where the q_i's are irreducible elements, we have $t = s$ and $q_i \sim p_{i'}$ for a suitable permutation $i \mapsto i'$ of $\{1, 2, \ldots, s\}$.

Definition 2.13. A *ring homomorphism* is a map $f : R \longrightarrow R'$ between two rings R and R' such that

$$f(1_R) = 1_{R'} \quad \text{and} \quad \begin{cases} f(a+b) = f(a) + f(b) \\ f(ab) = f(a)f(b) \end{cases} \quad \text{for every } a, b \in R.$$

A ring homomorphism is an *epimorphism*, a *monomorphism*, an *isomorphism* if it is, respectively, surjective, injective, bijective. If $R' = R$, then f is called an *endomorphism*; if, moreover, it is also bijective, it is an *automorphism*.

Example 2.13.1. If R is a ring and $a \in R$, the map $f_a : R \longrightarrow R$ defined by $f_a(x) := ax$ is a group homomorphism (monomorphism if and only if a is a non zero-divisor), but not a ring homomorphism, unless $a = 1$ i.e. $f_1 = \mathrm{id}_R$. Note that, also if $a = 0$ then f_0 is not a ring homomorphism (otherwise $f_0(1_R) = 1_R = 0_R$).

Definition 2.14. If $f : R \longrightarrow R'$ is a ring homomorphism, its *kernel* is the set $\ker(f) := \{a \in R \mid f(a) = 0\}$. The *image* of f is the set $\mathrm{Im}(f) := \{f(a) \mid a \in R\}$.

Remark 2.15. Since a ring homomorphism is, in particular, a group homomorphism between the underlying additive group structures, $\ker(f)$ and $\mathrm{Im}(f)$ are subgroups of R and R', respectively (see Ch.I, 1.18). It is easy to see that $\mathrm{Im}(f)$ is also a subring of R', while $\ker(f)$ is not a subring of R, since $1 \notin \ker(f)$. However $\ker(f)$ has the important structure of ideal that will be introduced in 2.16.

Let us denote by $\mathrm{Aut}_{\mathcal{G}}(R)$ and by $\mathrm{Aut}_{\mathcal{R}}(R)$ the sets of (additive) group automorphisms and ring automorphisms of a ring R, respectively (these sets turn out to be groups with respect to the composition of maps). In general, as observed above, it holds $\mathrm{Aut}_{\mathcal{R}}(R) \subseteq \mathrm{Aut}_{\mathcal{G}}(R)$.

Example 2.15.1. If $R = \mathbb{Z}_n$, the strict inclusion holds. In fact, let $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ be a group automorphism; if $f[1] = [a]$ for some $a \in \mathbb{Z}$, then $f[m] = [am]$, for every m. Therefore $\mathrm{Im}(f) = \langle [a] \rangle$; hence f is an automorphism if and only if a and n are coprime, i.e. $[a]$ is a unit in the ring $\mathbb{Z}_n$. Therefore $\mathrm{Aut}_{\mathcal{G}}(\mathbb{Z}_n)$ is isomorphic to the group of units of $\mathbb{Z}_n$. On the other hand, since $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ defined by $f[m] = [am]$ is a ring homomorphism if and only if $[a] = [1]$, we have that $\mathrm{Aut}_{\mathcal{R}}(\mathbb{Z}_n)$ consists only of the identity map.

Warning. Since we are mostly interested in giving results for commutative rings, from now on, we shall assume that all the rings considered are commutative.

Note that the kernel of a ring homomorphism $f : R \longrightarrow R'$ satisfies the following property: if $x \in \ker(f)$ and $r \in R$, then xr belongs to $\ker(f)$, since $f(xr) = f(x) \cdot f(r) = 0 \cdot f(r) = 0$.
This leads to the following definition:

Definition 2.16. If R is a ring and $I \subseteq R$, then I is an *ideal* if it is a subgroup of $(R, +)$ and if the following condition

$$\text{if } a \in R \text{ and } b \in I, \quad \text{then} \quad ab \in I$$

holds.
An ideal I is *proper* if it is properly contained in R.

Obviously the kernel of a ring homomorphism is an ideal. Let us compute the ideals in some particular cases.

Examples 2.16.1.
(1) In any ring R the subset 0_R consisting of the zero element is an ideal, called *zero ideal* and denoted by (0_R). Also the wole ring R is an ideal of itself. Both are called *trivial ideals.*
(2) Let us compute all the ideals of $\mathbb{Z}$. Assume $I \subseteq \mathbb{Z}$ is an ideal. Hence, in particular, I is a subgroup of $(\mathbb{Z}, +)$. On the other hand, as seen in Ch.I, 1.3.1 and 1.30, each subgroup of $(\mathbb{Z}, +)$ is a cyclic subgroup, hence it has the form: $(n) = \{mn \mid m \in \mathbb{Z}\}$. It is immediate to verify that such set is an ideal of $\mathbb{Z}$. Therefore the ideals of $\mathbb{Z}$ are exactly the (cyclic) subgroups, all of the form (n), where $n \in \mathbb{N}$.
(3) If F is a field, then it has only two ideals, which are (0_F) and F itself. Namely, if $I \subseteq F$ is a non–zero ideal, then there exists $x \in I$, where $x \neq 0_F$. Then x is invertible and $x \cdot x^{-1} \in I$, since I is an ideal. Then $1_F \in I$ and it is immediate to see that this implies $I = F$.

Definition 2.17. If $A \subseteq R$ is any subset, then the *ideal generated by* A is the intersection of all the ideals containing A and it is denoted by (A).

Note that (A) is the smallest ideal in R which contains A. It is easy to verify that (A) is the the following set:

$$\{a_1 r_1 + \cdots + a_n r_n \mid a_i \in A,\ r_i \in R,\ n \in \mathbb{N}\}$$

in fact this set is an ideal, it contains A and if an ideal I contains A, then (A) is surely contained in I. Hence we have a representation of (A) in terms of its elements.

Definition 2.18. If $A = \{a\}$, then the ideal generated by A is denoted by (a) and it is said *principal* ideal generated by a. It is clear that $(a) = \{ar \mid r \in R\}$.
More generally, if $A = \{a_1, \ldots, a_m\}$ is a finite set of elements, then the ideal (A) is $\{\sum_{i=1}^{m} a_i r_i \mid r_i \in R\}$ and is denoted by $(a_1, \ldots, a_m)$, instead of $(\{a_1, \ldots a_m\})$. If $I = (a_1, \ldots, a_m)$, then I is said a *finitely generated ideal* and $\{a_1, \ldots, a_m\}$ is called a *system of generators* of I.

Examples 2.18.1.
(1) With the above terminology, in any ring R, the trivial ideals are principal: (0_R) and (1_R), respectively.
(2) From 2.16.1, all the ideals of $\mathbb{Z}$ are principal.

If I is an ideal, then it is a normal subgroup of $(R,+)$, since R is abelian; so we can consider the quotient group R/I, whose elements are of the kind $[a] = a+I = \{a+b \mid b \in I\}$. It is clear that $(R/I,+)$ is an abelian group since $[a]+[b] = [a+b]$ (see Ch.I, 1.11). If we define in a similar way a product by $[a]\cdot[b] := [ab]$, it is immediate to verify that this product is well defined (this is a consequence of the condition defining an ideal given in 2.16).

Definition 2.19. The ring $(R/I,+,\cdot)$ constructed above is called the *quotient ring* of R w.r.t. I. The group homomorphism $\pi : R \longrightarrow R/I$ (defined in Ch.I, 1.20), whose kernel is I itself, turns out to be a ring homomorphism (epimorphism), called again *canonical projection.*

Example 2.19.1. We already defined the group quotient $\mathbb{Z}_n = \mathbb{Z}/(n)$. Since (n) is an ideal (see 2.16.1), then this is the quotient ring of $\mathbb{Z}$ w.r.t. the ideal (n). Also in the ring $\mathbb{Z}_n$ all the ideals are principal. To show this, we use an easy result (whose proof is omitted):
If R is a ring and $I \subset R$ is an ideal, then all the ideals of R/I are exactly $\pi(J)$, where π is the canonical projection $\pi : R \longrightarrow R/I$ and J is an ideal of R such that $I \subseteq J \subseteq R$. We denote $\pi(J)$ also by J/I.
Using this fact, all the ideal of $\mathbb{Z}_n$ are of the form $(m)/(n)$, where $(n) \subset (m)$, i.e. m divides n. It is immediate to see that $(m)/(n) = ([m])$, i.e. it is the principal ideal generated by $[m]$ in $\mathbb{Z}_n$.

The following results are analogous to the results given in Ch.I. Also the proofs are quite similar to the proofs given in there.

Proposition 2.20. *If $f : R \longrightarrow R'$ is a ring homomorphism, then f is a monomorphism if and only if* $\ker(f) = (0)$. □

Theorem 2.21. *(Fundamental theorem of ring homomorphisms) Let $f : R \longrightarrow R'$ be a ring homomorphism, $I := \ker(f)$ and $\pi : R \longrightarrow R/I$ be the canonical projection. Then there exists an injective ring homomorphism $h : R/I \longrightarrow R'$ such that $f = h \circ \pi$. In particular,* $\mathrm{Im}\,(f) \cong R/I$. □

Definition 2.22. Let R be any commutative ring. By a *polynomial* with coefficients in R we mean a sequence $(a_0, a_1, \ldots, a_n, \ldots)$ of elements of R where the a_i's are all zero but a finite number of them.

Definition 2.23. Let now R' be the set of all polynomials with coefficients in R, i.e. the set of the sequences $(a_0, a_1, \ldots, a_n, \ldots)$ such that $a_i \in R$, $a_i = 0$ for almost all i. In other words, $R' = \{f : \mathbb{N} \longrightarrow R \mid f(i) = 0 \text{ for almost all } i\}$. In R' we can define a sum pointwise:

$$(a_0, a_1, \ldots, a_n, \ldots) + (b_0, b_1, \ldots, b_n, \ldots) := (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots).$$

In this way $(R',+)$ becomes an abelian group (the zero is the sequence $(0, 0, \ldots, 0, \ldots)$). Then in R' we can define a product as follows:

$$(a_0, a_1, \ldots, a_n, \ldots) \cdot (b_0, b_1, \ldots, b_n, \ldots) := (c_0, c_1, \ldots, c_n, \ldots),$$

where

$$c_i := \sum_{j=0}^{i} a_j b_{i-j} = \sum_{j+k=i} a_j b_k.$$

With this product R' becomes a commutative ring (with the unity $1 = (1, 0, 0, \ldots)$), said *ring of polynomials over R*.

Notation. Usually we express a polynomial in a simpler way, by making some identifications. Firstly, since the map $R \longrightarrow R'$ defined by $a \mapsto (a, 0, 0, \ldots)$ is a ring monomorphism, we may identify R with its image in R', so we consider R as a subring of R'. On the other hand, let $x := (0, 1, 0, \ldots)$. It holds, using the product law defined above:

$$x^k = (0, 0, \ldots, 0, 1, 0, \ldots)$$

where 1 is placed in the $(k+1)$-th position. Note that $x^0 = (1, 0, \ldots, 0) = 1_R = 1_{R'}$. Therefore we have:

$$\begin{aligned}(a_0, a_1, \ldots, a_n, 0, 0, \ldots) &= (a_0, 0, \ldots)(1, 0, \ldots) + (a_1, 0, \ldots)(0, 1, 0, \ldots) + \cdots \\ &\qquad + (a_n, 0, \ldots)(0, \ldots, 1, 0, \ldots) \\ &= a_0 + a_1 x + \cdots + a_n x^n.\end{aligned}$$

It is natural, using the analogous of the notation of polynomial expressions, to denote the ring R' by $R[x]$. The addition and multiplication that we get from the above definitions are clearly the usual addition and multiplication of polynomials.

Definition 2.24. The ring $R[x]$ is called the *ring of polynomials over R in the indeterminate (or variable) x*.

Let us recall the following

Definition 2.25. If $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ is an element of $R[x]$, then the expression $a_i x^i$ occurring in $f(x)$ is called *monomial* of degree i of $f(x)$; the element $a_i \in R$ is called *coefficient* of the monomial $a_i x^i$. The *degree* of $f(x)$, denoted by $\deg(f)$, is the greatest i such that $a_i \neq 0$ (i.e. if $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ and $a_n \neq 0$, then $\deg(f) = n$).

Remark 2.26. A polynomial has degree 0 if and only if it belongs to $R \setminus \{0\}$. We set $\deg(0) = -\infty$. Two polynomials are equal if and only if they have the same degree and have coefficients respectively equal, i.e. $a_0 + a_1 x + \cdots + a_n x^n = b_0 + b_1 x + \cdots + b_m x^m$ if and only if $n = m$ and $a_i = b_i$ for all $i = 1, \ldots, n$.

It is immediate to verify:

Proposition 2.27. *If R is an integral domain, $f, g \in R[x]$, then:*

$$\deg(f + g) \leq \max\{\deg(f), \deg(g)\}, \qquad \deg(fg) = \deg(f) + \deg(g). \qquad \square$$

Proposition 2.28. *If R is an integral domain, then $R[x]$ is an integral domain.*

Proof. If $f, g \in R[x]$, $f \neq 0 \neq g$, say $f = a_n x^n + \cdots + a_0$ and $g = b_m x^m + \cdots + b_0$, then $fg = a_n b_m x^{n+m} + \cdots + a_0 b_0$, but $a_n \neq 0 \neq b_m$, so $a_n b_m \neq 0$ since R is a domain. $\square$

Let us now give some interesting results regarding polynomial rings over a field.

Proposition 2.29. *Let $f, g \in K[x]$, where K is a field, and suppose $f \neq 0$. Then there exist unique polynomials $q, r \in K[x]$ such that:*

$$g = fq + r$$

where $\deg(r) < \deg(f)$. □

Definition 2.30. Using the above notations, q is called the *quotient* and r the *remainder* (on dividing g by f).

We are going to mention two kind of consequences of the previous result: on one hand about the divisibility (and zeros) of a polynomial; on the other hand about the ideals in $K[x]$.
Recall that if $f, g \in K[x]$, then f *divides* g ($f|g$) if there exists a polynomial $h \in K[x]$ such that $g = fh$.

Proposition 2.31. *Let $f(x)$ be a non-zero polynomial in $K[x]$. Then $f(x)$ has a zero $a \in K$ (i.e. $f(a) = 0$) if and only if $x - a$ divides $f(x)$.*

Proof. From 2.29 we have that there exist $q, r \in K[x]$ such that $f = q(x - a) + r$ with $\deg(r) < \deg(x - a) = 1$, hence r is a constant. Since $f(a) = 0$, from $f = q(x - a) + r$ we get: $f(a) = 0 = r$, so $x - a$ divides f. The converse is trivial. □

As an easy consequence of this result we get:

Corollary 2.32. *If $f \in K[x]$ is a polynomial of degree n, then it has at most n zeros in K.* □

Theorem 2.33. *If K is a field, then the ring $K[x]$ is a domain with principal ideals.*

Proof. Note first that $K[x]$ is a domain by 2.28. Let now $I \subseteq K[x]$ be an ideal and assume $I \neq (0)$. Let $f \in I$ be a non-zero polynomial of minimum degree. If $g \in I$, then we can divide g by f and, according to 2.29, we get: $g = qf + r$, with $\deg(r) < \deg(f)$. From $r = g - qf$, we see that $r \in I$, and therefore $r = 0$, since its degree is less than the degree of f. This shows that $I = (f)$. □

Let us finally remark that, if R is a domain, then the units of $R[x]$ are precisely the elements of R which are units. In particular, if K is any field, the units of $K[x]$ are the non-zero elements of K.
From this observation, accordingly to 2.11, we get that in $K[x]$ a polynomial $f(x)$ is reducible (over K) if and only if it is the product of two polynomials of $K[x]$ of smaller degree. Any polynomial of degree one in $K[x]$ is clearly irreducible. The converse is not true, in general. For instance, $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible; in fact if $x^2 - 2 = (ax + b)(cx + d)$, then $ac = 1,\ ad + bc = 0,\ bd = -2$, and there are no solutions (in $\mathbb{Q}$) to these equations.
Anyway $x^2 - 2$ may be reducible in a suitable polynomial ring. In fact $x^2 - 2 \in \mathbb{Q}[x] \subset \mathbb{R}[x]$ and in $\mathbb{R}[x]$ the equality $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ holds.

Capitolo 3
Complementi di teoria degli anelli

Definizione 3.1. Sia A un dominio. La relazione $\mathcal{R}$ su $A \times A^*$ definita da

$$(a,b)\mathcal{R}(c,d) \Leftrightarrow ad = bc$$

risulta essere una relazione d'equivalenza. L'insieme quoziente $A \times A^*/\mathcal{R}$ si denota con $Q(A)$ e i suoi elementi con

$$[(a,b)] := \frac{a}{b}.$$

Proposizione 3.2. *Le operazioni in $Q(A)$ definite da:*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad e \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

sono ben definite. Inoltre, con tali operazioni, $Q(A)$ risulta un corpo; in particolare:

$$1_{Q(A)} = \frac{1_A}{1_A} \quad e \quad 0_{Q(A)} = \frac{0_A}{1_A}.$$

Infine, se A è commutativo, allora $Q(A)$ è un campo.

Dimostrazione. Immediata.

Definizione 3.3. Diciamo che $Q(A)$ è il *corpo* (risp. *campo*) *dei quozienti* di A.

Esempio 3.3.1. Se A è a sua volta un campo, ovviamente $Q(A) = A$.

Esempio 3.3.2. Sia $A = \mathbb{Z}$; allora $Q(A) = \mathbb{Q}$ è il campo dei numeri razionali.

Definizione 3.4. Se K è un campo e $A = K[x]$, il suo campo dei quozienti $Q(K[x])$ si denota con $K(x)$ e si dice *campo delle funzioni razionali* su K.

Definizione 3.5. Sia A un anello. Utilizzando le notazioni introdotte dopo 2.1.1, se

$$n \cdot 1_A \neq 0_A \quad \text{per ogni} \quad n \in \mathbb{N}$$

si dice che A ha *caratteristica zero*. Altrimenti, il minimo $p \in \mathbb{N}^*$ tale che $p \cdot 1_A = 0_A$ si dice *caratteristica* di A. Scriveremo $ch(A) = p$.

Esempio 3.5.1. Si prova facilmente che:
- $ch(\mathbb{Z}) = 0$; $ch(\mathbb{Q}) = 0$; $ch(\mathbb{R}) = 0$; $ch(\mathbb{C}) = 0$;
- per ogni $n \in \mathbb{N}$ vale $ch(\mathbb{Z}_n) = n$;
- se A è un qualunque anello, allora $ch(M_{n,n}(A)) = ch(A)$ e $ch(A[x]) = ch(A)$.

Osservazione 3.6. Se A ha caratteristica p positiva, allora $p \geq 2$.

Osservazione 3.7. Sia A un anello; l'applicazione

$$\begin{array}{rccc} \tau: & \mathbb{Z} & \longrightarrow & A \\ & n & \mapsto & n \cdot 1_A \end{array}$$

è un omomorfismo di anelli. Per il I teorema di omomorfismo di anelli

$$\mathbb{Z}/\ker(\tau) \cong \text{Im } (\tau) \subseteq A.$$

Definizione 3.8. Im (τ) si dice *sottoanello fondamentale* di A e si denota con $E(A)$.

Teorema 3.9. *Se A è un anello allora:*

$$E(A) \cong \begin{cases} \mathbb{Z}, \text{ se } ch(A) = 0 \\ \mathbb{Z}_p, \text{ se } ch(A) = p \end{cases}.$$

Dimostrazione. E' sufficiente provare che $\ker(\tau) = \{0\}$ se $ch(A) = 0$ e che $\ker(\tau) = (p)$ se $ch(A) = p$. Ma questo è ovvio dalla definizione di caratteristica.

Esempio 3.9.1. Si prova immediatamente che $E(\mathbb{Z}) = \mathbb{Z}$, $E(\mathbb{Z}_n) = \mathbb{Z}_n$ per ogni n.
E' facile vedere che $E(\mathbb{Z}[x]) = \mathbb{Z}$ e $E(\mathbb{Z}_n[x]) = \mathbb{Z}_n$.

Corollario 3.10. *Se A è un anello integro di caratteristica non nulla, allora $ch(A)$ è un numero primo; in particolare $E(A)$ è un corpo finito di ordine primo.*

Dimostrazione. Supponiamo che $ch(A) = nm$, con $n, m \in \mathbb{N}$ e n, m entrambi minori di nm. Dunque

$$0_A = (nm) \cdot 1_A = (nm) \cdot (1_A \cdot 1_A) = (n \cdot 1_A)(m \cdot 1_A)$$

dove l'ultima uguaglianza segue dalle proprietà enunciate dopo 2.1.1. Poiché A è integro, deve essere $n \cdot 1_A = 0$ oppure $m \cdot 1_A = 0$, ma ciò contraddice l'ipotesi $ch(A) = nm$.

Proposizione 3.11. *Sia A un anello integro e $ch(A) = p$. Allora, per ogni $n \in \mathbb{N}^*$ e per ogni $a, b \in A$ si ha:*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Dimostrazione. Si osservi che

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}.$$

Dunque $\binom{p}{i}$ è un intero per ogni $i = 1, \ldots, p-1$. Ma

$$\binom{p}{i} = \frac{p(p-1)(p-2)\cdots(p-i+1)}{i!}$$

e p è primo; pertanto anche

$$\frac{(p-1)(p-2)\cdots(p-i+1)}{i!} \in \mathbb{N}.$$

Questo implica che ogni $\binom{p}{i}$ è multiplo di p e quindi $\binom{p}{i}a^i b^{p-i} = 0$ in quanto $ch(A) = p$. In questo modo si prova che

$$(a+b)^p = a^p + b^p.$$

Elevando ambo i membri alla potenza p–esima per n volte, si ha la tesi.

Definizione 3.12. Sia K un campo; il sottoanello fondamentale $E(K)$ (detto anche *anello degli interi di* K) è integro, dunque esiste il suo campo dei quozienti $\overline{E}(K) := Q(E(K))$, detto *sottocampo fondamentale* di K.

Proposizione 3.13. *Sia K un campo. Allora il suo sottocampo fondamentale è:*

$$\overline{E}(K) \cong \begin{cases} \mathbb{Q}, \text{ se } ch(K) = 0 \\ \mathbb{Z}_p, \text{ se } ch(K) = p \end{cases}.$$

Dimostrazione. Immediata da 3.9.

Capitolo 4
Estensioni di campi

Ricordiamo che un polinomio $p(x) \in K[x]$, dove K è un campo, ha per radice $a \in K$ se e solo se $p(x) = (x-a)q(x)$, dove $q(x) \in K[x]$ è un opportuno polinomio (vedi 2.31, Cap.2). Pertanto i polinomi irriducibili in $K[x]$ non hanno radici in K.

Definizione 4.1. Siano $K \subset K'$ due campi. Se K è un sottocampo di K' diremo che K' è una *estensione* di K. In tal caso, poiché K' risulta essere un K–spazio vettoriale, la dimensione di K' su K si dice *grado* di K' su K e si denota con $(K' : K)$.
Se $(K' : K) \in \mathbb{N}$, diremo che l'estensione $K \subset K'$ è *finita*. Altrimenti diremo che è una *estensione infinita*.

Esempio 4.1.1. E' facile vedere che $(\mathbb{C} : \mathbb{R}) = 2$; si può provare che $(\mathbb{R} : \mathbb{Q}) = \infty$.

Definizione 4.2. Sia $K \subset K'$ un'estensione di campi e $a \in K'$. Se esiste un polinomio non nullo $f(x) \in K[x]$ tale che $f(a) = 0$, diciamo che a è *algebrico* su K. Altrimenti si dice *trascendente* su K.
Se ogni elemento di K' è algebrico su K, diremo che l'estensione $K \subset K'$ è *algebrica*. Altrimenti diremo che è *trascendente*.

Esempi 4.2.1.
(i) Ogni elemento $a \in K$ è algebrico su K, in quanto radice del polinomio $x - a \in K[x]$.
(ii) Il numero reale $\sqrt{2}$ è algebrico su $\mathbb{Q}$, in quanto radice di $x^2 - 2 \in \mathbb{Q}[x]$.
(iii) Ovviamente $\sqrt{2} \in \mathbb{R}$ è algebrico su $\mathbb{R}$ per (i): infatti è radice di $x - \sqrt{2} \in \mathbb{R}[x]$.
(iv) E' noto che $\pi \in \mathbb{R}$ è trascendente su $\mathbb{Q}$.

Osservazione - Definizione 4.3. Si dimostra che tutti gli elementi algebrici su K costituiscono un campo (detto *chiusura algebrica* di K e denotato con $\overline{K}$). Quindi se K' è un'estensione algebrica di K, allora $K' \subseteq \overline{K}$.
Se $K = \overline{K}$, si dice che K è un campo *algebricamente chiuso*.

Esempio 4.3.1. Il Teorema fondamentale dell'algebra ("ogni polinomio a coefficienti complessi ha almeno una radice complessa") implica che ogni polinomio a coefficienti reali ha tutte le radici in $\mathbb{C}$. Dunque $\overline{\mathbb{R}} \subseteq \mathbb{C}$. In realtà si ha che $\overline{\mathbb{R}} = \mathbb{C}$.
Si dimostra inoltre che $\overline{\mathbb{C}} = \mathbb{C}$, cioè $\mathbb{C}$ è un campo algebricamente chiuso.

Definizione 4.4. Se $K \subset K'$ è un'estensione di campi e $a \in K'$, denotiamo con $K[a]$ il più piccolo sottoanello di K' contenente K ed a e con $K(a)$ il più piccolo sottocampo di K' contenente K ed a. Quest'ultimo è detto *estensione semplice* di K mediante a.

E' facile provare il seguente risultato:

Proposizione 4.5. *Sia $K \subset K'$ un'estensione di campi e $a \in K'$. Allora:*
i) $K[a] = \{f(a) \mid f(x) \in K[x]\}$;
ii) $K(a) = \{f(a)/g(a) \mid f(x), g(x) \in K[x], g(a) \neq 0\} = Q(K[a])$. □

Osservazione 4.6. Sia K' una estensione del campo K e sia $a \in K'$ un elemento algebrico su K. Consideriamo l'omomorfismo di valutazione in a:

$$\begin{aligned} \varphi_a : K[x] &\longrightarrow K' \\ f(a) &\mapsto f(a) \end{aligned}$$

e chiaramente si ha Im $(\varphi_a) = K[a]$. Per il Teorema fondamentale di omomorfismo per anelli segue che

$$K[x]/\ker(\varphi_a) \cong \text{Im } (\varphi_a) = K[a].$$

Ricordando che $K[x]$ è un anello ad ideali principali, sappiamo che esiste un polinomio $P(x) \in K[x]$ tale che $\ker(\varphi_a) = (P(x))$. Il generatore $P(x)$ è definito a meno di una costante non nulla, quindi esiste un solo generatore monico: lo denotiamo con $p_a(x)$.

Si può provare il seguente fatto:

Proposizione-Definizione 4.7. *Sia $K \subset K'$ un'estensione di campi e $a \in K'$ un elemento algebrico su K. Sia $p(x) \in K[x]$ un polinomio monico. Allora sono equivalenti i seguenti fatti:*

- *$p(x)$ è $p_a(x)$;*
- *$p(x)$ è un polinomio irriducibile avente a come radice;*
- *$p(x)$ ha grado minimo tra i polinomi non nulli di $K[x]$ aventi a come radice.*

Se vale uno dei fatti precedenti, diciamo che $p(x)$ è il polinomio minimo di a su K. □

Esempio 4.7.1. In riferimento a 4.2.1: i polinomi citati in $(i), (ii), (iii)$ sono i polinomi minimi dei corrispondenti elementi. In particolare, in (ii), $x^2 - 2$ è il polinomio minimo di $\sqrt{2}$ su $\mathbb{Q}$. Se così non fosse, il polinomio minimo avrebbe grado 1, ma ciò è impossibile.

Proposizione 4.8. *Sia $K \subset K'$ un'estensione di campi e $a \in K'$. Allora:*

$$a \text{ è algebrico su } K \quad \Leftrightarrow \quad K[a] = K(a).$$

In tal caso, posto n il grado del polinomio minimo di a su K, ogni elemento $b \in K(a)$ ha la forma

$$b = b_0 + b_1 a + b_2 a^2 + \cdots + b_{n-1} a^{n-1}$$

per opportuni $b_i \in K$. In particolare $(K(a) : K) = n$.

Dimostrazione. (sull'esempio 4.2.1, (ii)). Mostriamo che:

i) $\mathbb{Q}[\sqrt{2}] = \{b_0 + b_1\sqrt{2} \mid b_i \in \mathbb{Q}\}$;
ii) $\mathbb{Q}[\sqrt{2}]$ è un campo, e quindi $\mathbb{Q}[\sqrt{2}] = Q(\mathbb{Q}[\sqrt{2}]) = \mathbb{Q}(\sqrt{2})$;
iii) $(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = 2 =$ grado del polinomio minimo di $\sqrt{2}$.

i) Per 4.5 (i), si ha $\mathbb{Q}[\sqrt{2}] = \{f(\sqrt{2}) \mid f(x) \in \mathbb{Q}[x]\}$; ovviamente se

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

allora

$$f(\sqrt{2}) = (a_0 + 2a_2 + \cdots + 2^k a_{2k} + \cdots) + \sqrt{2}(a_1 + 2a_3 + \cdots) = b_0 + b_1\sqrt{2}$$

per opportuni $b_0, b_1 \in \mathbb{Q}$.
ii) Se $z = b_0 + b_1\sqrt{2}$ è un elemento non nullo di $\mathbb{Q}[\sqrt{2}]$, si determina facilmente il suo inverso $z^{-1} := c_0 + c_1\sqrt{2}$. Infatti: se $b_1 = 0$, poiché $b_0 \neq 0$, esiste $b_0^{-1} \in \mathbb{Q}$, dunque $z^{-1} = b_0^{-1}$.
Sia dunque $b_1 \neq 0$. Occorre risolvere l'equazione

$$(b_0 + b_1\sqrt{2})(c_0 + c_1\sqrt{2}) = 1$$

nelle incognite $c_0, c_1 \in \mathbb{Q}$. Si ottiene immediatamente:

$$(b_0c_0 + 2b_1c_1) + (b_0c_1 + b_1c_0)\sqrt{2} = 1 \quad \Longrightarrow \quad \begin{cases} b_0c_1 + b_1c_0 = 0 \\ b_0c_0 + 2b_1c_1 = 1 \end{cases}.$$

Poiché $b_1 \neq 0$, si ottiene:

$$\begin{cases} c_0 = -\frac{b_0}{b_1} \cdot c_1 \\ -b_0 \cdot \frac{b_0}{b_1} \cdot c_1 + 2b_1c_1 = 1 \end{cases}.$$

Dalla seconda equazione:

$$c_1 = \frac{b_1}{2b_1^2 - b_0^2}$$

e il denominatore è non nullo, altrimenti $2b_1^2 - b_0^2 = 0$. Ma tale equazione non ha soluzioni $b_0, b_1 \in \mathbb{Q}$.
iii) Per (*i*) è chiaro che $\mathbb{Q}[\sqrt{2}]$ è un $\mathbb{Q}$-spazio vettoriale di dimensione 2, avendo come base $(1, \sqrt{2})$. Dunque con (*ii*) si conclude. □

Capitolo 5
Campi finiti

Definizione 5.1. Un campo finito K (cioè composto da un numero finito di elementi) si dice *campo di Galois*. Il numero dei suoi elementi si dice *ordine* e si denota con $|K|$. Un campo di Galois di ordine q si denota anche con $GF(q)$.

Proposizione 5.2. *Sia $K \subset K'$ un'estensione di campi con $(K' : K) = n$. Supponiamo che K sia finito di ordine p. Allora $|K'| = p^n$.*

Dimostrazione. Per definizione $\dim_K(K') = n$, quindi esiste un isomorfismo di K–spazi vettoriali: $K' \cong K^n$. Pertanto $|K'| = |K^n| = p^n$. □

Corollario 5.3. *Sia $GF(q)$ un campo finito di ordine q e caratteristica p. Allora $q = p^n$ per un opportuno $n \in \mathbb{N}$.*

Dimostrazione. Per 3.13, il sottocampo fondamentale di $GF(q)$ è isomorfo a $\mathbb{Z}_p$. Dunque $\mathbb{Z}_p \subseteq GF(q)$ è un'estensione di campi. Ponendo $n = (GF(q) : \mathbb{Z}_p)$, si conclude con 5.2. □

Esempio 5.3.1. Consideriamo un polinomio $f(x) \in \mathbb{Z}_p[x]$, irriducibile su $\mathbb{Z}_p$ di grado $h > 1$. Sia a una radice di $f(x)$. Dunque h è il grado del polinomio minimo di a su $\mathbb{Z}_p$ (tale polinomio è infatti uguale a f solo se f è monico). Pertanto per 4.8 si ha

$$\mathbb{Z}_p(a) = \mathbb{Z}_p[a] = \{b_0 + b_1 a + b_2 a^2 + \cdots + b_{h-1} a^{h-1} \mid b_i \in \mathbb{Z}_p\}.$$

e quindi $(\mathbb{Z}_p(a) : \mathbb{Z}_p) = h$. Dunque, per 5.2, $\mathbb{Z}_p(a)$ è un campo di Galois di ordine $q = p^h$.

Esempio 5.3.2. Vediamo un caso numerico dell'esempio 5.3.1.
Si consideri $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Si vede facilmente che $f(x)$ è irriducibile su $\mathbb{Z}_2$, in quanto nessun elemento di $\mathbb{Z}_2$ è radice di $f(x)$.
Indicata con a una sua radice, $\mathbb{Z}_2(a)$ è un campo di Galois di ordine $2^2 = 4$ e precisamente:

$$GF(4) = \mathbb{Z}_2(a) = \{b_0 + b_1 a \mid b_i \in \mathbb{Z}_2\} = \{0, 1, a, 1 + a\}.$$

E' un facile esercizio scrivere le tabelle della somma e del prodotto nel campo $GF(4)$. Per quest'ultima occorre tenere conto della relazione $a^2 = a + 1$, che si ricava dal fatto che a è radice di $f(x)$ e che i coefficienti di tale polinomio sono elementi di $\mathbb{Z}_2$.

Esempio 5.3.3. Vediamo un altro caso numerico dell'esempio 5.3.1.
Si consideri $f(x) = x^2 - x - 1 \in \mathbb{Z}_3[x]$. Si vede facilmente che $f(x)$ è irriducibile su $\mathbb{Z}_3$. Indicata con a una sua radice, $\mathbb{Z}_3(a)$ è un campo di Galois di ordine $3^2 = 9$. Dunque

$$GF(9) = \mathbb{Z}_3(a) = \{b_0 + b_1 a \mid b_i \in \mathbb{Z}_3\} = \{0, 1, 2, a, 1 + a, 2 + a, 2a, 1 + 2a, 2 + 2a\}.$$

Anche per tale campo finito si possono scrivere facilmente le tabelle delle operazioni.

Studiamo ora l'algebra moltiplicativa dei campi $GF(q)$.

Osservazione 5.4. Sia K un campo finito e $\alpha \in K$ un elemento non nullo. Allora le potenze di α: $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{-1}, \alpha^{-2}, \alpha^{-3}, \ldots$ non possono essere tutte distinte. In particolare, se $\alpha^n = \alpha^m$ per qualche $n \neq m$, allora $\alpha^{n-m} = 1$.

Tale fatto induce in modo naturale a dare la seguente:

Definizione 5.5. Sia K un campo finito e $\alpha \in K$ un elemento non nullo. Il minimo intero positivo n tale che $\alpha^n = 1$ si dice *ordine* di α e si indica con $ord(\alpha)$. L'ordine di 0_K non è definito.

Si ricordi che in 1.23, Cap. 1, abbiamo definito l'ordine di un elemento g di un gruppo moltiplicativo $(G, \cdot)$ come:

$$|g| := \#\{g^p \mid p \in \mathbb{Z}\}.$$

Si osservi che, se K è un campo finito, allora $(K^*, \cdot)$ è un gruppo moltiplicativo finito.
Per mostrare che le due nozioni di ordine coincidono, utilizziamo la seguente semplice proprietà:

Lemma 5.6. *Sia K un campo, $\alpha \in K^*$ e $n = ord(\alpha)$. Allora: per ogni $p, q \in \mathbb{N}$ con $p, q < n$ e $p \neq q$, si ha : $\alpha^p \neq \alpha^q$. In particolare le potenze $\alpha^0 = 1_K, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ sono elementi distinti di K.* □

Proposizione 5.7. *Sia K un campo e $\alpha \in K^*$. Allora*

$$|\alpha| = ord(\alpha).$$

Dimostrazione. Per 5.6, è chiaro che $ord(\alpha) = \#\{\alpha^0, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, dove $n = ord(\alpha)$. Dunque è sufficiente provare che

$$\{\alpha^0, \alpha, \alpha^2, \ldots, \alpha^{n-1}\} = \{\alpha^p \mid p \in \mathbb{Z}\}$$

e questo è un facile esercizio. □

La seguente proprietà caratterizza l'ordine di un elemento a: tale numero non è solo la minima potenza alla quale elevare a per ottenere 1; è anche l'unico sottomultiplo di ogni esponente al quale si può elevare a per ottenere 1.

Proposizione 5.8. *Siano K un campo finito, $\alpha \in K$ e $n \in \mathbb{N}$ un intero tale che $\alpha^n = 1$. Sono equivalenti i seguenti fatti:*
(i) per ogni $s \in \mathbb{N}$ vale:

$$\alpha^s = 1 \quad \Leftrightarrow \quad s \text{ è un multiplo di } n \text{ , cioè } n|s;$$

(ii) $n = ord(\alpha)$.

Dimostrazione. $(i) \Rightarrow (ii)$. Sia $S := \{s \in \mathbb{N}^* \mid \alpha^s = 1\}$ e sia $s_0 = \min S = ord(\alpha)$. Per ipotesi ogni elemento di S è multiplo di n; in particolare anche s_0 lo è e quindi $n \leq s_0$.

D'altra parte, $n \in S$ per l'ipotesi $\alpha^n = 1$, dunque $n \geq s_0$. Pertanto $n = s_0 = ord(\alpha)$.
$(ii) \Rightarrow (i)$. Dobbiamo provare l'equivalenza "$\Leftrightarrow$". "$\Leftarrow$" è ovvia.
"$\Rightarrow$" Ovviamente deve essere $s \geq n$; dividendo s per n si ha: $s = nq + r$ dove r è il resto della divisione e quindi $0 \leq r < n$. Pertanto

$$1 = \alpha^s = \alpha^{nq+r} = \alpha^{nq} \cdot \alpha^r = (\alpha^n)^q \cdot \alpha^r = \alpha^r$$

quindi, per definizione di ordine, deve essere $r = 0$. □

Proposizione 5.9. *Sia K un campo finito, $\alpha \in K$, $n = ord(\alpha)$. Allora per ogni $k \in \mathbb{N}$:*

$$ord(\alpha^k) = n/MCD(n, k).$$

Dimostrazione. Sia $d := MCD(n, k)$. Ovviamente $(\alpha^k)^{n/d} = (\alpha^n)^{k/d} = 1$; per 5.8 basta provare che

$$(\alpha^k)^s = 1 \quad \Rightarrow \quad s \text{ è multiplo di } n/d.$$

Per 5.8, se $(\alpha^k)^s = \alpha^{ks} = 1$ allora $n \,|\, (ks)$. Ciò implica che

$$\frac{n}{d} \quad \text{divide} \quad \frac{k}{d} \cdot s.$$

Ma n/d e k/d sono ovviamente coprimi; dunque, necessariamente, n/d divide s, come richiesto. □

Proposizione 5.10. *Sia K un campo finito, $\alpha, \beta \in K$ con $n := ord(\alpha)$ e $m := ord(\beta)$. Se n e m sono coprimi allora*

$$ord(\alpha\beta) = nm.$$

Dimostrazione. Chiaramente $(\alpha\beta)^{nm} = \alpha^{nm}\beta^{nm} = 1$. Per 5.8 basta provare che, se $(\alpha\beta)^s = 1$, allora s è multiplo di nm. Osserviamo che:

$$(\alpha\beta)^s = 1 \;\Rightarrow\; \begin{cases} \alpha^s = \beta^{-s} \;\Rightarrow\; \alpha^{ms} = \beta^{-ms} = 1 \;\Rightarrow\; n \,|\, (ms) \;\Rightarrow\; n \,|\, s \\ \beta^s = \alpha^{-s} \;\Rightarrow\; \beta^{ns} = \alpha^{-ns} = 1 \;\Rightarrow\; m \,|\, (ns) \;\Rightarrow\; m \,|\, s \end{cases}$$

dove le penultime implicazioni seguono da 5.8 e le ultime dal fatto che n e m sono coprimi. Pertanto s è multiplo di n e di m, dunque di nm, ancora per il fatto che sono coprimi. □

In analogia con la nozione di radici n–esime dell'unità nell'ambito dei numeri complessi (cfr. 1.24.1), si introduce la seguente:

Definizione 5.11. Sia K un campo finito e $\alpha \in K$. Diciamo che α è una *radice n–esima dell'unità* se $\alpha^n = 1$. In particolare, se $n = ord(\alpha)$, diremo che α è una radice n–esima *primitiva* dell'unità.
Se $K = GF(q)$ e $ord(\alpha) = q - 1$, diremo che α è un *elemento primitivo* del campo.

Teorema. 5.12. *(Teorema dell'elemento primitivo)*
In un campo finito K esiste un elemento primitivo e le sue potenze distinte coincidono con tutti gli elementi non nulli del campo. Equivalentemente, K^* è un gruppo ciclico.

Dimostrazione. Supponiamo che $|K| = q$, cioè che il campo sia $K = GF(q)$.
Se $q = 2$, il teorema è vero (l'elemento primitivo è 1_K).
Sia $q > 2$ e sia n il massimo ordine degli elementi del campo (dunque $n \leq q-1$). Sia $\alpha \in K$ tale che $ord(\alpha) = n$ e sia $\beta \in K^*$ un qualunque elemento distinto da α. Poniamo $m := ord(\beta)$.

(A) Vogliamo provare che $m \mid n$.
Altrimenti, supponiamo che m non divida n; dunque, posto $d := MCD(n, m)$, si ha che $d < m$. Per 5.9 si ha $ord(\beta^n) = m/d > 1$.
Chiaramente m/d è primo con n, dunque per 5.10, otteniamo

$$ord(\alpha \cdot \beta^n) = n \cdot m/d > n$$

in quanto $m/d > 1$. Ma ciò contraddice il fatto che n è il massimo ordine degli elementi di K. Pertanto è provato che $m \mid n$.

(B) Vogliamo provare che $n = q - 1$.
Applicando (A) si ha che $\beta^n = 1$, per ogni $\beta \in K^*$. Quindi tutti i $q-1$ elementi di K^* sono radici dell'equazione $x^n = 1$; poiché tale equazione ha al più n radici distinte, ne segue che $q - 1 \leq n$. Pertanto $n = q - 1$ e α è un elemento primitivo di K.

(C) L'ultima parte dell'enunciato è immediata: poiché α è elemento primitivo di ordine $q-1$, ciò significa che $\alpha, \alpha^2, \ldots, \alpha^{q-1} = 1$ sono elementi distinti e non nulli di K per 5.6. Essendo proprio in numero di $q - 1$, è chiaro che $K^* = \{\alpha, \alpha^2, \ldots, \alpha^{q-1}\} = \langle\alpha\rangle$.
□

Esempio 5.12.1. Si consideri $GF(5) = \mathbb{Z}_5$ (per semplicità denotiamo con a un elemento $[a]$ di $\mathbb{Z}_5$). Consideriamo le potenze dei suoi elementi non nulli e diversi da 1, cioè di: $2, 3, 4$. I sottogruppi (tutti ciclici) del gruppo moltiplicativo $\mathbb{Z}_5^*$ sono dati da:

$$< 2 >= \{2, 4, 3, 1\}, \quad < 3 >= \{3, 4, 2, 1\}, \quad < 4 >= \{4, 1\}.$$

Pertanto 2 e 3 hanno ordine 4 e quindi sono elementi primitivi di $\mathbb{Z}_5$, mentre 4 non lo è, pur essendo anch'esso radice dell'equazione $x^4 = 1$.

Corollario 5.13. *Gli elementi di $GF(q)$ sono tutte e sole le soluzioni dell'equazione*

$$x^q - x = 0.$$

Dimostrazione. Basta osservare che $x^q - x = x(x^{q-1} - 1)$, dunque le soluzioni dell'equazione devono soddisfare $x = 0$ (che ha per unica soluzione lo zero di $GF(q)$) oppure $x^{q-1} - 1 = 0$, che è soddisfatta da tutti gli elementi non nulli del campo, per 5.12. □

Il precedente risultato implica che una qualunque fattorizzazione del polinomio $x^q - x$ ripartisce gli elementi di $GF(q)$. Ad esempio, la fattorizzazione $x^q - x = x(x^{q-1} - 1)$ separa

gli elementi non nulli dallo 0. In generale, $x^q - x = f(x)g(x)$ separerà le radici di $f(x)$ da quelle di $g(x)$.

Lo scopo della seguente costruzione è di ripartire gli elementi di $GF(q)$ a seconda del loro ordine.

Teorema 5.14. *Supponiamo che $GF(q)$ contenga un elemento α che sia radice n–esima primitiva dell'unità. Allora il polinomio $x^n - 1$ si fattorizza in $GF(q)$ in tal modo:*

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i) = \prod_{i=1}^{n} (x - \alpha^i).$$

Dimostrazione. Poiché $\alpha^n = 1$, si ha $(\alpha^i)^n = 1$ per ogni $i = 0, \ldots, n-1$. Dunque le potenze $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ sono radici di $x^n - 1$. Inoltre sono tutte distinte per 5.6, in quanto α è primitiva di ordine n. Si ha quindi la tesi. □

Esempio 5.14.1. In 5.12.1 abbiamo esaminato gli elementi primitivi di $GF(5) = \mathbb{Z}_5$. In particolare, poiché $ord(2) = 4$, l'elemento $2 \in \mathbb{Z}_5$ è radice (primitiva) di $x^4 - 1$. D'altra parte, poiché $ord(4) = 2$, l'elemento $4 \in \mathbb{Z}_5$ è radice (primitiva) di $x^2 - 1$.
Pertanto i due polinomi suddetti sono riducibili in $\mathbb{Z}_5[x]$.
Il primo, ad esempio, si fattorizza come in 5.14, usando le potenze dell'elemento primitivo $\alpha = 2$:

$$x^4 - 1 = \prod_{i=1}^{4} (x - 2^i) = (x - 2) \cdot (x - 4) \cdot (x - 3) \cdot (x - 1).$$

Anche il secondo si fattorizza come in 5.14, usando le potenze dell'elemento primitivo $\alpha = 4$:

$$x^2 - 1 = \prod_{i=1}^{2} (x - 4^i) = (x - 4) \cdot (x - 1).$$

Osservazione 5.15. Se valgono le ipotesi di 5.14, si ha che $n \leq q-1$. Infatti, se $\alpha \in GF(q)$ è radice *primitiva* n–esima dell'unità, allora $\alpha, \alpha^2, \ldots, \alpha^n = 1$ sono n elementi distinti e non nulli di $GF(q)$. Quindi si ha quanto affermato.
Il seguente esempio illustra un caso in cui $n > q$: in tale situazione $x^n - 1$ non può fattorizzarsi totalmente (come in 5.14) in $GF(q)$. Occorrerà introdurre un'opportuna estensione.

Esempio 5.15.1. Non si può fattorizzare $x^3 - 1$ in $\mathbb{Z}_2[x]$ come nel teorema:

$$x^3 - 1 = (x - 1)(x^2 + x + 1)$$

e il secondo fattore è irriducibile in $\mathbb{Z}_2[x]$, come mostrato in 5.3.2.
In effetti, $\mathbb{Z}_2$ non contiene "abbastanza" elementi per contenere una radice terza primitiva dell'unità. Occorre individuare un'opportuna estensione (semplice) di $\mathbb{Z}_2$. In questo esempio, è sufficiente quella individuata in 5.3.2, cioè $GF(4) = \mathbb{Z}_2(a)$, dove a è una radice di $x^2 + x + 1$.

E' facile vedere che i due elementi non banali di $GF(4)$, cioè a e $1+a$, hanno entrambi ordine 3. In particolare sono radici terze primitive dell'unità. Ora si può applicare 5.14 in $GF(4)$, con l'elemento primitivo a. Tenendo presente che $a^2 = a+1$ e $a^3 = 1$, si ottiene:

$$x^3 - 1 = \prod_{i=1}^{3} (x - a^i) = (x-a)\cdot(x-a-1)\cdot(x-1).$$

Osservazione 5.16. Sia $\alpha \in GF(q)$ un elemento di ordine n. Se $d \,|\, n$, cioè se $n = dk$, allora

$$(\alpha^k)^d = \alpha^n = 1,\ (\alpha^{2k})^d = \alpha^{2n} = 1,\ \ldots, (\alpha^{dk})^d = \alpha^{dn} = 1$$

quindi $\alpha^k, \alpha^{2k}, \ldots, \alpha^{dk}$ sono le d radici dell'equazione $x^d = 1$.
E' quindi provato che, se $d \,|\, n = ord(\alpha)$ allora

$$\{\text{radici } d\text{–esime dell'unità}\} \subseteq \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}.\}$$

Poiché, chiaramente, gli elementi di ordine d sono particolari radici d–esime dell'unità (e precisamente quelle primitive), si ha immediatamente il seguente:

Corollario 5.17. *Sia $\alpha \in GF(q)$ un elemento di ordine n e sia d un divisore di n. Se $\beta \in GF(q)$ è un elemento di ordine d, allora $\beta = \alpha^k$, per qualche intero k.* □

Ricordiamo che, per 5.9, vale il risultato inverso: ogni potenza di α ha per ordine un divisore di $ord(\alpha)$. Pertanto, da 5.9 e 5.17 si ha immediatamente il seguente

Corollario 5.18. *Siano $\alpha, \beta \in GF(q)$ due elementi e si ponga $ord(\alpha) = n$ e $ord(\beta) = d$. Allora*

$$d|n \quad \Longleftrightarrow \quad \beta = \alpha^k, \quad \textit{per qualche intero } k.$$

□

Poiché nel teorema 5.14 compare una fattorizzazione di $x^n - 1$ che coinvolge le potenze di una radice n–esima dell'unità, questo ci suggerisce di ripartire tali potenze a seconda del loro ordine ottenendo una corrispondente fattorizzazione del polinomio di partenza.

Si ha in tal modo il seguente risultato:

Proposizione 5.19. *Nel campo $K = GF(q)$ per ogni $n \leq q-1$ si ha la fattorizzazione:*

$$x^n - 1 = \prod_{d\in\mathbb{N}, d|n} \ \prod_{\beta\in K, ord(\beta)=d} (x - \beta).$$

Dimostrazione. Immediata da 5.14 e 5.18. □

Definizione 5.20. Il polinomio (le cui radici sono tutti e soli gli elementi di ordine d del campo) definito da

$$Q^{(d)}(x) := \prod_{\beta \in K, ord(\beta)=d} (x - \beta)$$

si dice *d–esimo polinomio ciclotomico.*

Usando la precedente definizione, un'ovvia riformulazione di 5.19 è il seguente:

Teorema 5.21. *Nel campo $K = GF(q)$ per ogni $n \leq q-1$, il polinomio $x^n - 1$ si fattorizza come prodotto di tutti i d–esimi polinomi ciclotomici, dove d varia nei divisori di n; cioè:*

$$x^n - 1 = \prod_{d \in \mathbb{N}, d|n} Q^{(d)}(x).$$

□

Come in 5.15 e in 5.15.1, se $n > q-1$ occorre introdurre un'opportuna estensione di $GF(q)$.

Esempio 5.21.1. Vogliamo fattorizzare il polinomio $x^4 - x$ in un'opportuna estensione di $\mathbb{Z}_2$. Per 5.13 l'estensione richiesta è $GF(4) = GF(2^2)$. Ovviamente

$$x^4 - x = x(x^3 - 1) = x \cdot Q^{(1)}(x) \cdot Q^{(3)}(x).$$

Ovviamente $Q^{(1)}(x) = x - 1$; quindi

$$Q^{(3)}(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1.$$

Sappiamo che $x^2 + x + 1$ è irriducibile su $\mathbb{Z}_2$, quindi occorre costruire un'estensione del tipo $\mathbb{Z}_2(a) = \mathbb{Z}_2[a]$, dove a è una radice di $x^2 + x + 1$. Abbiamo visto che

$$\mathbb{Z}_2(a) = \{b_0 + b_1 a \mid b_i \in \mathbb{Z}_2\} = \{0, 1, a, 1 + a\} = GF(4)$$

e che i 3 elementi non nulli sono potenze di a; infatti $1 = a^3$ e $1 + a = a^2$.
Infine è chiaro che $a^2 = a + 1$ è la seconda radice di $x^2 + x + 1$, dunque

$$x^2 + x + 1 = (x - a)(x - a^2).$$

Pertanto la fattorizzazione di $x^4 - x$ in $GF(4)$ è la seguente:

$$x^4 - x = x(x - 1)(x - a)(x - a^2)$$

dove $(x - a)(x - a^2) = Q^{(3)}(x)$ è il terzo polinomio ciclotomico, nel quale compaiono tutti gli elementi di ordine 3 dell'estensione considerata.