1. Anells. Anell dels enters

Definició Un anell commutatiu amb unitat és una terna $(A, +, \cdot)$ on $+$ i $\cdot$ són operacions binàries del conjunt A satisfent:

– $(A, +)$ té les propietats: [estructura de grup commutatiu]
  associativa: $\forall a, b, c \in A, \quad (a + b) + c = a + (b + c)$
  commutativa: $\forall a, b \in A, \quad a + b = b + a$
  existència d'element neutre 0: $\forall a \in A, \quad a + 0 = a$
  existència d'element simètric: $\forall a \in A, \quad \exists a' \in A, \quad a + a' = 0$
– $(A, \cdot)$ té les propietats
  associativa: $\forall a, b, c \in A, \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$
  distributiva respecte de la suma: $\forall a, b, c \in A, \quad (a + b) \cdot c = a \cdot c + b \cdot c$
  commutativa: $\forall a, b \in A, \quad a \cdot b = b \cdot a$ (anell commutatiu)
  existència d'element neutre 1: $\forall a \in A, \quad a \cdot 1 = a$ (anell amb unitat)

Conjunt dels nombres enters: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$
$(\mathbb{Z}, +, \cdot)$ és un anell commutatiu amb unitat.

Definició Sigui $(A, +, \cdot)$ un anell amb unitat, $a \in A$ és invertible si existeix $a' \in A$ tal que $a \cdot a' = a' \cdot a = 1$.

Notació $a^{-1} = a'$, s'anomena invers de a
$A^* = \{a \in A : a \text{ és invertible}\}$

Remarca
– $\mathbb{Z}^* = \{1, -1\}$.
– Si un element té invers, aquest invers és únic.

Definició $(A, +, \cdot)$ és un cos si $A^* = A \setminus \{0\}$.

Exemples
– $(\mathbb{Z}, +, \cdot)$ no és un cos
– Són cossos: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ i $(\mathbb{C}, +, \cdot)$.

Definició Sigui $(A, +, \cdot)$ un anell, $a \in A$, $a \neq 0$, és divisor de zero si existeix $b \in A$, $b \neq 0$, tal que $a \cdot b = b \cdot a = 0$.

Remarca
– $(\mathbb{Z}, +, \cdot)$ no té divisors de zero.
– Els elements invertibles de l'anell no són divisors de zero

3. Polinomis

Definició Sigui $(\mathbb{K}, +, \cdot)$ un cos. Un polinomi amb coeficients en $\mathbb{K}$ i indeterminada x és una expressió $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ amb $a_n, \ldots, a_1, a_0 \in \mathbb{K}$.

Notació $\mathbb{K}[x] = \{a_n x^n + \cdots + a_1 x + a_0 : a_n, \ldots, a_1, a_0 \in \mathbb{K}\}$.

Dos polinomis $a(x) = a_n x^n + \cdots + a_1 x + a_0$ i $b(x) = b_m x^m + \cdots + b_1 x + b_0$ són iguals si, i només si, $a_i = b_i$, $0 \leq i \leq n$.

Sigui $a(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{K}[x]$ un polinomi, anomenem

Polinomi constant: si $a_i = 0$ per a tot $i \geq 1$.

Grau: si $a(x)$ és diferent de zero, el grau és el màxim n tal que $a_n \neq 0$.

Notació $\deg(a(x))$, $\mathrm{gr}(a(x))$.

$\deg(0) = -\infty$.

Coeficient principal: a_n, si $a(x)$ té grau n.

Polinomi mònic: si el coeficient principal és 1.

Operacions entre polinomis

Siguin $a(x) = a_n x^n + \cdots + a_1 x + a_0$ i $b(x) = b_n x^n + \cdots + b_1 x + b_0$ polinomis de $\mathbb{K}[x]$.

Suma $a(x) + b(x)$: coeficient de $x^i = a_i + b_i$

Producte $a(x)b(x)$: coeficient de $x^i = a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0$.

$(\mathbb{K}[x], +, \cdot)$ és un anell commutatiu amb unitat.

Proposició Siguin $a(x), b(x) \in \mathbb{K}[x]$. Aleshores

1. $\deg(a(x)) = 0 \Leftrightarrow a(x) = a_0$ i $a_0 \neq 0$.
2. $\deg(a(x) + b(x)) \leq \max\{\deg(a(x)), \deg(b(x))\}$
3. $\deg(a(x)b(x)) = \deg(a(x)) + \deg(b(x))$.

Corol.lari Els elements invertibles de $\mathbb{K}[x]$ són els polinomis constants no nuls:

$$\mathbb{K}[x]^* = \mathbb{K}^*$$

.

4. Anell de polinomis $\mathbb{K}[x]$

$\mathbb{K}$ serà un cos, per exemple, $\mathbb{F}_p$, $\mathbb{Q}$, o $\mathbb{R}$.

Recordem que $(\mathbb{K}[x], +, \cdot)$ és un anell amb unitat, i $\mathbb{K}[x]^* = \mathbb{K}^*$.

Teorema de la divisió Siguin $a(x), b(x) \in \mathbb{K}[x]$, amb $b(x) \neq 0$. Aleshores existeixen dos únics polinomis $q(x)$ (quocient) i $r(x)$ (residu) tals que

$$a(x) = b(x)q(x) + r(x), \text{ on } r(x) = 0 \text{ o } \deg(r(x)) < \deg(b(x)).$$

Definicions Siguin $a(x), b(x) \in \mathbb{K}[x]$,

$b(x)$ és divisor de $a(x)$ o bé $a(x)$ és múltiple de $b(x)$ si el residu de la divisió de $a(x)$ entre $b(x)$ és $r(x) = 0$.

Notació $b(x)|a(x)$

Remarca $\forall b(x) \in \mathbb{K}[x],\ b(x)|0$.

Divisors impropis de $a(x)$: són els polinomis $\lambda a(x)$ i λ, per a tot $\lambda \in \mathbb{K}^*$.

Divisors propis de $a(x)$ en $\mathbb{K}[x]$: els divisors diferents dels impropis.

Polinomi irreductible a $\mathbb{K}[x]$: polinomi de grau ≥ 1 que no té divisors propis a $\mathbb{K}[x]$, és a dir, que no es pot escriure com a producte de polinomis de grau estrictament menor a $\mathbb{K}[x]$.

Definició Siguin $a(x), b(x) \in \mathbb{K}[x]$.

Un màxim comú divisor de $a(x)$ i $b(x)$ és un polinomi de $\mathbb{K}[x]$ de grau màxim que divideix a $a(x)$ i a $b(x)$.

Notació $\mathrm{mcd}(a(x), b(x))$.

Remarques:
- Si $d(x)$ és un $\mathrm{mcd}(a(x), b(x))$, aleshores $\lambda d(x)$ és també un $\mathrm{mcd}(a(x), b(x))$, $\forall \lambda \in \mathbb{K}$.
- Hi ha un únic màxim comú divisor mònic.
- Si $c(x)|a(x)$ i $c(x)|b(x)$, aleshores $c(x)|\mathrm{mcd}(a(x), b(x))$.
- Si $d(x)$ i $k(x)$ són mcd de $a(x), b(x)$, aleshores $\exists \lambda \in \mathbb{K}^*$ tal que $d(x) = \lambda k(x)$.
- Si $a(x)$ és irreductible: $\mathrm{mcd}(a(x), b(x)) = 1$ si, i només si, $b(x)$ no és un múltiple de $a(x)$.

Lema

Siguin $a(x), b(x), k(x) \in \mathbb{K}[x]$. Aleshores

$$\mathrm{mcd}(a(x), b(x)) = \mathrm{mcd}(a(x) + b(x)k(x), b(x)).$$

Teorema (Algorisme d'Euclides)

Siguin $a(x), b(x) \in \mathbb{K}[x]$, $b(x) \neq 0$. Definim $r_0(x) = a(x)$ i $r_1(x) = b(x)$.

Considerem les divisions enteres,

$$\begin{array}{rcll} r_0(x) & = & r_1(x)q_1(x) + r_2(x), & 0 \leq \deg(r_2(x)) < \deg(r_1(x)) \\ r_1(x) & = & r_2(x)q_2(x) + r_3(x), & 0 \leq \deg(r_3(x)) < \deg(r_2(x)) \\ & & \cdots & \\ r_{n-2}(x) & = & r_{n-1}(x)q_{n-1}(x) + r_n(x), & 0 \leq \deg(r_n(x)) < \deg(r_{n-1}(x)) \\ r_{n-1}(x) & = & r_n(x)q_n(x) & \end{array}$$

Aleshores, $\mathrm{mcd}(a(x), b(x)) = \begin{cases} b(x), & \text{si } n = 1, \text{ és a dir , } r_2(x) = 0; \\ r_n(x), & \text{altrament.} \end{cases}$

Teorema (Identitat de Bezout)

Per a tot $a(x), b(x), \in \mathbb{K}[x]$ existeixen $s(x), t(x) \in \mathbb{K}[x]$ tals que

$$a(x)s(x) + b(x)t(x) = \mathrm{mcd}(a(x), b(x)).$$

Remarca

$\mathrm{mcd}(a(x), b(x)) = 1 \Leftrightarrow \exists\, s(x), t(x) \in \mathbb{K}$ tals que $a(x)s(x) + b(x)t(x) = 1$

Cálculs: Algoritme d'Euclides estès

$$\begin{array}{ll} s_0(x) = 1, & t_0(x) = 0, \\ s_1(x) = 0, & t_1(x) = 1, \\ s_k(x) = s_{k-2}(x) - q_{k-1}(x)s_{k-1}(x), & 2 \leq k \leq n, \\ t_k(x) = t_{k-2}(x) - q_{k-1}(x)t_{k-1}(x), & 2 \leq k \leq n. \end{array}$$

k	0	1	2	3	$\cdots$	$n-1$	n
$s_k(x)$	1	0	$s_2(x)$	$s_3(x)$	$\cdots$	$s_{n-1}(x)$	$s_n(x)$
$t_k(x)$	0	1	$t_2(x)$	$t_3(x)$	$\cdots$	$t_{n-1}(x)$	$t_n(x)$
$q_k(x)$		$q_1(x)$	$q_2(x)$	$q_3(x)$	$\cdots$	$q_{n-1}(x)$	$q_n(x)$
$r_k(x)$	$r_0(x) = a(x)$	$r_1(x) = b(x)$	$r_2(x)$	$r_3(x)$	$\cdots$	$r_{n-1}(x)$	$r_n(x)$

Es té: $a(x)s_k(x) + b(x)t_k(x) = r_k(x)$, per a tot k, $0 \leq k \leq n$.

En particular, $a(x)s_n(x) + b(x)t_n(x) = r_n(x) = \mathrm{mcd}(a(x), b(x))$.

Divisors impropis de $a(x)$: són els polinomis $\lambda a(x)$ i λ, per a tot $\lambda \in \mathbb{K}^*$

Divisors propis de $a(x)$: els divisors diferents dels impropis

Polinomi irreductible: polinomi de grau ≥ 1 que no té divisors propis, és a dir, que no es pot escriure com a producte de polinomis de grau estrictament menor

Arrel d'un polinomi: α és arrel de $a(x)$ si $a(\alpha) = 0$

Teorema del residu Siguin $\alpha \in \mathbb{K}$ i $a(x) \in \mathbb{K}[x]$. Aleshores,

1. $a(\alpha) = 0 \iff (x - \alpha) | a(x)$.
2. El nombre d'arrels de $a(x)$ és $\leq \deg(a(x))$.

Proposició Sigui $a(x) \in \mathbb{K}[x]$.

1. Els polinomis de grau 1 són irrreductibles i tenen exactament una arrel.
2. Si un polinomi de grau ≥ 2 té una arrel, llavors no és irreductible.
3. Els polinomis de grau 2 o 3 són irreductibles $\iff$ no tenen cap arrel.

Teorema Per a tot polinomi $a(x) \in \mathbb{K}[x] - \mathbb{K}$ existeixen $\lambda \in \mathbb{K}$, enters positius $n_1, n_2, \ldots, n_k$ i polinomis mònics irreductibles $f_1(x), f_2(x), \ldots, f_k(x)$, únics llevat l'ordre, tals que

$$a(x) = \lambda f_1(x)^{n_1} f_2(x)^{n_2} \ldots f_k(x)^{n_k}.$$

Aquesta igualtat s'anomena factorització de $a(x)$ en producte de factors irreductibles.

5. Anell quocient de polinomis

Fixem $f(x) \in \mathbb{K}[x]$, amb $f(x) \neq 0$ i sigui $n = deg(f)$.

Definició Siguin $a(x), b(x) \in \mathbb{K}[x]$. Direm que

$a(x)$ és congru amb $b(x)$ mòdul $f(x)$ si $f(x)|(a(x) - b(x))$

Notació $a(x) \equiv b(x) \pmod{f(x)}$

Formulació equivalent
$a(x) \equiv b(x) \pmod{f(x)}$ si, i només si, la divisió entera de $a(x)$ i $b(x)$ per $f(x)$ dóna el mateix residu.

Ser congru mòdul $f(x)$ és una relació d'equivalència, és a dir, compleix:
1.- $a(x) \equiv a(x) \pmod{f(x)}$ (P. reflexiva)
2.- $a(x) \equiv b(x) \pmod{f(x)} \Rightarrow b(x) \equiv a(x) \pmod{f(x)}$ (P. simètrica)
3.- $a(x) \equiv b(x) \pmod{f(x)}$ i $b(x) \equiv c(x) \pmod{f(x)} \Rightarrow$
$a(x) \equiv c(x) \pmod{f(x)}$ (P. transitiva)

Sigui $P_n(\mathbb{K}) = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} | a_i \in \mathbb{K}, i \in \{0, \ldots, n-1\}\}$. Per a tot $a(x) \in \mathbb{K}[x]$ existeix un únic polinomi $r(x) \in P_n(\mathbb{K})$ tal que
$$a(x) \equiv r(x) \pmod{f(x)}.$$

Definició Classe de $a(x)$ mòdul $f(x)$: conjunt dels polinomis congrus amb $a(x)$ mòdul $f(x)$. Es denota:
$$\begin{aligned} \overline{a(x)} = & \quad \{b(x) \in \mathbb{K}[x] : a(x) \equiv b(x) \mod f(x)\} \\ = & \quad \{a(x) + f(x)g(x) : g(x) \in \mathbb{K}[x]\} \end{aligned}$$

Observem:
– $\overline{a(x)} \neq \emptyset$, ja que $a(x) \in \overline{a(x)}$.
– $\overline{a(x)} = \overline{b(x)} \iff a(x) \equiv b(x) \pmod{f(x)}$.
– $\overline{a(x)} \cap \overline{b(x)} = \emptyset \iff a(x) \not\equiv b(x) \pmod{f(x)}$.

Definició Conjunt quocient de $\mathbb{K}[x]$ mòdul $f(x)$

$$\begin{aligned} \mathbb{K}[x]/(f(x)) &= \{\overline{a(x)} : a(x) \in \mathbb{K}[x]\} \\ &= \left\{\overline{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}} | a_i \in \mathbb{K}, i \in \{0, \ldots, n-1\}\right\} \end{aligned}$$

Compatibilitat de la relació d'equivalència amb les operacions a $\mathbb{K}[x]$
Siguin $a(x), b(x), c(x), d(x) \in \mathbb{K}[x]$ polinomis tals que $a(x) \equiv b(x) \pmod{f(x)}$ i $c(x) \equiv d(x) \pmod{f(x)}$, aleshores:
$$a(x) + c(x) \equiv b(x) + d(x) \pmod{f(x)}, \text{ i}$$
$$a(x)c(x) \equiv b(x)d(x) \pmod{f(x)}.$$

Definició Es defineixen les operacions següents a $\mathbb{K}[x]$,

suma: $\overline{a(x)} + \overline{b(x)} := \overline{a(x) + b(b)}$,

producte: $\overline{a(x)} \cdot \overline{b(x)} := \overline{a(x) \cdot b(x)}$.

Proposició $(\mathbb{K}[x]/(f(x)), +, \cdot)$ és un anell commutatiu amb unitat.

Elements invertibles a $\mathbb{K}[x]$

Proposició Siguin $f(x), a(x) \in \mathbb{K}[x]$, amb $\deg(f) \geq 1$.
$\overline{a(x)}$ invertible a $\mathbb{K}[x]/(f(x))$ si, i només si, $\mathrm{mcd}(a(x), f(x)) = 1$.
És a dir, $(\mathbb{K}[x]/(f(x)))^* = \left\{\overline{a(x)} : \mathrm{mcd}(a(x), f(x)) = 1\right\}$.

Remarca: Si $f(x)$ és irreductible, aleshores

$$(\mathbb{K}[x]/(f(x)))^* = \left\{\overline{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}} | a_i \in \mathbb{K}\right\} - \{\bar{0}\}.$$

Proposició $\mathbb{K}[x]/(f(x))$ és un cos si, i només si, $f(x)$ és un polinomi irreductible.

En particular: Si $\mathbb{K} = \mathbb{F}_p$ i $f(x) \in \mathbb{F}_p[x]$ irreductible de grau n, aleshores el cos $\mathbb{F}_p[x]/(f(x))$ té cardinal p^n.

6. Cossos finits

Teorema

1. Els cossos finits són de la forma $\mathbb{Z}_p$ o $\mathbb{Z}_p[x]/(f(x))$, on $f(x) \in \mathbb{Z}_p[x]$ és un polinomi irreductible, p nombre primer.
   Notació: $\mathbb{F}_p = \mathbb{Z}_p$,
   $\mathbb{F}_q = \mathbb{Z}_p[x]/(f(x))$, on $q = p^{deg(f)}$.

2. Per cada enter $r \geq 1$ i per cada primer p existeix un cos finit de p^r elements.

3. Dos cossos finits del mateix ordre són isomorfs.

Característica d'un cos finit. Donat una cos finit de p^r elements, direm el cos té característica p.

Observem que p és l'enter positiu més petit tal que

$$\overbrace{1 + \cdots + 1}^{p} = 0 \quad \text{i} \quad \overbrace{1 + \cdots + 1}^{s} \neq 0, \forall s, 1 \leq s < p.$$

Sigui p primer i $r \geq 1$ enter. El cos finit $\mathbb{F}_q$ té $q = p^r$ i el conjunt dels invertibles $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ té $q-1$ elements

Proposició $(\mathbb{F}_q^*, \cdot)$ té estructura de grup multiplicatiu (cíclic).

Definicions
Ordre de $\beta \in \mathbb{F}_q^*$, $\text{ord}(\beta)$: l'enter $m \geq 1$ més petit tal que $\beta^m = 1$.
Element primitiu: l'element $\alpha \in \mathbb{F}_q$ tal que $\text{ord}(\alpha) = q-1$.

Propietats de l'ordre Sigui $\beta \in \mathbb{F}_q$ i $m = \text{ord}(\beta)$. Aleshores

1. $m|(q-1)$, és a dir, l'ordre d'un element divideix el cardinal de $\mathbb{F}_q^*$.
2. $s \in \mathbb{Z}$: $\beta^s = 1 \Leftrightarrow m|s$.
3. $\beta^{q-1} = 1$.
4. $\text{ord}(\beta^d) = \frac{m}{\text{mcd}(m,d)}$, per a tot $d \in \mathbb{Z}$, $d \geq 1$.
5. L'únic element d'ordre 1 és l'1.

Proposició El nombre d'elements d'ordre d a $\mathbb{F}_q^*$ és $\begin{cases} \phi(d), & \text{si } d|(q-1); \\ 0, & \text{altrament.} \end{cases}$

Corol.lari 1 Tot cos finit té un element primitiu.

Corol.lari 2 El nombre d'elements primitius a $\mathbb{F}_q$ és $\phi(q-1)$.

Definició Fixat $\beta \in \mathbb{F}_q^*$ un element primitiu es defineix logaritme discret en base β a l'aplicació

$$\begin{array}{rccl} \log_\beta : & \mathbb{F}_q^* & \to & \mathbb{Z}_{q-1} \\ & \gamma & \mapsto & i, \text{ si } \gamma = \beta^i \end{array}$$

L'aplicació està ben definida i és bijectiva.

Definició Un polinomi $f(x) \in \mathbb{F}_p[x]$ és diu primitiu si és irreductible i $\alpha = \bar{x} \in \mathbb{F}_p[x]/(f(x))$ és un element primitiu del cos.