Def: $(M,*)$ es un monoide si $*$ es cerrada, asociativa, y tiene elemento neutro.

Def: $(G,*)$ es un grupo si es un monoide y cada elemento de G tiene simétrico n.a $*$.

Def: $U(M) = \{a \in M : \exists a^{-1} \in M : aa^{-1} = 1\}$. Es un grupo.

Def: $(A,+,\cdot)$ es un anillo si:

- $(A,+)$ es un grupo conmutativo.
- $(A,\cdot)$ es un monoide
- $a(b+c) = ab+ac$; $(b+c)a = ba+ca$

Props. anillos

- $a0 = 0 = 0a$
- $|A| \geq 2 \iff 1 \neq 0$
- $(-a)b = -(ab) = a(-b)$
- $(-a)(-b) = ab$
- $(-1)a = -a$
- $(-1)(-1) = 1$
- $\left(\sum_1^n a_i\right)\left(\sum_1^m b_j\right) = \sum_1^n \sum_1^m a_i b_j$

Def: Un cuerpo es un anillo conmutativo con $U(A) = A^* \stackrel{\wedge}{=} A \setminus \{0\}$

Def: $(A,+,\cdot)$ anillo, $\emptyset \neq S \subseteq A$. S es subanillo de A si: $(S,+,\cdot)$ es anillo

- $-1, 1 \in S$
- $x,y \in S \Rightarrow x+y \in S$
- $x,y \in S \Rightarrow xy \in S$

Def: Un dominio de integridad es un anillo conmutativo no trivial donde A^* es cerrado para $\cdot$

Equivalencias:

- $\forall x,y \in A \ \forall a \in A^* \quad ax = ay \Rightarrow x = y$
- $\forall a,b \in A \ a \neq 0, \ ab = 0 \Rightarrow b = 0$
- $\forall a,b \in A \quad ab = 0 \Rightarrow a = 0 \vee b = 0$
- $\forall a,b \in A^* \quad ab \neq 0$
- $\exists x \in A \ ax = b \Rightarrow \exists! x \in A \ ax = b$
- En conjuntos finitos, es un cuerpo
- $S \preceq A$ D.I. $\Rightarrow S$ D.I.

Def: $a|b \iff \exists c \in A^* : ac = b$ Def: $a \sim b \iff a|b \wedge b|a$

Props. divisibilidad

- $0|b \iff b = 0$
- $a|1 \iff a \in U(A)$
- $\forall a \in A: a|0$
- $u \in U(A) \Rightarrow u|a \ \forall a \in A$
- $\forall a \in A \ a|a$
- $a|b \wedge b|c \Rightarrow a|c$
- $a|b \wedge a|c \Rightarrow a|bx+cy$
- $a|b \Rightarrow a|bc$
- $(c \neq 0) \ a|b \iff ac|bc$

Def: Un dominio euclídeo es un dom. de int. si $\exists \phi : A^* \to \mathbb{N}$

1) $\phi(ab) \geq \phi(a)$ 2) $\forall a,b \in A^* / \phi(a) \geq \phi(b) \ \exists q,r \in A: a = bq + r \wedge (r = 0 \vee \phi(r) < \phi(b))$

Ejemplos: $\mathbb{Z}$, $A[x]$ (A D.I.), $\mathbb{Z}[\sqrt{n}]$ $(n = -1, 1, -2, 2, 3)$

Def: El máximo común divisor de a y b, $(a,b) = d$ es un número tal que:

1) $d|a, d|b$ 2) $c|a, c|b \Rightarrow c|d$

Props. mcd

- $(a,b) = (b,a)$
- $(a,b) = a \iff a|b$
- $(a,0) = a$
- $(a,1) = 1$
- $a|c, b|c \ (a,b) = 1 \Rightarrow ab|c$
- p irr. $\iff p = ab \Rightarrow a \in U(A) \vee b \in U(A)$
- p irr. $(p,a) = p|a \ ? \ p : 1$;
- $(a,(b,c)) = ((a,b),c)$
- $(ac,bc) = (a,b)c$
- $(a,b) = 1, (a,c) = 1 \iff (a,bc) = 1$
- $c|a, c|b \Rightarrow \left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a,b)$
- $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$
- $a|b \Rightarrow a|(a,b)c$
- $a|bc, (a,b) = 1 \Rightarrow a|c$
- $(a,b) = (a - qb, b) \ \forall q \in A$

Def: Un dominio de ideales principales es un D.I. donde todo ideal es principal.

Def: Un ideal es un subconjunto no vacío ~~donde cada~~ cerrado para sumas y múltiplos

Teorema: Todo dominio euclídeo es dominio de ideales principales.

Teorema: A DIP. $\forall a,b \in A\ \exists (a,b)$, $\exists u,v \in A$: $au+bv = (a,b)$

Teorema: A DIP, $a,b \in A^*$, $c \in A$:

1) $\exists x,y \in A$: $ax+by=c \iff (a,b) \mid c$ 2) $x = x_0 + k\, b/d \quad y = y_0 - k\, a/d$

Def: $a,b \in A$ D.I., $m \in A$ es mínimo común múltiplo de a,b si:

1) $a \mid m$, $b \mid m$ 2) $a \mid c,\ b \mid c \Rightarrow m \mid c$

Prop: $\exists [a,b] \Rightarrow \exists (a,b)$, $(a,b)[a,b] = ab$

Teorema: $\forall a,b \in A\ \exists (a,b) \Rightarrow \forall a,b \in A\ \exists [a,b]$

Def: A D.I., $I \subseteq A$ ideal. $a \equiv_I b \iff a-b \in I$

Props $\equiv$

- $a \equiv b \iff a+c \equiv b+c$
- $a \equiv b,\ c \equiv d \Rightarrow a+c \equiv b+d$
- $a \equiv 0 \iff a \in I$
- $a \equiv b \Rightarrow ac \equiv bc$
- $a \equiv b,\ c \equiv d \Rightarrow ac \equiv bd$
- $(c,m) = 1 \Rightarrow (a \equiv_m b \iff ac \equiv_m bc)$

Def: $\varphi: A \to B$ es homomorfismo si:

1) $\varphi(a+b) = \varphi(a)+\varphi(b)$ 2) $\varphi(ab) = \varphi(a)\varphi(b)$ 3) $\varphi(1) = 1$

Props:

- $\varphi(0) = 0$
- $u \in U(A) \Rightarrow \varphi(u) \in U(B)$
- $\varphi: A \hookrightarrow B$. $A \cong \operatorname{Img}\varphi$
- $\varphi(-a) = -\varphi(a)$
- $\operatorname{Img}\varphi \leq B$

Propiedad universal del anillo de polinomios

Sea $\varphi: A \underset{\text{hom}}{\overset{\text{con}}{\to}} B^{\text{con}}$. $\forall u \in B\ \exists! \varphi_u: A[x] \xrightarrow{\text{homo}} B$ tal que:

1) $\varphi_u(a) = \varphi(a)\ \forall a \in A \cong \{p \in A[x] : gr(p) = 0\}$

2) $\varphi_u(x) = u$

Anillos cocientes

Sea $I \subseteq A$ ideal. $A/I = \{[x] : x \in A\}$, $[x] = \{y \in A : x \equiv_I y\}$. A/I es un anillo.

Def: $\operatorname{Ker}(\varphi) = \varphi^{-1}(0)$ Prop: $\operatorname{Ker}(\varphi) = \{0\} \iff \varphi$ es monomorfismo

Teorema (1er t. de isomorfía): Si $\varphi: A \xrightarrow{\text{hom}} B \Rightarrow \exists \overline{\varphi}: A/\operatorname{Ker}\varphi \xrightarrow{\sim} \operatorname{Img}\varphi$, dado por $\overline{\varphi}([a]) = \varphi(a)$

Teorema: A DIP. $n \in A$, $n \neq 0$, $n \notin U(A)$.

1) $[a] \in U(A/nA) \iff (a,n) = 1\ \forall a \in A$

2) $\forall x \in A/nA$ $x \mid 0 \lor x \in U(A/nA)$

$ax \equiv_m b$

1) Existe solución $\iff (a,m) \mid b$
2) Es equivalente a $a'x \equiv_{m'} b'$, $a' = a/d$, $b' = b/d$, $m' = m/d$
3) una solución particular será $x_0 = b'u'$, donde $1 = (a', m') = a'u' + m'v'$
4) una solución óptima será, $x_0 = 0$ o $\varphi(x_0) < \varphi(m')$
5) la solución general será: $x = x_0 + km'$

$$\begin{cases} x \equiv_{m_1} a_1 \\ x \equiv_{m_2} a_2 \end{cases}$$

1) Existe solución $\iff a_1 \equiv_{(m_1, m_2)} a_2$
2) si tiene solución, el sistema es equivalente a $x \equiv_{[m_1, m_2]} x_0$ para una solución particular x_0
3) Para hallar x_0, hacemos $a_1 + m_1 k_0 \equiv_{m_2} a_2$

Resto de a^{b^c} al dividir por m:

1) si $(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv_m 1$.

 1.1) Hallar x, tal que $x \equiv_{\varphi(m)} b^c$
 1.2) $a^{b^c} \equiv_m a^{x + k\varphi(m)} \equiv_m a^x$
2) En otro caso, descomponer a en primos, $a = \prod p^i$.
 $R(a^{bc}) = \prod R(p^{b^c})$
3) Si a es primo, y $(a,m) \neq 1 \Rightarrow$ hallar k tal que $a^k \equiv_m a$

Algoritmo de Euclides

ENTRADA: $a, b \in A^*$ D.E.
SALIDA: $((a,b), u, v) \mid ((a,b) = au + bv)$

Proceso:

1) Hallar $\varphi(a), \varphi(b)$. Si $\varphi(a) < \varphi(b)$, intercambiar.

2) Hallar q_1, r_1 tales que $a = bq_1 + r_1$.

3) SI $r = 0$, DEVUELVE $(b, 0, 1)$. FIN

EN OTRO CASO:

Añade una fila a la tabla:

$$\begin{array}{c|cc} a & 1 & 0 \\ b & 0 & 1 \\ r_1 & u_1 & v_1 \\ \vdots & & \vdots \\ r_n & u_n & v_n \\ 0 & & \end{array}$$

calcula u_{i+2}, v_{i+2}:

$u_{i+2} := u_i - q_{i+2} u_{i+1}$

$v_{i+2} := v_i - q_{i+2} v_{i+1}$

LLAMA: EUCLIDES(b, r_1).
* DEVUELVE:

Ecuaciones diofánticas $ax + by = c$

1) Hallar (a,b). La ecuación tiene solución sólo si $(a,b) \mid c$

2) Calcular $a' := \frac{a}{(a,b)}$, $b' := \frac{b}{(a,b)}$, $c' := \frac{c}{(a,b)}$

3) Hallar u, v tales que $(a,b) = au + bv \Rightarrow 1 = a'u + b'v$

4) Una solución particular es $x_0 = c'u$, $y_0 = c'v$

5) La solución general es: $x = x_0 + Kb'$, $y = y_0 - Ka'$

Mínimo común múltiplo entre a y b)

1) Hallar (a,b)
2) $[a,b] = \frac{ab}{(a,b)}$

Descomposición en $\mathbb{Z}[\sqrt{n}]$

•) $\beta \mid \alpha \Rightarrow N(\beta) \mid N(\alpha)$

•) $N(\alpha)$ primo $\Rightarrow \alpha$ irreducible

•) α primo $\Rightarrow N(\alpha) = p$ ó $\pm p^2$ (primo)

Descomposición en $A[x]$

•) $ax+b$ $(a,b)=1$ es irr. en $A[x]$

•) $f(k) = 0 \Rightarrow f$ no irr.

•) $gr(f) = 2$ ó 3 (f irr $\Leftrightarrow \nexists k : f(k)=0$) y es prim.)

Criterio de reducción módulo un primo

p irr. de $\mathbb{Z}$. $\sum a_i x^i \mapsto \sum R_p(a_i) x^i$. Si $gr(f) = gr(f_p)$,

f_p no t. div. de grado n en $\mathbb{Z}_p[x] \Rightarrow f$ no tiene en $\mathbb{Z}[x]$

Criterio de Eisenstein

$f(x) = \sum a_i x^i$ primitivo, $n \geq 2$

i) ($\exists p$ irr. : $p \mid a_i$ $(0 \dots n-1)$, $p^2 \nmid a_0$) $\Rightarrow f$ irreducible

ii) ($\exists p$ irr : $p \mid a_i$ $(1 \dots n)$, $p^2 \nmid a_n$) $\Rightarrow f$ irreducible