Unidad 4: Semigrupos, Monoides y Grupos

Lema: • e es único si existe
• x^{-1} es único si existe

Lema: $*$ asoc. y $\exists\, x^{-1}, y^{-1} \Rightarrow \exists\, (x*y)^{-1} = y^{-1} * x^{-1}$

Def.: $*$ cerrada en Y si $x*y \in Y \;\forall\, x,y \in Y$ revisar apunte
↳ si $Y \subset X$, $(Y,*)$ hereda las props. de $*$ en X

$X/\sim \;\to$ conj. cociente: $\{[a] \,/\, a \in X\}$ $\equiv \overline{a}$
↳ clase eq.: $\{y \in X \,/\, a \sim y\}$
↳ definido por la proy. canónica
↳ $\pi : X \to X/\sim$
$\pi(x) = [x]$

Def: $*$ se induce a $X/\sim$ si

$$\left.\begin{array}{l} x \sim x' \\ y \sim y' \end{array}\right\} x*y \sim x'*y'$$

↳ $\Rightarrow [x]*[y] = [x*y]$
$X/\sim$ X

Def: • $\mathbb{Z}_m = \mathbb{Z}/_{\equiv(m)}$
↳ $x \sim y \Leftrightarrow x \equiv y(m) \Leftrightarrow x-y = km,\; k \in \mathbb{Z}$ $x \equiv y \bmod m$
↳ x/m e y/m tienen el mismo resto

• $+$ y $*$ se inducen a $\mathbb{Z}_m$

Ej: $\mathbb{Z}_5 = \mathbb{Z}/_{\equiv(5)} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ e
$\overline{2}+\overline{4} = \overline{2+4} = \overline{6} = \overline{1}$
$\overline{2}^{-1} = \overline{2^{-1}} = \overline{-2} = \overline{3}$

Teorema: si $*$ inducida a $X/\sim$ $\Rightarrow$ preserva
- asoc.
- conm.
- neutro $([e])$
- inversos $([x^{-1}])$

Teorema: $\bar{k} \in \mathbb{Z}_m$, $\bar{k}$ admite inv. mult. $\Leftrightarrow$ $\text{mcd}(k,m)=1$

↳ k y m son coprimos

$\therefore$ p primo $\Rightarrow$ todo elem salvo $\bar{0}$ admite inv. en $\mathbb{Z}_p$

↳ $\therefore (\mathbb{Z}, *)$ grupo $\Rightarrow$ sacar el 0

Definición: X conj. y $\cdot : X \times X \to X$

1. $\cdot$ asoc. $\Rightarrow (X, \cdot)$ semigrupo
2. $(X, \cdot)$ semig. y admite e $\Rightarrow$ monoide
3. $(X, \cdot)$ monoide y admite $x^{-1}\ \forall x$ $\Rightarrow$ grupo
3. $\cdot$ conm. y $(X, \cdot)$ grupo / semig. / monide $\Rightarrow (X, \cdot)$ grupo / semig. / monoide abeliano

Notación: en grupos, la op. se omite $\Rightarrow x \cdot y = xy$

↳ ojo: no confundir con not. aditiva

Def: estructura producto

$(x,y) * (x',y') = (x *_1 x', y *_2 y')$

$$(X, *_1) \text{ y } (Y, *_2) \Rightarrow (X \times Y, *)$$

Props.:

1. la estruct. producto preserva semig., monoide y grupo
2. la estruct. cociente 〃

Teorema: en $(X, \cdot)$ grupo

$$a \cdot b = a \cdot c \Rightarrow b = c$$
$$b \cdot a = c \cdot a \Rightarrow b = c$$

→ no se puede usar cancelación si $(X, \cdot)$ no es grupo

Definición: subestructuras

1. $(Y,*)$ subsemig. de X si $(X,*)$ semig. y $*$ cerrada para Y
2. $(Y,*)$ submonoide de X si $(X,*)$ monoide, $*$ cerrada para Y y $e\in Y$
3. $(Y,*)$ subgrupo de X si $(X,*)$ grupo, $*$ cerrada para Y, $e\in Y$ y $x^{-1}\in Y$ $\forall x\in Y$

→ Alternativamente: sea G grupo

a. $(H,*)$ subgrupo de G si $H\neq\emptyset$, $*$ cerrada para H y $(H,*)$ grupo → notese que $H\subset G$ y H monoide/semig. $\not\Rightarrow$ H submonoide/subsemig. de G

b. H subgrupo de G $\Leftrightarrow$ $H\neq\emptyset$, $H\subset G$ y $ab^{-1}\in H$ $\forall a,b\in H$

Def: Morfismos

Sean $(X,\cdot)$ y $(Y,*)$, $f:X\to Y$ es un morfismo u homomorfismo de semigrupos $f(x\cdot y)\mapsto f(x)*f(y)$

- Si además $f(e_X)=e_Y$ $\Rightarrow$ f homom. de monoide
- " $f(x^{-1})=f(x)^{-1}$ $\forall x\in X$ $\Rightarrow$ f homom. de grupos
- " f biyectivo tq f^{-1} homomorfismo $\Rightarrow$ f isomorfismo

Teorema: $(G,\cdot)$ y $(H,*)$ grupos

$f:G\to H$ homom. de grupos $\Leftrightarrow$ f homom. de semig.

Teorema: $f:X\to Y$, $g:Y\to Z$ homomorfismos

1. $g\circ f$ homomorfismo
2. f isomorfismo $\Rightarrow$ f^{-1} isomorfismo
3. f y g isomorfos $\Rightarrow$ $g\circ f$ isomorfo

Def.: el grupo $(\mathrm{Iso}(X),\circ)$ se denomina grupo de isomorfismos de X

Props. de la Práctica 4

Prop. : sea $(X, *)$ semig.

1. $x^n * x^m = x^{n+m}$
2. $(x^n)^m = x^{nm}$

Prop. : sea $(X, *)$ grupo $\Rightarrow (xy)^{-1} = y^{-1}x^{-1}$

Def. : $f : X \to Y$ equivariante si $x \sim y \Rightarrow f(x) = f(y)$

Prop: sea G grupo

G abeliano $\Leftrightarrow (ab)^n = a^n b^n \ \forall a, b \in G$ y $n \in \mathbb{Z}$

Def. : sea $f : G \to H$ homom. de grupos

$$\ker(f) = \{x \in G : f(x) = e_H\}$$

luego $\ker(f)$ es subgrupo de G $\hookrightarrow$ Importante : $\ker(f)$ es siempre normal

Capítulo 5: Grupos

Repaso:

$(G, *)$ grupo si
- $*$ asociativa
- $\exists\, e \in G$ para $*$
- $\exists\, x^{-1}\ \forall x \in G \,/\, xx^{-1} = e$

} e y x^{-1} deben conmutar siempre

además $*$ conm. $\Rightarrow$ grupo abeliano

↳ sea $H < G$ y G abeliano $\Rightarrow H$ abeliano

Notación:
- $o(G) = |G|$ para G conjunto
- $o(a) = |\langle a \rangle|$ para a elemento

Caracterización: Subgrupos

Sea G grupo y $H \subset G$, H subgrupo si:
1. $(H, \cdot)$ es grupo
2. H cerrado para $\cdot$, $e \in H$ y $x^{-1} \in H\ \forall x \in H$
3. $xy^{-1} \in H\ \forall x, y \in H$ → preferida
   ↳ y $H \neq \emptyset$

Notación: Multiplicativa vs. aditiva

- $a^0 = e$
- $a^n = a^{n-1} \cdot a$
- $a^{n+m} = a^n \cdot a^m$
- $a^{nm} = (a^n)^m$

Multiplicativa
- la potencia no implica productos
- leer como $a^n = \underbrace{a \cdot a \cdot a \cdot \ldots \overset{\text{op. del grupo}}{\cdot} a}_{n \text{ veces}}$

- $0a = 0$
- $na = (n-1)a + a$
- $(n \overset{\text{suma}}{+} m)a = na \overset{\text{op. grupo}}{+} ma$
- $(mn)a = m(na)$

Aditiva
- no es un producto entre escalar y elem. de G
- leer como $na = \underbrace{a + a + a + \ldots \overset{\text{op. del grupo}}{+} a}_{n \text{ veces}}$

Notación:

$H < G \longrightarrow H$ subgrupo de G

$H \triangleleft G \longrightarrow H$ subgrupo normal de G

Def.:

$\langle a \rangle$ es siempre el menor subgrupo de G tq $a \in \langle a \rangle$

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\} < G$$

$\hookrightarrow \therefore \exists\ a^0 = e$ y a^{-1}

$\langle a \rangle$ se llama subgrupo cíclico de G generado por a

si $\langle a \rangle = G \Rightarrow G$ grupo cíclico con a generador de G

$\hookrightarrow$ ej: $\langle 1 \rangle = \mathbb{Z}$, $\langle -1 \rangle = \mathbb{Z}$ $\Big\}$ a generador $\Rightarrow -a$ generador

$\hookrightarrow$ para $a \neq e$

$\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$

$\langle 0 \rangle = \{\bar{0}\}$

$\langle 1 \rangle = \mathbb{Z}_8$

$\langle 2 \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$

$\langle 3 \rangle = \{\bar{0}, \bar{3}, \bar{6}, \bar{1}, \bar{4}, \bar{7}, \bar{2}, \bar{5}\} = \mathbb{Z}_8$

$\hookrightarrow$ podría haber parado acá

$\langle 4 \rangle = \{\bar{0}, \bar{4}\}$

$\langle 5 \rangle = \mathbb{Z}_8$

$\langle 6 \rangle = \{\bar{0}, \bar{6}, \bar{4}, \bar{2}\}$

$\langle 7 \rangle = \mathbb{Z}_8$

Notar que $\bar{a}$ generador de $\mathbb{Z}_m$ sii a y m coprimos

$\hookrightarrow mcd(a, m) = 1$

Lema:

- Todo subgrupo H de $(\mathbb{Z}, +)$ es cíclico
- $H = \langle 0 \rangle$ o bien $H = \langle m \rangle$ tq. m es el menor entero positivo en H

$\hookrightarrow$ en criollo, siempre elegimos el menor generador

Lema: $H_1, H_2 < G \Rightarrow H_1 \cap H_2 < G$

Lema: G grupo cíclico

$o(G) = \infty \Rightarrow G \simeq \mathbb{Z}$

$o(G) = k \Rightarrow G \simeq \mathbb{Z}_k$

Def.:

$\langle X \rangle = \{ a_1^{n_1} a_2^{n_2} \dots a_k^{n_k} : a_1, a_2, \dots, a_n \in X \}$ → ej: $\langle \{n, n+1\} \rangle = \mathbb{Z}$

↳ subgrupo de G generado por X

↳ el producto entre los subgrupos cíclicos de X (ó todos los prods. finitos de elems. de X e inversos de X)

$n + \underbrace{(-n-1)}_{(-1)(n+1)} \in \langle \{n, n+1\} \rangle$

$1 \in \langle \{n, n+1\} \rangle$

Comienza "The Twilight Zone"

Lema: sea G grupo, $\sim$ rel. eq. tq $G/\sim$ grupo (con op. inducida)

1. $H = [e] < G$

2. $\forall x, y \in G,\ x \sim y \iff x y^{-1} \in H \lor x^{-1} y \in H$

→ ¿de que me sirve?

Def.: sea G grupo, $H < G$ y $a, b \in G$

- $a \equiv_r b\,(H)$ si $ab^{-1} \in H$
- $a \equiv_l b\,(H)$ si $a^{-1} b \in H$

↳ congruente a izq. con módulo H

notar que 'mod' es un caso específico de esta

Lema: $\equiv_r(H)$ y $\equiv_l(H)$ son rel. eq. tales que

- $[a]_r = Ha = \{ha : h \in H\} = \bar{a} \in G/\equiv_r(H)$ → están implícitos, $\nexists$ coclase sin especificar el H
- $[a]_l = aH = \{ah : h \in H\} = \bar{a} \in G/\equiv_l(H)$

clase de eq. de a a izq. ↳ coclase a izquierda

Teorema: $H < G$ con $(G, *)$ grupo

sea $\underbrace{\equiv_r(H) = \equiv_l(H)}_{H \triangleleft G} \Rightarrow *$ se induce a $G/\sim \Rightarrow G/\sim$ grupo

↳ $\sim = \equiv_r(H)$ ó $\sim = \equiv_l(H)$

Teorema:

$G/\sim$ grupo con op. que se induce de G $\iff \exists\, H < G$ tq $\sim = \equiv_r(H) = \equiv_l(H)$

Definición:

$N \triangleleft G \to N < G$ y $\equiv_r(N) = \equiv_l(N)$ $\to$ ó $Na = aN \ \forall a \in G$

$G/N \to G/\sim$ con $\sim = \equiv_r(N)$ ó $\sim = \equiv_l(N)$

$\hookrightarrow G/N = \{gN : g \in G\} = \{Ng : g \in G\}$

Teorema:
sean $N < G$, son equivalentes

1. $N \triangleleft G \to N$ normal
2. $aN = Na \ \forall a \in G$
3. $aNa^{-1} \subseteq N \ \forall a \in G$

$\hookrightarrow aNa^{-1} = \{ana^{-1} : n \in N\}$

Lema:
sea $H < G$

H normal $\Longleftrightarrow [a]_r = [a]_l \ \forall a \in H$

Teorema:
sea $H < G$

1. $o([a]_r) = o([a]_l) = o(H) \to o(Ha) = o(aH) = o(H)$
2. $o(G/\equiv_r(H)) = o(G/\equiv_l(H)) \to H$ determina la misma cant. de coclases a der. y a izq.

Notación:

obs: $\bigcup_{a \in G/\equiv_l} [a]_l = \bigcup_{a \in G/\equiv_r} [a]_r = G$

$[G:H] = o(G/\equiv_r(H)) = o(G/\equiv_l(H))$

$\hookrightarrow$ índice de H en G

Teorema Lagrange:
sea $H < G \Rightarrow o(G) = [G:H]\, o(H)$ ← producto en $\mathbb{N}$

- $o(G) < \infty \Rightarrow o(a) \mid o(G) \ \forall a \in G$
- $o(G) < \infty \Rightarrow o(H) \mid o(G)$

$\hookrightarrow |H|$ divide a $|G|$

Teorema:
todo G grupo con $o(G)$ primo es cíclico y no tiene subgrupos propios

Teorema: Peq. T. de Fermat

sea p primo y $a \in \mathbb{Z} \,/\, p \nmid a \Rightarrow a^{p-1} \equiv 1\,(p)$

a no divisible por p

Corolario:

p primo y $a \in \mathbb{Z} \Rightarrow a^{p} \equiv a(p)$

Facto: "Una forma simple de hallar subgrupos normales es a través del núcleo de un homomorfismo"

Def.: Sean G y G' grupos y $f: G \to G'$

- $f(xy) = f(x)f(y) \Rightarrow f$ homomorfismo
- f homom. iny. $\Rightarrow f$ monomorfismo
- f " sobr. $\Rightarrow f$ epimorfismo
- f " biy. $\Rightarrow f$ isomorfismo

Teorema:

sean $f: G \to G'$ homom. y $\ker(f) = \{x \in G : f(x) = e_{G'}\}$

1. $\ker(f) \triangleleft G$
2. f monom. $\Leftrightarrow \ker(f) = \{e_G\}$

Teorema: 1er T. de Isomorfismo

$f: G \to H$ epimorfismo $\Rightarrow G/\ker(f)$ isomorfo a H

↳ se desprende además que cualq. subgrupo normal es núcleo de un homomorfismo y visceversa

Facto:

es un isomorfismo

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"'] & H \\ G/\ker(f) \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

π es siempre un epimorfismo

$\bar{f}([g]) = f(g)$

$\bar{f}(\pi(g)) = f(g)$

$\therefore \bar{f} \circ \pi = f$

clasificación de grupos cíclicos

Teorema: sea $f: G \to G'$ isom. de grupos
G grupo cíclico $\Rightarrow f(G)$ subgr. cíclico de G' y sus generadores son las imágenes de los generadores de G

Corolario: $f: G \to G'$ isom. grupos $\Rightarrow o(a) = o(f(a)) \ \forall a \in G$

Teorema: G grupo cíclico
1. $o(G) = \infty \Rightarrow G \simeq (\mathbb{Z}, +)$
2. $o(G) = m \Rightarrow G \simeq (\mathbb{Z}_m, +)$ para algún m

Corolario: sea $H < G$
G cíclico $\Rightarrow H$ cíclico

Teorema: sea $G = \langle a \rangle$ grupo cíclico
1. $o(G) = \infty \Rightarrow a$ y a^{-1} son los únicos generadores de G
2. $o(G) = m \Rightarrow a^k$ generador de $G \Leftrightarrow (k:m) = 1$

Corolario: sea G grupo cíclico
$o(G) = p$ con p primo $\Rightarrow G$ no tiene subgrupos propios

Teorema: sea G grupo y $a \in G$
1. $o(a) = \infty \Leftrightarrow (a^k = e \Leftrightarrow k = 0)$, luego a^k son $\neq$ para $k \neq$
2. $o(a) \neq \infty \Leftrightarrow \exists m \in \mathbb{N}$ tq $a^m = e$, luego $o(a) = \min\{k \in \mathbb{N} : a^k = e\}$ y $a^r = a^s \Leftrightarrow r \equiv s(m)$

T. Chino del resto + Alg. Euclides

$$S = \begin{cases} x \equiv a_1 (m_1) \\ x \equiv a_2 (m_2) \\ x \equiv a_3 (m_3) \end{cases}$$

1. Verificar que los m_i sean coprimos.
   Si no lo son, verificar par a par que:
   $a_1 \equiv a_2 (mcd(m_1, m_2)) \rightarrow$ para $a_1 > a_2$

2. Separar sistema en partes
   $$S_1 = \begin{cases} x \equiv a_1 (m_1) \\ x \equiv 0 (m_2) \\ x \equiv 0 (m_3) \end{cases}$$

3. Resolver subsistemas con Alg. Euc.
   1. $m' = m_2 . m_3$
      busco v' / $m'v' \equiv 1 (m_1)$
   2. Alg. Euc. para $mcd(m', m_1) \rightarrow$ Sea $m' > m_1$
      $m' = \smile . m_1 + \smile$
      $= \dots$
      $= \smile . \smile + 1$ //
      reemplazar buscando
      $1 = \underbrace{\smile}_{v'} . m' \pm \smile . m_1$
   3. $x_1 = a_1 . v' . m'$

4. $\tilde{x} = x_1 + x_2 + x_3$

5. Verificar $\tilde{x}$ en congruencias de S