Universidad de la República
Facultad de Ciencias
Centro de Matemática

Grupos

Notas adaptadas por Mariana Haim para el curso "Anillos y Módulos" 2021.

0.1. Generalidades

Definición 0.1.1 (Grupo)**.** Un *grupo* es una terna $(G, *, e)$, donde

- G es un conjunto,
- $* : G \times G \to G$ es una función
- $e \in G$

tal que se verifica:

(G1) $a * (b * c) = (a * b) * c \quad \forall a, b, c \in G$,

(G2) $a * e = e * a = a \quad \forall a \in G$,

(G3) para cada $a \in G$ existe $b \in G$ tal que $a * b = b * a = e$.

La función $*$ se dice la *operación* del grupo y el elemento e se dice *elemento neutro*, en virtud de la propiedad $(G2)$ (ver proposición 0.1.1.1).

La propiedad $(G1)$ se conoce como *asociatividad* del grupo y el elemento b que verifica $(G3)$ se dice *inverso*, a veces *opuesto* de a (ver proposición 0.1.1.2).

Una terna $(G, *, e)$ que verifica las propiedades $(G1)$ y $(G2)$ se dice *monoide*.

Cuando la operación y el neutro se sobreentienden, notamos el grupo o monoide G en lugar de $(G, *, e)$.

Muchas de las propiedades que probaremos para grupos valen también en el contexto de monoides, pero no es de interés para este curso generalizar la teoría a este nivel. La noción de monoide fue presentada porque nos será de utilidad en el capítulo siguiente.

Ejemplos 0.1.1 (Grupos)**.**

1. Los enteros con la suma $(\mathbb{Z}, +, 0)$.
2. Los racionales no nulos con el producto $(\mathbb{Q}^*, \cdot, 1)$.
3. Las matrices cuadradas invertibles con coeficientes reales con el producto $(\mathrm{GL}_n(\mathbb{R}), \cdot, I_n)$.
4. Las funciones biyectivas de un conjunto en sí mismo con la composición $(\mathrm{Biy}(A), \circ, \mathrm{Id}_A)$.

Proposición-Definición 0.1.1.

1. **Unicidad del neutro:** Si $e' \in G$ verifica $e' * a = a * e' = a$, entonces $e = e'$.
2. **Unicidad del inverso de un elemento dado:** Dados $a, b, c \in G$, si tenemos $a * b = b * a = e$ y $a * c = c * a = e$, entonces $b = c$. Esto nos permite notar a^{-1} al (único) inverso de a.
3. **Propiedad cancelativa:** Dados $a, b, c \in G$ si $a * b = a * c$ entonces $b = c$.

Demostración. 1. Si $e' * a = a$, por $(G2)$ se tiene $e' * a = e * a$ y para $b \in G$ se tiene $(e' * a) * b = (e * a) * b$. Aplicando $(G1)$ se deduce $e' * (a * b) = e * (a * b)$. Tomando b como en $(G3)$ obtenemos $e' * e = e * e$ de donde $e' = e$ por $(G2)$.

2. Es claro poniendo $b = b * e = b * (a * c) = (b * a) * c = e * c = c$ (a partir de ahora queda como ejercicio para el lector verificar qué axiomas o propiedades de los grupos se usan en cada paso de las demostraciones).

3. Se deduce como sigue:

$$b = e * b = (-a * a) * b = -a * (a * b) = -a * (a * c) = (-a * a) * c = e * c = c$$

□

Definición 0.1.2 (Subgrupo)**.** Un subconjunto $H \subseteq G$ se dice *subgrupo* de G si

- $a * b \in H \quad \forall a, b \in H$,
- $0 \in H$,
- $-a \in H \quad \forall a \in H$.

Si H es un subgrupo de G notamos $H \leqslant G$.

Definición 0.1.3 (Submonoide)**.** Si G es un monoide y H es un subconjunto de G. Decimos que H es un submonoide si verifica las primeras dos condiciones de la definición anterior.

Observación 0.1.1. Todo subgrupo es un grupo.
Todo submonoide es un monoide.

Ejemplos 0.1.2 (Subgrupos)**.** 1. Si tomamos el grupo de los complejos con la suma usual $(\mathbb{C}, +, 0)$, tenemos:

$$\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C}$$

y para todo $n \in \mathbb{N}$, $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\} \leqslant Z$.

2. Además $0 := \{e\} \leqslant G$ y $G \leqslant G$. Decimos que 0 y G son los subgrupos triviales de G.

En la siguiente proposición, presentamos dos construcciones clásicas de la Teoría de Grupos.

Proposición 0.1.1. *1. Sea G un grupo. Si H y K son subgrupos de G entonces también lo es $H \cap K$.*

2. Si H, K son grupos, el producto cartesiano $H \times K$ tiene estructura de grupo definiendo $(h, k) * (h', k') := (h * h', k * k')$.
Notamos $H \times K := (H \times K, *, (e, e))$ y lo llamamos producto directo *de H y K.*

Demostración. A cargo del lector. □

0.2. Grupos abelianos

En este curso trabajaremos únicamente con grupos cuya operación es conmutativa, reciben el nombre de Grupos Abelianos.

Definición 0.2.1 (Grupo abeliano)**.** Un grupo $(G, +, 0)$ se dice *abeliano* si se verifica:

(G4) $a + b = b + a \quad \forall a, b \in G.$

La propiedad (G4) se conoce como *conmutatividad*.

En el caso abeliano, la operación suele notarse + y llamarse *suma* del grupo. Además el neutro suele notarse 0, y el inverso de $a \in G$ suele llamarse *opuesto* y notarse $-a$.

Observaciones 0.2.1.

1. Los grupos de los ejemplos 0.1.1.1 y 0.1.1.2 son abelianos. Los de los ejemplos 0.1.1.3 y 0.1.1.4 no lo son.
2. Todo subgrupo de un grupo abeliano es un grupo abeliano.

Proposición 0.2.1 (Suma de subgrupos)**.** *Si H y K son subgrupos de G y G es abeliano, entonces:*

- $H + K := \{h + k \mid h \in H, k \in K\}$ *es un subgrupo de G.*
- *Son equivalentes:*

  (i) $H \cap K = \{0\}$,

  (ii) Si $h, h' \in H, k, k' \in K$ *son tales que* $h + k = h' + k'$ *entonces* $h = h', k = k'$.

  En este caso se dice que la suma de H y K es directa *y se nota $H \oplus K$ en lugar de $H + K$.*

Demostración.

- Tenemos que $0 = 0 + 0 \in H + K$. Si $h + k, h' + k' \in H + K$, se tiene:

$$\begin{aligned}(h + k) - (h' + k') &= h + (k - h') - k' \\ &= h + (-h' + k) - k' \\ &= h - h' + k - k' \\ &= (h - h') + (k - k') \in H + K\end{aligned}$$

- Si $h + k = h' + k'$, entonces $h - h' = k' - k \in H \cap K = \{0\}$. Por lo tanto $h - h' = 0$ y $k - k' = 0$, de donde $h = h'$, $k = k'$.

  Recíprocamente, sea $g \in H \cap K$. Como $g, 0 \in H$, $0, g \in K$ cumplen $g + 0 = 0 + g$ se deduce que $g = 0$. □

0.3. Morfismos de grupos

En esta sección nos referimos a grupos generales (no necesariamente abelianos) pero mantenemos la notación utilizada en el contexto abeliano.

Definición 0.3.1 (Morfismo de grupos)**.** Sean $(A, *, 0_A)$ y $(B, *, 0_B)$ grupos y $f : A \to B$ una función. Decimos que f es un *morfismo de grupos*, si:

$$f(x * y) = f(x) * f(y) \quad \forall x, y \in A$$

Proposición 0.3.1. *Sea $f : A \to B$ morfismo de grupos.*

1. $f(0_A) = 0_B$,
2. $f(-x) = -f(x)\ \ \forall x \in A$,

Demostración. A cargo del lector. □

Para $X \subseteq A, Y \subseteq B$ y $f : A \to B$ una función, recordamos que

$$f(X) = \{f(x) \mid x \in X\}, \qquad f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}.$$

Proposición 0.3.2. *1. Si $f : A \to B$ y $g : B \to C$ son morfismos de grupos, entonces $g \circ f : A \to C$ es morfismo de grupos.*

2. *Si A es un grupo, entonces $\mathrm{id}_A : A \to A$ es un morfismo de grupos.*
3. *Sea $f : A \to B$ morfismo de grupos.*
   Si $K \leqslant A$, entonces $f(K) \leqslant B$. Si $H \leqslant B$, entonces $f^{-1}(H) \leqslant A$.

Demostración. A cargo del lector. □

Recordamos que todo grupo tiene como subgrupo al conjunto formado únicamente por el elemento neutro. Dicho subgrupo lo notamos siembre 0.

Definición 0.3.2 (Núcleo e imagen)**.** Sea $f : A \to B$ morfismo de grupos. El *núcleo* y la *imagen* de f son respectivamente:

$$\mathrm{Ker}(f) = \{a \in A \mid f(a) = e_B\}, \qquad \mathrm{Im}\,(f) = \{b \in B \mid \exists a \in A : f(a) = b\}.$$

Proposición 0.3.3. *1.* $\mathrm{Ker}(f) \leqslant A, \mathrm{Im}\,(f) \leqslant B$.

2. *f es inyectiva si y sólo si* $\mathrm{Ker}(f) = 0$, *f es sobreyectiva si y sólo si* $\mathrm{Im}\,(f) = B$.
3. *La función $O : A \to B$ definida por $O(x) = e_B, \forall x \in B$ es un morfismo de grupos con núcleo A e imagen el grupo* 0.

Dem. A cargo del lector.

Definición 0.3.3. Un morfismo de grupos inyectivo se dice *monomorfismo de grupos.*

Un morfismo de grupos sobreyectivo se dice *epimorfismo de grupos.*

Un morfismo de grupos biyectivo se dice *isomorfismo de grupos.* Además si existe un isomorfismo de grupos $f : A \to B$ decimos que A y B son grupos *isomorfos* (o *isomorfos via f* si queremos explicitar el isomorfismo) y notamos $A \cong B$ (o $A \cong_f B$).

Un morfismo $G \to G$ se dice *endomorfismo* de G.

Un isomorfismo $G \to G$ se dice *automorfismo* de G.

Proposición 0.3.4. *1. Si $f : A \to B$ es un isomorfismo de grupos, entonces $f^{-1} : B \to A$ es un (iso)morfismo de grupos.*

2. *Si G es un grupo, entonces $Aut(G) = \{f : G \to G \mid f$ es isomorfismo$\}$ es un grupo con la composición.*

Demostración. A cargo del lector. □

Lema 0.3.5. *Sea $(G, +, 0)$ un grupo abeliano y $H, K \leqslant G$. Sea además $f : H \times K \to H + K$ definida por $f(h, k) = h + k$. Entonces:*

- *f es un epimorfismo de grupos,*
- *f es un isomorfismo si y sólo si $H \cap K = \{0\}$.*

Demostración. Es fácil ver que f es epimorfismo de grupos.

Supongamos ahora que $H \cap K = \{0\}$. Veamos que $\operatorname{Ker} f = \{0\}$: $f(h,k) = 0$ implica $h = -k \in H \cap K$ y por tanto $h = k = 0$.

Recíprocamente, si f es inyectiva, tomemos $x \in H \cap K$. Como $f(x,-x) = x - x = 0$ se tiene $(x,-x) = (0,0)$ y por tanto $x = 0$. □

Observación 0.3.1. La segunda afirmación puede expresarse como sigue: si H y K son subgrupos de un grupo abeliano G cuya suma es directa, entonces se tiene

$$H \times K \cong H \oplus K.$$

Por esta razón estos grupos suelen llamarse en el caso abeliano *suma directa externa* de H y K y *suma directa interna* de H y K respectivamente, o solamente *suma directa* de H y K si no interesa la distinción.

0.4. Grupo cociente

Proposición-Definición 0.4.1 (Congruencia)**.** Sean A un grupo y $H \leqslant A$. La relación en A definida por:

$$a \equiv_H b \Leftrightarrow a - b \in H \quad (a, b \in A)$$

es una relación de equivalencia, que llamamos relación de *conAruencia módulo H*.

Demostración. Es reflexiva porque $0 \in H$, es simétrica porque H es cerrado por opuestos y es transitiva porque H es cerrado por la suma. □

Proposición-Definición 0.4.2. Sea A un grupo abeliano y $H \leqslant A$. Notemos $\overline{a}$ a la clase de equivalencia de $a \in A$.

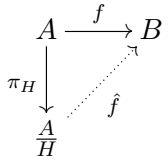
1. Si $a \equiv_H a'$ y $b \equiv_H b'$, entonces $a + b \equiv_H a' + b'$.
2. Si definimos
$$+ : A/_{\equiv_H} \times A/_{\equiv_H} \to A/_{\equiv_H}$$
mediante $\overline{a} + \overline{b} = \overline{a+b}$, entonces $(A/_{\equiv_H}, +, \overline{0})$ es un grupo que llamamos *grupo cociente* de A por H y notamos $\frac{A}{H}$.
3. La función $\pi_H : A \to \frac{A}{H}$ definida por $\pi_H(x) = \overline{x}, \forall x \in A$ es un epimorfismo de grupos que llamamos *proyección canónica* de A en el cociente $\frac{A}{H}$.

Demostración.
1. En efecto, $(a+b)-(a'+b') = (a-a')+(b-b') \in H$ porque $a-a', b-b' \in H$ (observar que se usa fuertemente la conmutatividad en A).
2. Por la parte anterior, tiene sentido la definición. Es fácil ver que esta nueva operación "hereda" las propiedades de A, en otras palabras: de la asociatividad de la operación de A se deduce la asociatividad de esta nueva operación; de la conmutatividad se deduce la nueva conmutatividad, el nuevo neutro es $\overline{0}$ y $-\overline{a} = \overline{-a}$, $\forall a \in A$.
3. A carAo del lector. □

Observación 0.4.1. Observar que $\overline{0} = \{x \in A \mid x - 0 \in H\} = H$ y que

$$\frac{A}{\{0\}} \cong A; \quad \frac{A}{A} = \{0\}.$$

Teorema 0.4.1 (Propiedad Universal del Cociente)**.** *Sea $f : A \to B$ un morfismo de grupos. Si A es abeliano y $H \leqslant \operatorname{Ker} f$, existe un único morfismo $\hat{f} : \frac{A}{H} \to B$ que hace conmutar el siguiente diagrama:*



Además, se tiene $\operatorname{Im} \hat{f} = \operatorname{Im} f$ *y* $\operatorname{Ker} \hat{f} = \frac{\operatorname{Ker} f}{H}$.

Demostración. Para que el diagrama conmute, es necesario que $\hat{f}(\overline{a}) = f(a)$, lo que prueba la unicidad.

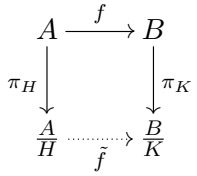
Para la existencia, veamos que tiene sentido definir $\hat{f}(\overline{a}) := f(a)$: en efecto, si $a \equiv a'$, entonces $a - a' \in H \subseteq \operatorname{Ker} f$ y por tanto $f(a) - f(a') = f(a - a') = 0$. Queda a cargo del lector verificar que la función $\hat{f}$ así definida es un morfismo de grupos.

Es claro que las imágenes de f y $\hat{f}$ coinciden. Por otro lado como $H \subseteq \operatorname{Ker} f$ tiene sentido considerar el grupo $\frac{\operatorname{Ker} f}{H}$. Además:

$$\overline{a} \in \frac{\operatorname{Ker} f}{H} \iff a \in \operatorname{Ker} f \iff f(a) = 0 \iff \hat{f}(\overline{a}) = 0 \iff \overline{a} \in \operatorname{Ker} \hat{f} \qquad \square$$

Corolario 0.4.2 (Teoremas de isomorfismo)**.** *Sea A un grupo abeliano.*

1. *Si $f : A \to B$ es un morfismo de grupos, entonces $\frac{A}{\operatorname{Ker} f} \cong \operatorname{Im} f$.*
2. *Si $H, K \leqslant A$ entonces $\frac{H+K}{H} \cong \frac{K}{H \cap K}$.*
3. *Si $H \leqslant K \leqslant A$ entonces $\frac{A/H}{K/H} \cong \frac{A}{K}$.*
4. *Si $f : A \to B$ es un morfismo de grupos, con B también abeliano, y $H \leqslant A, K \leqslant B$ con $f(H) \subseteq K$, entonces existe un único morfismo $\tilde{f} : \frac{A}{H} \to \frac{B}{K}$ que hace conmutar el siguiente diagrama:*



Demostración.

1. En el contexto del teorema anterior, se deduce que $\hat{f} : \frac{A}{\operatorname{Ker} f} \to B$ es morfismo de grupos con $\operatorname{Im} \hat{f} = \operatorname{Im} f$ y $\operatorname{Ker} \hat{f} = \frac{\operatorname{Ker} f}{\operatorname{Ker} f} = 0$, por lo que $\hat{f} : \frac{A}{\operatorname{Ker} f} \to \operatorname{Im} f$ es un isomorfismo.

2. Sea $f : K \to \frac{H+K}{H}$ definida por $f(k) = \overline{k}$. Es claro que f es un morfismo de grupos. Además si $\overline{h+k} \in \frac{H+K}{H}$ entonces $\overline{h+k} = \overline{k} = f(k)$ por lo que $\operatorname{Im} f = \frac{H+K}{H}$. Por otra parte $f(k) = 0$ si y sólo si $k \in H$ de donde $\operatorname{Ker} f = H \cap K$. Usando la parte anterior, se deduce la tesis.

3. Consideremos $\pi_H : A \to \frac{A}{H}$ la proyección canónica. Es claro que $\pi_H(K) = \frac{K}{H}$ por lo que aplicando la parte 4 se tiene que π_H induce un morfismo $\tilde{\pi_H} : A/K \to \frac{A/H}{K/H}$ que verifica $\tilde{\pi_H}([a]_K) = \overline{[a]_H}$, donde $[a]_H$ denota la clase de equivalencia de $a \in A$ según la congruencia módulo H y $\overline{x}$ denota la clase de equivalencia de $x \in A/H$ módulo K/H. Queda a cargo del lector verificar que $\tilde{\pi_H}$ es efectivamente un isomorfismo.

4. A cargo del lector. □

Teorema 0.4.3. *Sea G un grupo abeliano y $H \leqslant G$. Existe una correspondencia biyectiva entre los conjuntos:*

$$\mathcal{F}_1 = \left\{ L \leqslant \frac{G}{H} \right\} \quad y \quad \mathcal{F}_2 = \{K \leqslant G \mid K \supseteq H\}$$

que preserva la inclusión.

Demostración. Sean $\Lambda : \mathcal{F}_2 \to \mathcal{F}_1$ definida como $\Lambda(K) = \frac{K}{H}$ y $\Omega : \mathcal{F}_1 \to \mathcal{F}_2$ definida como $\Omega(L) = \pi_H^{-1}(L)$.

Observar primero que $\Lambda(K) = \frac{K}{H} = \pi_H(K)$ es un subgrupo de $\frac{G}{H}$ y que $\Omega(L) \supseteq \pi_H^{-1}(\{0\}) = H$.

Queda para el lector verificar que estas funciones son inversas entre sí.

Por otra parte, es claro que si $L \subseteq L'$ entonces $\Lambda(L) = \pi_H(L) \subseteq \pi_H(L') = \Lambda(L')$. □