UNIVERSIDAD DE MURCIA

Samuel Fernández Riquelme
7 de noviembre de 2025

# Grupos y Anillos

*– Alto, policía, ha cometido usted un crimen.*
*– Lo asumo.*
*– Lo arresto.*

## Índice

# 1. Anillos

Caulquiera podrá interpretar el propósito de esta sección a partir del encabezado. Se redactaran solo aquellos ejercicios que susciten un interés especial (bajo mi criterio).

**1.1.7** *Demostrar que si $(X, *)$ es un monoide finito y $x \in X$ entonces las siguientes condiciones son equivalentes:*

*(i)* *$x$ es cancelable por un lado.*

*(ii)* *$x$ es cancelable.*

*(iii)* *$x$ tiene simétrico por un lado.*

*(iv)* *$x$ es simétrico.*

DEMOSTRACIÓN: El flujo de la prueba va a ser el siguiente: suponer $x$ cancelable por la izquierda y concluir que $x$ tiene simétrico por la derecha, para deducir, seguidamente, que $x$ es cancelable por la derecha. Queda a las necesidades de cada uno convencerse de la suficiencia de este argumento.

Supongamos $x$ cancelable por la izquierda y definamos la aplicación $f : X \to X$ dada por

$$f(a) = x * a.$$

Bajo éstas hipótesis, $f$ es biyectiva. En efecto, para probar la inyectividad aplicamos el ser $x$ cancelable y llegamos a que

$$f(a) = f(a') \Rightarrow x * a = x * a' \Rightarrow a = a'.$$

Más aún, gracias a un resultado del ejercicio 1.1.2, como $X$ es un conjunto finito $f$ es además sobreyectiva (o, si me permites, biyectiva). En consecuencia, para $e$ el nuetro de $X$, existe $a \in X$ cumpliendo $f(a) = e$, por lo que, en definitiva, nos queda

$$x * a = f(a) = e,$$

es decir, $x$ tiene simétrico por la derecha.

Siguiendo esta línea, veamos que $x$ es cancelable por la derecha, suponiendo para ello $y, z \in X$ arbitrarios tales que $y * x = z * x$. El único paso restante es comprobar que

$$y = y * e = y * x * a = z * x * a = z * e = z.$$

Q.E.D.

**1.1.8** *Sea $*$ una operación en un conjunto $X$ y supongamos que $*$ tiene un neutro y tres elementos $a, b, c$ tales que $a \neq c$, $b$ es el simétrico por la izquierda de $a$ y $c$ es el simétrico por la izquierda de $b$. Demostrar que $*$ no es asociativa.*

DEMOSTRACIÓN: Es un razonamiento directo, únicamente es necesario examinar la expresión $c * b * a$:

$$(c * b) * a = e * a = a \neq c = c * e = c * (b * a).$$

Q.E.D.

*Concluir que si $(M, *)$ es un monoide en el que todo elemento tiene simétrico por la izquierda, entonces $(M, *)$ es un grupo.*

DEMOSTRACIÓN: Sea $a \in M$ arbitrario. Por hipótesis, $a$ tiene simétrico por la izquierda, digámosle $b$, y este, a su vez, tiene también simétrico por la izquierda $c$. No obstante, como $*$ es asociativa, para no llegar a contradicción al aplicar el resultado anterior, se debe dar $a = c$. En consecuencia, para terminar, nos queda que

$$\begin{aligned} a * b &= c * b = e, \\ b * a &= e, \end{aligned}$$

por lo que $a$ es invertible. Q.E.D.

**1.2.2** *Sea $m \in \mathbb{Z}$. Demostrar que si $m$ no es cuadrado en $\mathbb{Z}$, entonces tampoco es un cuadrado en $\mathbb{Q}$.*

DEMOSTRACIÓN: Nos ocuparemos, en su lugar, de probar el contrarrecíproco de la proposición del enunciado. Suponemos $m = q^2$ donde $q = a/b \in \mathbb{Q}, a, b \in \mathbb{Z}, b > 0$ y $\text{mcd}(a, b) = 1$. En consecuencia, deducimos que

$$m = \frac{a^2}{b^2},$$

y al despejar $a^2 = b^2 m$ notamos que

$$a^2 = b(bm) \Longrightarrow b \mid a^2,$$

donde invocamos el Lema de Euclides para obtener $b \mid a$. No obstante, como $a$ y $b$ eran coprimos, la única causa justificada es que $b = 1$, por lo que concluimos finalmente que $m = a^2$. Q.E.D.

**1.3.2** *Decimos que un entero $d$ es* libre de cuadrados *si $p^2$ no divide a $d$ para ningún número primo $p$ (en particular, 1 es libre de cuadrados). Demostrar que para todo $m \in \mathbb{Z}$ existe un $d \in \mathbb{Z}$ libre de cuadrados tal que $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{d}]$.*

DEMOSTRACIÓN: Iniciamos la demostración factorizando $m = up_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, donde $u \in \{-1, 1\}$, y definiendo, a continuación, los números

$$n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}, \quad d = up_1^{a_1 - 2b_1} p_2^{a_2 - 2b_2} \cdots p_k^{a_k - 2b_k}, \quad \text{con } b_i = \left\lfloor \frac{a_i}{2} \right\rfloor.$$

Por una parte, es inmediato notar que $m = n^2 d$ y, por otra parte, el método de construcción nos asegura que $0 \leq a_i - 2b_i \leq 1$, para cada $1 \leq i \leq k$, con lo que deducimos que $d$ es libre de cuadrados.

Habiendo definido estos números auxiliares, notamos que para cada $a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ se cumple

$$a + b\sqrt{m} = a + b\sqrt{n^2 d} = a + bn\sqrt{d} \in \mathbb{Q}[\sqrt{d}],$$

con lo que inferimos que $\mathbb{Q}[\sqrt{m}] \subseteq \mathbb{Q}[\sqrt{d}]$. Recíprocamente, si $a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, entonces

$$a + b\sqrt{d} = a + \frac{b}{n} n\sqrt{d} = a + \frac{b}{n}\sqrt{m} \in \mathbb{Q}[\sqrt{m}],$$

deduciendo finalmente que $\mathbb{Q}[\sqrt{m}] = \mathbb{Q}[\sqrt{d}]$. Q.E.D.

*¿Ocurre lo mismo si cambiamos $\mathbb{Q}$ por $\mathbb{Z}$?*

SOLUCIÓN: Tomando $m = 12$ se puede comprobar que $\mathbb{Z}[\sqrt{d}] \not\subseteq \mathbb{Z}[\sqrt{12}]$, para todo $d$ libre de cuadrados. □

**1.7.1** *Sea $a \in \mathbb{R}$. ¿Qué se deduce al aplicar el Primer Teorema de Isomorfía al homomorfismo $\mathbb{R}[X] \to \mathbb{R}$, dado por $P(X) \mapsto P(a)$? ¿Y qué se deduce al aplicarlo al homomorfismo $\mathbb{R}[X] \to \mathbb{C}$, dado por $P(X) \mapsto P(i)$?*

SOLUCIÓN: La respuesta a la primera pregunta se resume en una aplicación directa que no requiere ninguna ingeniosidad. En cambio, el segundo interrogante encierra un gran enigma. Por ello, como resolver misterios es lo único que aviva nuestro alma, vamos a darle unas reflexiones.

En primer lugar, vamos a verificar que dicho homomorfismo es suryectivo. Con tal fin, dotémosle de un nombre más manejable; pudiera ser $f$. Este paso es bastante elemental, pues para cualquier $z = a + ib \in \mathbb{C}, a, b \in \mathbb{R}$ es evidente que

$$f(a + bX) = z,$$

donde $a + bX \in \mathbb{R}[X]$ sin ninguna clase de dubitacón.

El siguiente y último paso se basa en comprobar que $\mathrm{Ker} f = \langle X^2 + 1 \rangle$. Para ello notamos que, dado $P(X) \in \mathbb{R}[X]$, se tiene[1]

$$f(P(X)) = 0 \iff P(i) = 0 \iff (X - i) \mid P(X),$$

y por ser todos los coeficientes reales

$$(X - i) \mid P(X) \iff (X + i) \mid P(X).$$

Esta secuencia de equivalencias se puede sintetizar como $f(P(X)) = 0$ si y solo si[2] $P(X) \in \langle X - i \rangle \cap \langle X + i \rangle$ y $P(X) \in \mathbb{R}[X]$, considerando tanto $\langle X - i \rangle$ como $\langle X + i \rangle$ ideales de $\mathbb{C}[X]$. Es más, el estudiante aventurero puede convencerse de que $\langle X - i \rangle + \langle X + i \rangle = \langle 1 \rangle$, por lo que, invocando el Teorema Chino de los Restos, extraemos que $\langle X - i \rangle \cap \langle X + i \rangle = \langle X - i \rangle \langle X + i \rangle = \langle X^2 + 1 \rangle$.

Concluimos de esta manera que $\mathrm{Ker} f = \mathbb{R}[X] \cap \langle X^2 + 1 \rangle$ ideal de $\mathbb{R}[X]$, por lo que abusaremos un poco de la notación y diremos que $\mathrm{Ker} f = \langle X^2 + 1 \rangle$. Para terminar, aplicamos ahora sí el Primer Teorema de Isomorfía y concluimos que

$$\frac{\mathbb{R}[X]}{\langle X^2 + 1 \rangle} \simeq \mathbb{C}.$$

□

**1.7.2** *Demostrar el recíproco del Teorema Chino de los Restos para anillos; es decir, probar que si $I_1, ..., I_n$ son ideales de un anillo $A$ tales que la aplicación $f : A \to \prod_{i=1}^{n} A/I_i$, dada por $f(a) = (a + I_1, ..., a + I_n)$ es suprayectiva, entonces $I_i + I_j = (1)$, para todo $i \neq j$.*

DEMOSTRACIÓN: Es suficiente con probar que, dados $i < j$, se cumple $1 \in I_i + I_j$. En efecto, sean $1 \leq i < j \leq n$ arbitrarios. En consecuencia, por ser $f$ suprayectiva, existe $a \in A$ satisfaciendo

$$f(a) = (0 + I_1, ..., 0 + I_i, ..., 1 + I_j, ..., 0 + I_n),$$

deduciendo, en particular, que $a + I_i = 0 + I_i$ y $a + I_j = 1 + I_j$ o, dicho de otra manera, $a \in I_i$ y $1 - a \in I_j$. Para dar término a la demostración, inferimos que

$$1 = a + (1 - a) \in I_i + I_j.$$

Q.E.D.

[1] El lector debe hacerse a la idea que se trata de divisibilidad de polinomios en el contexto de $\mathbb{C}$.
[2] O, más llanamente, $f(P(X)) = 0 \iff P(X) \in \mathbb{R}[X] \cap \langle X - i \rangle \cap \langle X + i \rangle$.

**2.1.9** *Demostrar que las siguientes condiciones son equivalentes para un anillo $A$.*

*(1) $A$ tiene un único ideal maximal.*

*(2) $A$ tiene un ideal propio $I$ que contiene todos los elementos no invertibles de $A$.*

*(3) El conjunto de los elementos invertibles de $A$ es un ideal.*

*(4) Para todo $a, b \in A$, si $a + b$ es invertible, entonces $a$ ó $b$ es invertible.*

Demostración: (1) $\Rightarrow$ (2). Llamemos $I$ al único ideal maximal de $A$. En consecuencia, para cada $a \in A$ no invertible arbitrario, el ideal propio $(a)$ está contenido en un ideal maximal (por Proposición 2.8) que, por unicidad, no puede ser otro distinto de $I$. De esta manera, deducimos que $(a) \subseteq I$ y, en particular, $a \in I$.

(2) $\Rightarrow$ (3). Denotemos $J = \{a \in A : a \text{ no es invertible}\} \subseteq I$ el conjunto de los elementos no invertibles de $A$, donde $I$ es un ideal propio. Veamos que $J$ se trata de un ideal. En efecto, el producto por un elemento general se comprueba de manera *nonchalant*. Por otra parte, para la suma interna, dados $x, y \in J$, sabemos que $x, y \in I$ y, por ser este ideal, la suma $x + y \in I$, pero como $I$ es propio $x + y$ no puede ser invertible, ergos, $x + y \in J$.

(3) $\Rightarrow$ (4). Consideremos $J = \{a \in A : a \text{ no es invertible}\}$ el ideal de todos elementos no invertibles de $A$. Vamos a probar el contrarrecíproco de la propiedad (4). Para ello, dados $a, b \in J$ (i.e. no invertibles), las cualidades de los ideales nos aseguran que $a + b \in J$, por lo que $a + b$ tampoco es invertible.

(4) $\Rightarrow$ (1). Por hipótesis, $I = \{a \in A : a \text{ no es invertible}\}$ es ideal de $A$ (recomendable, hilar cabos si desconfías). Para ver que es maximal, sea $J$ ideal de $A$ tal que $I \subsetneq J$. Por subsiguiente, existe $a \in J \setminus I$ cumpliendo, por definición, que $a$ es invertible, por lo que se debe dar $J = (a) = A$.

Al tratar la unicidad, notamos que todo ideal propio debe estar contenido[3] en $I$. Como, por definición, todo ideal $J$ maximal es propio, inferimos que $J \subseteq I$, concluyendo así final y rotundamente que $J = I$ y, por tanto, $I$ es único. Q.E.D.

**2.1.11** *Sea $A$ una anillo cuya característica es un número primo $p$. Demostrar que la aplicación $x \mapsto x^{p^n}$ es un endomorfismo de $A$ para todo $n \in \mathbb{Z}^{\geq 0}$.*

Demostración: La piedra angular de la prueba es verificar que $(x + y)^p = x^p + y^p$ y, con este objetivo en mente, nos servirá saber que, para $p$ primo y $0 < r < p$, se cumple

$$p \mid \binom{p}{r}, \tag{1}$$

propiedad que se deduce de la identidad

$$\binom{p}{r} = \frac{p}{r}\binom{p-1}{r-1}$$

al seguir la cadena de implicaciones lógicas

$$\binom{p}{r} = \frac{p}{r}\binom{p-1}{r-1} \Rightarrow r\binom{p}{r} = p\binom{p-1}{r-1} \Rightarrow p \mid r\binom{p}{r},$$

y notar, finalmente, que $\text{mcd}(p, r) = 1$ para invocar el Lema de Euclides.

Luego de este breve preámbulo, abordamos la demostración por el método de inducción; sobre $n$ para ser precisos. Por simplicidad, denotaremos las distintas aplicaciones por $f_n : A \to A$, donde

[3] Si un ideal $J$ posee un elemento invertible, entonces $J = A$.

$f_n(x) = x^{p^n}$. El caso base $n = 0$ es de una sensillez insultante, pues se trata de la aplicación identidad (un evidente endomorfismo).

Para el paso inductivo, supongamos que $f_n$ es un endomorfismo y observemos, en primer lugar, que $f_{n+1}(x) = x^{p^{n+1}} = (x^{p^n})^p = (f_1 \circ f_n)(x)$. En consecuencia, inferimos que $f_{n+1} = f_1 \circ f_n$, por lo que es suficiente con probar que $f_1$ es endomorfismo. Cotejar la conservación del producto y de la unidad se deja como desafío elemental para el lector. En cuanto a la suma, nos valemos del consagrado Binomio de Newton[4] para desarrollar

$$f_1(x+y) = (x+y)^p = \sum_{r=0}^{p} \binom{p}{r} x^{p-r} y^r = x^p + y^p + \sum_{r=1}^{p-1} \binom{p}{r} x^{p-r} y^r,$$

y, a continuación, aplicamos (1), unido al hecho de que $p$ es la característica de $A$, para llegar a que

$$x^p + y^p + \sum_{r=1}^{p-1} \binom{p}{r} x^{p-r} y^r = x^p + y^p = f_1(x) + f_1(y).$$

Habiendo probado que $f_1$ es endomorfismo, el resto de la demostración se sigue del principio de inducción. Q.E.D.

**2.1.12** *Demostrar que, si $K$ es un cuerpo finito con un subcuerpo $F$, entonces el cardinal de $K$ es una potencia del cardinal de $F$.*

DEMOSTRACIÓN: Consideramos $K$ como $F$ espacio vectorial y tomamos, a continuación, una base $\mathcal{B} = \{u_1, ..., u_n\}$ de $K$, cuya existencia viene asegurada por ser $K$ finitamente generado ($K =< K >$).

Con estas definiciones notamos que la aplicación $\varphi : F^n \to K$ dada por

$$\varphi(\lambda_1, ..., \lambda_n) = \lambda_1 u_1 + \cdots + \lambda_n u_n$$

es biyectiva. La sobretividad la obtenemos por ser $\mathcal{B}$ sistema generador y, por otra parte, sabemos que la independencia lineal de $\mathcal{B}$ nos da unicidad en la representación de cada elemento de $K$, por lo que $\varphi$ es inyectiva. En definitiva, deducimos que

$$|K| = |F^n| = |F|^n.$$

Q.E.D.

*Deducir que:*

*(1) El cardinal de cualquier cuerpo finito es potencia de un número primo.*

SOLUCIÓN: Dado $K$ un cuerpo finito cualquiera, vamos a examinar $F := \{n1 : n \in \mathbb{Z}\}$ el subanillo primo de $K$. Debido a que $K$ es cuerpo sabemos que, en particular, es dominio, por lo que $F$ también es dominio.

Para determinar la característica de $F$ nos percatamos de que, al ser $K$ finito, existen $n, m \in \mathbb{Z}$ distintos tales que $n1 = m1$, y al pasar restando resulta en que $(n-m)1 = 0$, para deducir inmediatamente que $\mathrm{Car}(K) = \mathrm{Car}(F) \neq 0$, pues $n - m \neq 0$. Más aún, aplicando el ejercicio 2.1.5 deducimos que $\mathrm{Car}(K) = \mathrm{Car}(F) = p$, con $p \in \mathbb{N}$ primo.

A continuación, tocaría comprobar que $|F| = \mathrm{Car}(F) = p$, pero os doy la oportunidad privilegiada de perfilar vuestro auto-entendimiento y que hagais los argumentos pertinentes.

[4]Para los escépticos, el Binomio de Newton es válido para cualquier anillo conmutativo.

(Indicación: encontrar biyección con $\mathbb{Z}_p$.) *Moving on*, si asumimos dicha afirmación como dogma, invocamos el primer resultado del ejercicio para llegar a que

$$|K| = |F|^n = p^n, \quad n \in \mathbb{N}.$$

□

*(2) Si $K$ es un cuerpo finito con un subcuerpo $F$, entonces existen un número primo $p$ y enteros positivos $n$ y $m$ tales que $n \mid m, |F| = p^n$ y $|K| = p^m$.*

SOLUCIÓN: Banal[5]. □

**2.2.7** *Sea $S = \{s_1, ..., s_n\}$ un subconjunto finito de un anillo $A$ y supongamos que para cada $i \neq j$ se verifica que $(s_i, s_j) = A$. Demostrar que $mcm(S) = \prod_{i=1}^n s_i$.*

DEMOSTRACIÓN: Como anotación inicial, aclaramos que $(s,t) = (s) + (t)$ para cualesquiera dos elementos $s, t$ de un anillo $A$. Dicho lo cual, notamos que las hipótesis descritas en el enunciado son un caso particular de las pedidas en el Teorema Chino de los Restos, por lo que invocamos dicho resultado para deducir

$$\bigcap_{i=1}^n (s_i) = \prod_{i=1}^n (s_i) = \left( \prod_{i=1}^n s_i \right),$$

donde la última igualdad se deja al cuidado del lector. Por último, en vigor del apartado (2) del ejercicio 2.2.5, concluimos que

$$\text{mcm}(S) = \prod_{i=1}^n s_i.$$

Q.E.D.

**2.3.2** *Sea $D$ un dominio y supongamos que existe un aplicación $\mu : D \to \mathbb{Z}^{\geq 0}$ que verefica las tres propiedades siguientes:*

- *$\mu(ab) = \mu(a)\mu(b)$ para cualesquiera $a, b \in D$.*
- *$\mu(a) = 0$ si y sólo si $a = 0$.*
- *$\mu(a) = 1$ si y sólo si $a$ es unidad.*

*Demostrar que si $\mu(a)$ es irreducible, entonces $a$ es irreducible en $D$.*

DEMOSTRACIÓN: Sea $a \in D$ tal que $\mu(a)$ es irreducible y supongamos que $a = bc, b, c \in D$. Por la primera propiedad de $\mu$ sabemos que

$$\mu(a) = \mu(bc) = \mu(b)\mu(c),$$

y como $\mu(a)$ es irreducible por hipótesis $\mu(b) \in \mathbb{Z}^* \vee \mu(c) \in \mathbb{Z}^*$. No obstante, como la imagen por $\mu$ es no negativa, podemos afirmar que $\mu(b) = 1 \vee \mu(c) = 1$, con lo que deducimos que $b \in D^* \vee c \in D^*$. Este razonamiento nos permite concluir que $a$ es irreducible. Q.E.D.

[5] Banach.

*Demostrar que $D$ es un dominio de factorización.*

DEMOSTRACIÓN: Abordamos la demostración por inducción completa sobre el valor de $\mu(a)$. Para el caso base, si $\mu(a) = 1$, entonces $a$ es unidad y se puede factorizar.

En cuanto al paso inductivo, dado $n \geq 1$, supongamos que $x \in D$ se puede factorizar si $1 \leq \mu(x) \leq n$ y veamos que si $\mu(a) = n + 1$ entonces $a$ también es factorizable. En efecto, sea $a \in D$ tal que $\mu(a) = n + 1$. Si $a$ fuese irreducible, ya habríamos términado, por lo que asumiremos que $a$ es reducible. Consecuentemente, existen $b, c \in D \setminus D^*$ cumpliendo $a = bc$, y al invocar la primera propiedad de $\mu$ nos queda que

$$\mu(b)\mu(c) = \mu(a) = n + 1,$$

de donde deducimos[6] que $\mu(b), \mu(c) > 1$ y, por tanto, $1 < \mu(b), \mu(c) < n+1$. En particular, tanto $b$ como $c$ satisfacen la hipótesis de inducción, por lo que son factorizables y así será $a$, pues si $b = up_1 \cdots p_k$ y $c = vq_1 \cdots q_l$ escribimos

$$a = bc = (uv)p_1 \cdots p_k q_1 \cdots q_l.$$

Q.E.D.

**2.5.4** (Del documento auxiliar.) *Sea $D$ un dominio euclídeo con función euclidea $\delta$. Probar que si $a, b \in D \setminus \{0\}$ son tales que $\delta(ab) = \delta(a)$, entonces $b$ es unidad.*

DEMOSTRACIÓN: Definamos $p = ab$ y usemos el Lema 2.28 para deducir que

$$\delta(p) = \delta(a) \leq \delta(x), \forall x \in (a) \setminus \{0\} \Longrightarrow (p) = (a),$$

por lo que $p$ y $a$ son asociados o, dicho de forma más conveniente, $p = au$ con $u \in D^*$. Rememorando la definición de $p$ inferimos que $ab = au$, para concluir $b = u \in D^*$. Q.E.D.

[6] Como $a \neq 0$ se tiene que $b, c \neq 0$ y, por otra parte, como $b$ y $c$ no son unidades, por la tercera propiedad, sus imagenes son distintas de 1.

# 2. Grupos