Problemas resueltos de Estructuras Algebraicas

Números, polinomios, anillos, ideales, grupos, subgrupos normales, homomorfismos, productos directos y semidirectos)

Yolanda Fuertes y Dragan Vukotić
(con la colaboración de Margarita Otero)

Universidad Autónoma de Madrid, 1997

(revisado y actualizado en 2024)

NÚMEROS

Problema 1 *Sea p un número primo y $a \in \mathbb{Z}$. Si a no es múltiplo de p, demuéstrese que*
(a) $a^{p^2} - a^p$ es divisible por p;
(b) Para $p > 2$, $(a+p)^p$ y a^p son congruentes módulo p^2, pero no módulo p^3. ¿Qué ocurre si $p = 2$?

SOLUCIÓN. Para dos números naturales m, n, denotemos por (m,n) su máximo común divisor. Siendo p primo, tenemos $(a,p) \in \{1,p\}$. Puesto que a no es un múltiplo de p, se sigue que $(a,p) = 1$ y, por tanto, también $(a^p,p) = 1$. Por el pequeño teorema de Fermat, concluimos que

$$(a^p)^p \equiv a^p (mod\ p)\ ;$$

es decir, $p \mid a^{p^2} - a^p$.

(b) El pequeño teorema de Fermat es inutil aquí, ya que sólo nos permite concluir que $(a+p)^p$ y a^p son congruentes módulo p y nada más. Por eso, para $p > 2$, utilizaremos la fórmula binomial de Newton:

$$\begin{aligned}(a+p)^p - a^p &= \binom{p}{1} a^{p-1}p + \binom{p}{2} a^{p-2}p^2 + \ldots + \binom{p}{3} a^{p-3}p^3 + \ldots + \binom{p}{p-1} ap^{p-1} + p^p \\ &= p^2 a^{p-1} + Np^3\ ,\end{aligned}$$

ya que el coeficiente binomial $\binom{p}{2} = p\frac{p-1}{2}$ es divisible por p, siendo éste un número natural y siendo p y 2 números coprimos (lo que implica $2 \mid (p-1)$). Los demás términos son todos obviamente divisibles por p^3, ya que $p \geq 3$.

La suma $p^2 a^{p-1} + Np^3$ es claramente divisible por p^2, pero no por p^3, ya que $(a^{p-1}, p) = 1$.

En el caso $p = 2$, el número a tiene que ser impar y, por lo tanto, tenemos $(a+p)^p - a^p = (a+2)^2 - a^2 = 4(a+1)$, que es divisible por $8 = p^3$. ■

Problema 2 *Demostrar que los polinomios $X^p + Y^p$ y $(X+Y)^p$ son iguales en el anillo de polinomios $\mathbb{Z}_p[X,Y]$ para p primo.*

SOLUCIÓN. Por un razonamiento parecido al del apartado (b) del ejercicio anterior, todos los coeficientes binomiales

$$\left(\begin{array}{c} p \\ j \end{array} \right), \quad j = 1, 2, \ldots p-1 ,$$

son divisibles por p y en $\mathbb{Z}_p$ se tiene: $\overline{np} = \overline{0}$; por consiguiente,

$$(X+Y)^p = X^p + \sum_{j=1}^{p-1} \left(\begin{array}{c} p \\ j \end{array} \right) X^j Y^{p-j} + Y^p = X^p + Y^p$$

en $\mathbb{Z}_p[X,Y]$.

¡Ojo! El grado de un polinomio no se puede reducir ni por el teorema de Fermat ni por ningún otro razonamiento. Si X es una variable, entonces $X^p \neq X$ (esto es solamente cierto para los valores de X cuando éste es un elemento de $\mathbb{Z}_p$). En estos dos casos concretos, los polinomios considerados ya no se pueden simplificar más. ■

Problema 3 *Denotemos por φ la función de Euler. Sean p, q dos primos distintos y m, n dos números naturales cualesquiera. Calcúlese el valor de $\varphi(p^m q^n)$.*

SOLUCIÓN. Recordemos que para $k \in \mathbb{N}$, $k \geq 2$, $\varphi(k)$ es el cardinal del subconjunto de $\{1, 2, \ldots, k-1\}$ formado por los números coprimos con k. También conocemos la propiedad multiplicativa de φ (vista en clase): $\varphi(kl) = \varphi(k)\varphi(l)$ para $(k,l) = 1$. Así pues,

$$\varphi(p^m q^n) = \varphi(p^m)\varphi(q^n)$$

y el problema se ha reducido a hallar $\varphi(p^m)$, el número de coprimos con p^m entre los números k tales que $1 \leq k < p^m$. Considerando el conjunto complementario (de los números que tienen algún divisor común > 1 con p), nos damos cuenta que éste consiste precisamente en los números divisibles por p y menores que $p^m = p^{m-1} \cdot p$, que son precisamente los de la forma $k \cdot p$, donde $1 \leq k < p^{m-1}$. Por lo tanto, hay precisamente $p^{m-1} - 1$ de esos, lo que implica

$$\begin{aligned} \varphi(p^m) &= |\{\text{menores que } p^m\}| - |\{\text{menores que } p^m \text{ y divisibles por } p\}| \\ &= (p^m - 1) - (p^{m-1} - 1) \\ &= p^{m-1}(p-1) . \end{aligned}$$

La respuesta final es

$$\varphi(p^m q^n) = p^{m-1}(p-1)q^{n-1}(q-1)\,.$$

■

POLINOMIOS

Problema 4 *Estudiar la reducibilidad de los siguientes polinomios:*
(a) $6X+3$ *en* $\mathbb{Q}[X]$ *y* $\mathbb{Z}[X]$.
(b) $\frac{1997}{1998}X^5 + 200X^4 - \pi X + \sqrt{3'9}$ *en* $\mathbb{R}[X]$.

SOLUCIÓN. Recordemos: un elemento es reducible si se puede escribir como producto de dos elementos de los que ninguno es una unidad (elemento invertible).

(a) Si $6X+3 = P(X)\,Q(X)$, entonces $1 = gr(6X+3) = gr(P)+gr(Q)$. Por lo tanto, $gr(P) = 1$ y $gr(Q) = 0$ ó al revés; se sigue que $6X+3 = a(bX+c)$, $a, b, c \in \mathbb{Q}$. y $a, b \neq 0$. Entonces a es invertible en $\mathbb{Q}$. Conclusion: el polinomio es irreducible en $\mathbb{Q}[X]$.

En $\mathbb{Z}[X]$ tenemos $6X+3 = 3(2X+1)$ y ninguno de los polinomios $P(X) = 3$, $Q(X) = 2X+1$ es invertible en $\mathbb{Z}[X]$ (hay que comprobarlo para el segundo de ellos, pero es fácil). Por lo tanto, $6X+3$ es reducible. ¡Ojo con estos casos!

(b) Recordemos una proposición vista en clase: un polinomio cuyos coeficientes son reales siempre tiene las raices complejas emparejadas (las "verdaderas", que no son números reales): z es una raíz si y sólo si $\overline{z}$ lo es. (Es imprescindible que los coeficientes sean reales; conviene buscar contraejemplos en el caso de algún coeficiente complejo). Pero nuestro polinomio es de grado cinco y debe tener 5 raices complejas. Por lo tanto, una de ellas seguro que es real: $a \in \mathbb{R}$ (puede ser que 3 de ellas, o las 5, sean reales.) Entonces el polinomio tiene un factor $X-a$. Despues de dividirle por éste, se obtiene otro factor con coeficientes reales, por lo cual nuestro polinomio es reducible. ■

Problema 5 *Descompóngase el polinomio* $P(X) = X^4 + 3X^2 + 4$ *en factores irreducibles en* $\mathbb{Q}[X], \mathbb{R}[X], \mathbb{C}[X]$ *y* $\mathbb{Z}_7[X]$.

SOLUCIÓN. Utilizaremos el viejo truco de representar $P(X)$ como diferencia de cuadrados:

$$P(X) = (X^4 + 4X^2 + 4) - X^2 = (X^2+2)^2 - X^2 = (X^2+2+X)(X^2+2-X)\,.$$

Esta es la descomposición en factores irreducibles en $\mathbb{Q}[X]$ y $\mathbb{R}[X]$ ya que los dos factores, siendo polinomios cuadráticos sin raices en $\mathbb{R}$, no pueden descomponerse más en ninguno de esos anillos. Por supuesto, cada uno de ellos tiene dos ceros en $\mathbb{C}$: los ceros de X^2+X+2

son $\varepsilon_{1/2} = -\frac{1}{2} \pm \frac{i\sqrt{7}}{2}$, mientras que $X^2 - X + 2$ tiene como raices $\varepsilon_{3/4} = \frac{1}{2} \pm \frac{i\sqrt{7}}{2}$. La descomposición completa es

$$P(X) = (X - \varepsilon_1)(X - \varepsilon_2)(X - \varepsilon_3)(X - \varepsilon_4) .$$

En $\mathbb{Z}_7$ el polinomio $X^2 + X + \overline{2}$ tiene un cero: $\overline{3}$, que es doble:

$$X^2 + X + \overline{2} = (X - \overline{3})(X + \overline{4}) = (X - \overline{3})^2 = (X + \overline{4})^2 ;$$

lo mismo sucede con $X^2 - X + \overline{2}$:

$$X^2 - X + \overline{2} = (X - \overline{4})(X + \overline{3}) = (X - \overline{4})^2 = (X + \overline{3})^2 .$$

Por lo tanto,

$$P(X) = (X - \overline{3})^2 (X - \overline{4})^2 = (X + \overline{4})^2 (X + \overline{3})^2 . \blacksquare$$

Problema 6 *¿Es reducible en $\mathbb{Q}[X]$ el polinomio $P(X) = X^4 - 2X^3 + 2X - 3$? Justificar la respuesta.*

SOLUCIÓN. El polinomio es primitivo, por lo cual es reducible (o irreducible) simultaneamente en $\mathbb{Q}[X]$ y $\mathbb{Z}[X]$ (por el teorema de Gauss). Estudiaremos entonces su reducibilidad en $\mathbb{Z}[X]$.

Es fácil ver que $P(X)$ no tiene ningún cero en $\mathbb{Z}$: todas las posibles raices enteras tendrían que ser divisores de 3 (que son 1, -1, 3, -3), pero ninguno de estos números es una raíz de $P(X)$. Esto, por supuesto, no implica la irreducibilidad del polinomio (puede tener factores cuadráticos), pero nos hace pensar en esa posibilidad.

Desafortunadamente, no se puede aplicar directamente el criterio de Eisenstein, a falta de un primo p conveniente (ni con $p = 2$ ni con $p = 3$ se cumplen las condiciones del teorema). No obstante, recordemos que los polinomios $P(X)$ y $P(X + 1)$ son reducibles (o irreducibles) simultaneamente (visto en clase). Por lo tanto, probaremos esta otra posibilidad, lo que nos permite cambiar los coeficientes:

$$P(X + 1) = (X + 1)^4 - 2(X + 1)^3 + 2(X + 1) - 3 = X^4 + 2X^3 - 2 .$$

A este polinomio ya podemos aplicarle Eistenstein con $p = 2$: observamos que $2 \mid 2$, $2 \mid (-2)$, pero $2^2 \not| (-2)$.

Conclusión: $P(X)$ es irreducible en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$. $\blacksquare$

Comentario: si no funcionan los razonamientos con $P(X)$, $P(X + 1)$, también se puede probar con $P(X - 1)$, $P(X + 2)$, etc., dependiendo del caso particular.

Problema 7 *(a) Estudiar la reducibilidad de* $P(X) = X^{11} - 11\,X + 45$ *en* $\mathbb{Q}[X]$.
(b) Descomponer $P(X)$ *en factores lineales en* $\mathbb{Z}_5[X]$.

SOLUCIÓN. (a) No funciona el razonamiento con $P(X+1)$, ya que el coeficiente independiente que se obtiene no es divisible por 11. Sin embargo, funciona la misma idea con $P(X-1)$:

$$P(X-1) = X^{11} - 11 \sum_{j=2}^{10} (-1)^{11-j} \left(\begin{array}{c} 11 \\ j \end{array} \right) X^j + 55\,.$$

Todos los coeficientes binomiales son divisibles por 11, siendo éste un número primo. Por el criterio de Eisenstein (con $p = 11$), los polinomios $P(X+1)$ y $P(X)$ son irreducibles.

(b) En $\mathbb{Z}_5[X]$ tenemos

$$P(X) = X^{11} - X = X\,(X^{10} - \overline{1}) = X\,(X^5 - \overline{1})\,(X^5 + \overline{1}) = X\,(X - \overline{1})^5\,(X + \overline{1})^5\,,$$

otra vez debido a la propiedad de los coeficientes binomiales y números primos. ■

Problema 8 *¿Existe algún* $a \in \mathbb{R}$ *para el cual el polinomio* $P(X) = X^5 - \frac{10a^2}{3} X^3 + 5a^4 X - 8a^3$ *tiene un cero de orden exactamente 3? Razonar la respuesta.*

SOLUCIÓN. Para que P tenga un cero triple c, el mismo número c tiene que ser un cero doble de la derivada $P'(X)$ (por un teorema visto en clase; puede verse directamente, escribiendo $P(X) = (X-c)^3 Q(X)$, donde $Q(c) \neq 0$, y considerando $P'(X) = 3(X-c)^2 Q(X) + (X-c)^3 Q'(X)$ y luego $P'(c)$). Esto nos proporciona la condición siguiente:

$$P'(X) = 5X^4 - 10a^2 X^2 + 5a^4 = 5(X^4 - 2a^2 X + a^4) = 5(X^2 - a^2)^2 = 5(X-a)^2 (X+a)^2 = 0\,.$$

Por lo tanto, hay dos posibles valores para c: $c = a$ y $c = -a$.

En el primer caso tenemos

$$0 = P(a) = \frac{8}{3} a^5 - 8a^3 = \frac{8}{3} a^3 (a^2 - 3)\,;$$

por lo tanto, $a = 0$, $a = \sqrt{3}$ ó $a = -\sqrt{3}$. En el caso $a = 0$ el polinomio $P(X)$ tendría un cero de orden 5, lo cual es imposible. Los dos casos restantes son posibles (¡comprobarlo!).

En el caso $c = -a$ tenemos

$$0 = P(-a) = -\frac{8}{3} a^5 + 8a^3 = -\frac{8}{3} a^3 (a^2 - 3)$$

y otra vez aparecen las mismas posibilidades - no hay nada nuevo que considerar.

La respuesta final es: para $a = \sqrt{3}$ el polinomio $P(X)$ tiene un cero triple $X = \sqrt{3}$, y, para el valor $a = -\sqrt{3}$, también se tiene un cero de orden tres: $X = -\sqrt{3}$. ■

Problema 9 *El criterio de reducción módulo p dice lo siguiente: si $P(X)$ es un polinomi mónico con coeficientes enteros, p es un número natural primo y $P(X)$ es irreducible en $\mathbb{Z}_p[X]$, entonces $P(X)$ es también irreducible en $\mathbb{Z}[X]$ (y, por tanto, tambieén en $\mathbb{Q}[X]$).*

(a) Demuéstrese que $X^4+5X+12$ es irreducible en $\mathbb{Q}[X]$.

(b) Utilícese el mismo polinomio del apartado (a) para comprobar que si $P(X)$ es reducible en $\mathbb{Z}_p[X]$, no se puede concluir lo mismo en $\mathbb{Z}[X]$ (es decir, el criterio de reducción módulo p nos es útil si y sólo si podemos obtener un polinomio irreducible después de la reducción). Hay que tener mucho cuidado con esto, ya que en muchos exámenes se han visto "soluciones" (incorrectas, por supuesto) de este estilo.

SOLUCIÓN. (a) Aplicaremos el criterio de reducción módulo 5 (primo). El polinomio se convierte en $X^4+\overline{2}$. Es fácil ver que éste no tiene raíces en $\mathbb{Z}_5$ y, por tanto, no puede tener factores lineales con coeficientes en $\mathbb{Z}_5$. Se deja al lector comprobar que cada una de las posibles factorizaciones

$$X^4+\overline{2}=(X^2+aX+\overline{2})(X^2+bX+\overline{1}), \qquad X^4+\overline{2}=(X^2+aX-\overline{2})(X^2+bX-\overline{1})$$

($a, b \in \mathbb{Z}_5$) nos lleva a la contradicción. Por consiguiente, el polinomio dado es irreducible en $\mathbb{Z}_5[X]$ y, por tanto, también en $\mathbb{Z}[X]$ y en $\mathbb{Q}[X]$. (Obsérvese que $\overline{2}=\overline{1}\cdot\overline{2}=(-\overline{1})\cdot(-\overline{2})$ son las únicas factorizaciones de $\overline{2}$ en $\mathbb{Z}_5$, ya que en este caso $-\overline{2}=\overline{3}$ etc.)

(b) Reduciendo módulo 3, se obtiene $X^4+\overline{2}X$, un polinomio obviamente reducible; sin embargo, el polinomio $X^4+5X+12$ es irreducible en $\mathbb{Z}[X]$ (demostrado en (a)). Ejemplos semejantes a este se pueden construir para cualquier otro primo p. ■

ANILLOS. IDEALES. CUERPOS

Problema 10 *¿Son primos o maximales en $\mathbb{Z}[X]$ los ideales $<X^2,3>$, $<X,3>$ y $<X>$? Explicar. También estudiar los cocientes $\mathbb{Z}[X]/<X^2,3>$, $\mathbb{Z}[X]/<X,3>$ y $\mathbb{Z}[X]/<X>$. Decidir si son dominios de integridad o cuerpos y si algunos de ellos pueden ser isomorfos.*

SOLUCIÓN. Primero demostraremos que el ideal $<X^2,3>$ no es primo. Para ello, observemos que $X^2-9=1\cdot X^2-3\cdot 3\in<X^2,3>$ y $X^2-9=(X-3)(X+3)$, pero que ninguno de los polinomios $X-3$, $X+3$ pertenece al ideal $<X^2,3>$ (y ninguno de ellos es una unidad del anillo $\mathbb{Z}[X]$). Por ejemplo, si $X-3$ perteneciera a $<X^2,3>$, esto implicaría $X-3=X^2P(X)+3Q(X)$ para algunos polinomios $P(X)$, $Q(X)$. Comparando los coeficientes, se puede ver facilmente que $P(X)$ tiene que ser identicamente cero, lo que nos deja con $X-3=3Q(X)$ y esto es una contradicción, ya que los coeficientes de $Q(X)$ son enteros (¡escribir todos los detalles!). Conclusión: $<X^2,3>$ no es un ideal primo y, por consiguiente, tampoco es maximal. Por un

teorema visto en clase, el anillo cociente $\mathbb{Z}[X]/<X^2,3>$ no es un dominio de integridad (por lo tanto, no es un cuerpo).

Veremos ahora que $<X,3>$ es un ideal maximal. Para ello, observemos que $<X>$ es un ideal en el anillo $<X,3>$ (que a la vez es un ideal del anillo $\mathbb{Z}[X]$). Por el Segundo Teorema de Isomorfía para los anillos, tenemos

$$\mathbb{Z}[X]/<X,3> \cong (\mathbb{Z}[X]/<X>)/(<X,3>/<X>) ;$$

pero $\mathbb{Z}[X]/<X> \cong \mathbb{Z}$ (las clases en el anillo cociente son $\overline{a_0 + a_1X + \ldots + a_nX^n} = \overline{a_0}$, ya que $\overline{X} = \overline{0}$; un isomorfismo entre $\mathbb{Z}[X]/<X>$ y $\mathbb{Z}$ viene dado por $\varphi(\overline{a_0 + a_1X + \ldots + a_nX^n}) = \varphi(\overline{a_0}) = a_0$) y $<X,3>/<X> \cong 3\mathbb{Z}$ (puesto que todos los polinomios son del anillo $\mathbb{Z}[X]$; el isomorfismo es parecido al φ anterior). Por lo tanto,

$$\mathbb{Z}[X]/<X,3> \cong \mathbb{Z}/(3\mathbb{Z}) \cong \mathbb{Z}_3$$

y éste es un cuerpo. Por lo tanto, el ideal $<X,3>$ es maximal.

Ya sabemos que $\mathbb{Z}[X]/<X> \cong \mathbb{Z}$ (dominio de integridad, pero no cuerpo) y, por tanto, $<X>$ es un ideal primo y no es maximal. También lo podíamos haber comprobado directamente: $<X> \subset <X,3>$ (si $P(X) \in <X>$, entonces $P(X) = XQ(X) = XQ(X) + 0 \cdot 3 \in <X,3>$) y $<X> \neq <X,3>$ (por ejemplo, $3 \notin <X>$), lo que nos dice que existe un ideal más grande que $<X>$. Luego $<X>$ es primo, ya que si $P(X)Q(X) = XR(X)$ con P, Q no invertibles (es decir, P, $Q \neq \pm 1$), fácilmente se deduce que $X \mid P(X)$ ó $X \mid Q(X)$.

Las propiedades "ser un dominio de integridad" y "ser un cuerpo" son preservadas por los isomorfismos de anillos. Puesto que tenemos un anillo cociente que no es un dominio de integridad (ni un cuerpo), otro que es un dominio de integridad, pero no cuerpo, y un tercero que es un cuerpo, es evidente que no puede haber dos de ellos isomorfos entre sí.

Comentario: el caso de $\mathbb{Z}[X]$ es muy distinto de $\mathbb{Q}[X]$: siendo $\mathbb{Q}$ cuerpo, todos los ideales en $\mathbb{Q}[X]$ son principales (generados por un elemento) - visto en clase. Luego, a cualquier ideal de $\mathbb{Q}[X]$ que contenga una constante, necesariamente le tiene que pertenecer el elemento 1, por lo cual el ideal es igual a $\mathbb{Q}[X]$. ■

Problema 11 *(a) ¿Son isomorfos los cuerpos $\mathbb{Q}[\sqrt{14}]$ y $\mathbb{Q}[\sqrt{15}]$? Justifíquese la respuesta.*

(b) Demúestrese que

$$I = \{14m + n\sqrt{14} : \ m, n \in \mathbb{Z},\} \subset \mathbb{Z}[\sqrt{14}]$$

es un ideal del anillo $\mathbb{Z}[\sqrt{14}]$. ¿Es principal o no? (Búsquese el razonamiento más sencillo posible.)

(c) ¿Cuántos ideales distintos tiene el anillo $\mathbb{Q}[\sqrt{14}]$?

SOLUCIÓN. (a) La respuesta es NO. Supongamos que sí. Sea $\varphi : \mathbb{Q}[\sqrt{14}] \to \mathbb{Q}[\sqrt{15}]$ un isomorfismo. Entonces sabemos que $\varphi(1) = 1$. Por lo tanto, $14 = \varphi(14) = \varphi((\sqrt{14})^2) = (\varphi(\sqrt{14}))^2$ por las propiedades básicas de isomorfismos. Sea $\varphi(\sqrt{14}) = a + b\sqrt{15}$, donde $a, b \in \mathbb{Q}$. Entonces se sigue

$$14 = (a + b\sqrt{15})^2 \Rightarrow 2ab\sqrt{15} = 14 - a^2 - 15b^2$$

y esto es imposible: si $a, b \neq 0$, entonces $\sqrt{15} \in \mathbb{Q}$ (contradicción); si $a = 0$, entonces $14 = 15b^2$, lo cual es imposible ($b \in \mathbb{Q}$), etc.

(b) Para ver que I es un ideal, hace falta comprobar que para todo $r, s \in I$ y para todo $x \in \mathbb{Z}[\sqrt{14}]$ se cumplen las condiciones $r - s \in I$ y $rx \in I$ (¡y nada más!). Luego hay que ver que está generado por un solo elemento. Hay una manera rápida de verlo todo a la vez: un elemento cualquiera de I puede escribirse de la forma siguiente:

$$14m + n\sqrt{14} = \sqrt{14}(n + m\sqrt{14}) \, .$$

Puesto que $n + m\sqrt{14}$ es un elemento típico del anillo $\mathbb{Z}[\sqrt{14}]$, se sigue que

$$I = \{\sqrt{14}a : \ a \in \mathbb{Z}[\sqrt{14}]\} = <\sqrt{14}>,$$

el ideal generado por $\sqrt{14}$. Por definición, I es un ideal principal en $\mathbb{Z}[\sqrt{14}]$.

(c) Siendo $K = \mathbb{Q}[\sqrt{14}]$ un cuerpo, tiene solamente dos ideales: $\{0\}$ y K. (Si $I \subset K$ es un ideal $\neq \{0\}$ de un cuerpo K, existe un $x \in K$, $x \neq 0$; entonces $x^{-1} \in K$ y, por lo tanto, $1 = x^{-1}x \in I$, lo que implica $I = K$.) Esto significa, por ejemplo, que el "ideal" definido por

$$I = \{14q + r\sqrt{14} : \ q, r \in \mathbb{Q}\}$$

es lo mismo que $\mathbb{Q}[\sqrt{14}]$. ■

Problema 12 *Hallar todos los posibles automorfismos del anillo $\mathbb{Z}[\sqrt{3}]$ y comprobar que lo son.*

SOLUCIÓN. Sea $\varphi : \mathbb{Q}[\sqrt{3}] \to \mathbb{Q}[\sqrt{3}]$ un automorfismo. Ya sabemos que $\varphi(1) = 1$ es cierto; aplicando esta propiedad, obtenemos $3 = \varphi(3) = \varphi((\sqrt{3})^2) = (\varphi(\sqrt{3}))^2$. Sea $\varphi(\sqrt{3}) = a + b\sqrt{3}$, donde $a, b \in \mathbb{Z}$. Entonces se sigue

$$3 = (a + b\sqrt{3})^2 \quad \Rightarrow \quad 2ab\sqrt{3} = 3 - a^2 - -3b^2 \quad \Rightarrow \quad ab = 0 \, , \quad a^2 + 3b^2 = 3 \, .$$

Puesto que la hipótesis $b = 0$ fácilmente se reduce al absurdo, se deduce que $a = 0$ y $b = \pm 1$. Por lo tanto, los únicos candidatos para ser la imagen de $\sqrt{3}$ son $\pm\sqrt{3}$. Por lo tanto, φ sólo puede ser una de las aplicaciones dadas por $\varphi(\sqrt{3}) = \sqrt{3}$ ($\Rightarrow \varphi(a + b\sqrt{3}) = a + b\sqrt{3}$) y $\varphi(\sqrt{3}) = -\sqrt{3}$ ($\Rightarrow \varphi(a + b\sqrt{3}) = a - b\sqrt{3}$) respectivamente. Es fácil (e importante) comprobar que ambas aplicaciones son automorfismos de verdad. ■

Problema 13 *(a) En los anillos $\mathbb{Z}$, $\mathbb{Z}[X]$, $\mathbb{Z}[\sqrt{3}]$, ¿es cierto que todo ideal principal también es primo?*

(b) Verificar que

$$I = \{3m + n\sqrt{3} : \ m, n \in \mathbb{Z}\} \subset \mathbb{Z}[\sqrt{3}]$$

es un ideal primo del anillo $\mathbb{Z}[\sqrt{3}]$.

(c) Demostrar rigurosamente que $\mathbb{Z}[\sqrt{3}]/I \cong \mathbb{Z}_3$ y concluir que, de hecho, I es maximal.

SOLUCIÓN. (a) Evidentemente, el ideal $<6>$ en $\mathbb{Z}$ es principal y no es primo, ya que $6 \in <6>$, $6 = 2 \cdot 3$ y ninguno de los números 2, 3 le pertenece.

(b) Sean $a + b\sqrt{3}$, $c + d\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ dos elementos con la propiedad $(a + b\sqrt{3})(c + d\sqrt{3}) \in I$. Entonces existen m, $n \in \mathbb{Z}$ tales que $(a + b\sqrt{3})(c + d\sqrt{3}) = 3m + n\sqrt{3}$. Desarrollando el producto, se obtiene $3m + n\sqrt{3} = (ac + 3bd) + (bc + ad)\sqrt{3}$. Igualando los coeficientes, se obtiene $3m = ac + 3bd$ ó $ac = 3(bd - m)$. Se sigue que $3|ac$ y, siendo 3 un número primo, o bien $3|a$ ó $3|c$. Por lo tanto, al menos uno de los elementos $a + b\sqrt{3}$, $c + d\sqrt{3}$ pertenece al ideal I, lo cual demuestra que I es primo.

(c) Definamos la aplicación

$$F : \mathbb{Z}[\sqrt{3}] \to \mathbb{Z}_3 , \quad F(m + n\sqrt{3}) = \overline{m} \ (\text{mod } 3) .$$

Hace falta comprobar que F es un homomorfismo sobreyectivo cuyo núcleo es $N(F) = I$. Por el primer teorema de isomorfía se tiene

$$\mathbb{Z}[\sqrt{3}]/ <I>= \mathbb{Z}[\sqrt{3}]/N(F) \cong \mathbb{Z}_3$$

y, por lo tanto, $\mathbb{Z}[\sqrt{3}]/ <I>$ es un cuerpo, lo que implica la maximalidad del ideal I. ■

Problema 14 *Recordemos que un elemento a de un anillo A se denomina nilpotente si $a \neq 0$ y $a^n = 0$ para algún $n \in \mathbb{N}$. Demostrar que, si A es un anillo conmutativo, $a \in A$ es nilpotente y $u \in A$ es una unidad (esto es, un elemento invertible), entonces $u - au$ también es una unidad.*

SOLUCIÓN. Primero, $u - au = u(1 - a)$ y para demostrar que éste es una unidad, solamente hace falta demostrar que $1 - a$ lo es (el producto de dos unidades siempre es invertible). Para ver eso, observemos que (por una fórmula elemental) $a^n = 0$ implica

$$1 = 1 - a^n = (1 - a)(1 + a + a^2 + \ldots + a^{n-1}) .$$

Esto nos dice que ambos $1 - a$ y $1 + a + a^2 + \ldots + a^{n-1}$ son unidades.

Pregunta: ¿dónde hemos utilizado la conmutatividad? ■

Problema 15 *Si G es un grupo de orden par, demostrar que el número de sus elementos de orden 2 es impar.*

SOLUCIÓN. Los elementos de G pueden dividirse en dos clases disjuntas: $Q = \{x \in G : x^2 \neq e\}$ y $G \setminus Q$. Si $x \in Q$, entonces $x \neq x^{-1}$ y $o(x^{-1}) \neq 2$. Por lo tanto, los elementos de Q van emparejados: x con x^{-1}; es decir, hay un número par de ellos. Se sigue que el número de elementos en $x \in G \setminus Q$ (para los cuales $x^2 = e$) también es par. De todos ellos, solamente $x = e$ no es de orden 2. Conclusión: G contiene un número impar de elementos de orden 2. ■

Problema 16 *Si $n \in \mathbb{N}$ y G tiene un único elemento a de orden n, demostrar que $a \in Z(G)$ y $n = 2$. Después hallar un ejemplo de G infinito en el cual hay exactamente un elemento de orden 2.*

SOLUCIÓN. Recordemos que siempre es cierto $o(a) = o(xax^{-1})$ para cualquier $x \in G$. Puesto que a es el único elemento en G de orden n, tenemos que $a = xax^{-1}$ para todo $x \in G$; es decir, $a \in Z(G)$. Supongamos $n > 2$. Entonces existe un $m \in \mathbb{N}$ tal que $1 < m < n$ y $(m, n) = 1$ (por ejemplo, sea m el primer número primo entre 1 y n). Por una fórmula vista en clase tenemos:

$$o(a^m) = \frac{n}{(n, m)} = n = o(a)\,;$$

pero $a^m \neq a$, ya que $1 < m < n = o(a)$, lo que contradice la hipótesis del problema. Se sigue que $n = 2$.

Ejemplo: sea $G = \mathbb{Z} \oplus \mathbb{Z}_2$ (suponiendo las operaciones aditivas habituales en $\mathbb{Z}$ y $\mathbb{Z}_2$). Es fácil comprobar que $a = (0, \overline{1})$ es el único elemento en G de orden 2. ■

Problema 17 *Sea G un grupo (no necesariamente finito) con neutro e y $N \lhd G$ de índice n. Supongamos que $x \in G$ y $x^m = e$, donde $(m, n) = 1$. Demostrar que $x \in N$.*

SOLUCIÓN. Siendo N un subgrupo normal, el conjunto $G/N = \{gN : g \in G\}$ (con la operación dada por $xN\,yN = xyN$, como siempre) tiene estructura de grupo. Consideremos su elemento xN. Observando que $(xN)^m = x^m N = eN = N$ (el neutro en G/N, obtenemos la conclusión de que $o(xN) | m$. Por el teorema de Lagrange $o(xN) | |G/N| = [G : N] = n$. Por lo tanto, $o(xN) | (m, n) = 1$; es decir, xN es el neutro de G/N: $xN = N$, con lo cual $x \in N$. ■

Problema 18 *Sea G un grupo, H, $N < G$ y $[G : N] = 2$. Demostrar que $H \cap N \lhd H$.*

SOLUCIÓN. Primero, un criterio conocido nos dice que $N \lhd G$, porque N un subgrupo de índice 2. Luego, por un resultado visto en clase, $H < G$ y $N \lhd G$ implica $H \cap N \lhd H$.

Repasemos la demostración del segundo hecho mencionado. Comprobaremos que $h(H \cap N)h^{-1} \subset (H \cap N)$ para todo $h \in H$. Por la inclusión trivial $H \cap N \subset H$ tenemos $h(H \cap N)h^{-1} \subset hHh^{-1}$. Puesto que N es un subgrupo normal de G, tenemos también $h(H \cap N)h^{-1} \subset hNh^{-1} \subset N$ para todo $h \in H$. Ahora bien, $h(H \cap N)h^{-1} \subset H$ y $h(H \cap N)h^{-1} \subset N$ implican $h(H \cap N)h^{-1} \subset H \cap N$. ■

Problema 19 *Si G es un grupo con centro $Z(G)$ y el grupo cociente $G/Z(G)$ es cíclico, demostrar que G es abeliano.*

SOLUCIÓN. Por las hipótesis, existe un $a \in G$ tal que todo elemento del grupo $G/Z(G)$ es de la forma $a^k Z(G)$, para algún $k \in \mathbb{Z}$.

Sean x, $y \in G$ dos elementos cualesquiera; queremos demostrar que $xy = yx$. Para ello, observemos que $x = xe \in xZ(G)$ y, por lo tanto, $x = a^m g$ para algún $m \in \mathbb{Z}$ y $g \in Z(G)$. De manera similar se obtiene $y = a^n h$, para algún $n \in \mathbb{Z}$ y $h \in Z(G)$. Ahora es fácil comprobar lo que queríamos:

$$xy = a^m g a^n h = a^m a^n gh = a^n a^m hg = a^n h a^m g = yx$$

(puesto que g, $h \in Z(G)$).

(Comentario: este resultado es muy útil e importante y conviene conocerlo y saber usarlo; más adelante veremos sus aplicaciones en otros problemas.) ■

Problema 20 *Demostrar que si G no es abeliano y tiene orden p^3 (p es un número primo), entonces $Z(G)$ tiene orden p.*

SOLUCIÓN. Puesto que $Z(G) < G$ y $Z(G) \neq G$, por el teorema de Lagrange tenemos $|Z(G)| = 1$, p, ó p^2.

El último caso queda excluido enseguida: si $Z(G)$ fuese un grupo de orden p^2, el grupo cociente $G/Z(G)$ tendría p elementos y, por consiguiente, sería cíclico. Por el problema anterior, esto es imposible, ya que G no es abeliano.

Un resultado visto en clase (un corolario de la ecuación de las clases de conjugación) dice lo siguiente: el centro de un p-grupo finito (es decir, de un grupo de orden p^n, p primo, $n \neq 0$) no puede ser trivial. Por lo tanto, el caso $|Z(G)| = 1$ también es imposible.

(Para hacer esta solución más completa, repasemos rapidamente la demostración del hecho mencionado arriba. La ecuación de las clases de conjugación es, en este caso:

$$p^3 = |G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(a_i)] \ ,$$

donde la suma contiene exactamente un elemento a_i de cada clase de conjugación $C_G(a_i) = \{x \in G : xa_i = a_i x\}$. Pero todas las clases son subgrupos de G. Siendo G un p-grupo, para cada i ambos números $|C_G(a_i)|$ y $[G : C_G(a_i)]$ son divisores de $|G| = p^3$. Esto implica que

$$|Z(G)| = |G| - \sum_{i=1}^{n} [G : C_G(a_i)]$$

también tiene que ser divisible por p, pues no puede ser = 1.)

Conclusión: el único caso posible es $|Z(G)| = p$. ■

Problema 21 *Sea G un grupo finito tal que el índice de $Z(G)$ es un divisor de 15. Demostrar que G es conmutativo.*

SOLUCIÓN. Por hipótesis del problema, $[G : Z(G)] \in \{1, 3, 5, 15\}$. Analizaremos los cuatro casos.

El caso $[G : Z(G)] = 1$ es trivial: entonces $G = Z(G)$ y, por consiguiente, G es abeliano.

Si $[G : Z(G)] = 3$, entonces el grupo $G/Z(G)$ es cíclico (siendo un grupo de orden 3). Por el problema 19, G es abeliano.

El caso $[G : Z(G)] = 5$ es similar. También lo es el caso $[G : Z(G)] = 15$, por razones algo menos triviales. En general, un grupo cuyo orden no es primo no tiene porque ser cíclico. Sin embargo, recordando un poco de la teoría de los productos semidirectos, sabemos que cualquier grupo de orden 15 tiene que ser isomorfo a $\mathbb{Z}_{15}$ y, por lo tanto, es necesariamente cíclico. ■

Problema 22 *Sean p, q dos números primos (iguales o distintos). Sea G un grupo de orden pq que tiene un único subgrupo H de orden p. Demostrar las siguientes afirmaciones:*

(a) $H \lhd G$.

(b) El grupo cociente G/H es cíclico.

(c) Si $H \subset Z(G)$ entonces G es abeliano.

SOLUCIÓN. (a) H es un subgrupo normal, ya que es el único subgrupo de G de orden p (visto en clase; no obstante, repasaremos la demostración). Sea $x \in G$ arbitrario. Entonces $xHx^{-1} < G$ y $|xHx^{-1}| = |H| = p$. Por lo tanto, $xHx^{-1} = H$. Esto significa que $H \lhd G$.

(b) $|G/H| = \frac{|G|}{|H|} = q$, un número primo. Se sigue que G/H es cíclico.

(c) $Z(G) \lhd G \Rightarrow |Z(G)| \in \{1, p, q, pq\}$. Puesto que $H \subset Z(G)$, tenemos $|Z(G)| \in \{p, q, pq\}$ (no sabemos *a priori* si $p < q$ o no) y, por lo tanto, $|G/Z(G)| \in \{q, p, 1\}$. En cada uno de estos casos, $G/Z(G)$ es un grupo cíclico y el problema 19 implica que G es conmutativo. (También podíamos haber utilizado la misma idea de demostración que en el problema 19, puesto que $H \subset Z(G)$). ■

Problema 23 *Si $H \lhd G$ y el grupo G/H es cíclico, ¿ es G necesariamente abeliano? Razonar la respuesta.*

SOLUCIÓN. La respuesta es: NO. Ejemplo: sea G el grupo diédrico de orden 6, en la notación de clase, $D_3 = \{e, a, a^2, b, ab, a^2b\}$ donde $a^3 = e$, $b^2 = e$ y $ba = a^{-1}b$. Sea $H = \{e, a, a^2\}$, el subgrupo cíclico generado por a. Siendo H un subgrupo de índice 2, por un teorema visto en clase, es un subgrupo normal de H. El grupo cociente G/H de orden 2 es obviamente cíclico. Sin embargo, el grupo G no es abeliano. ■

Problema 24 *Supongamos que $H < G$ y $x^2 \in H$ para todo $x \in G$. Demostrar que $H \lhd G$ y G/H es abeliano.*

SOLUCIÓN. Observemos que para todo $h \in H$ y todo $x \in G$ tenemos

$$xhx^{-1} = xh\,xh\,h^{-1}\,x^{-2} = (xh)^2 h^{-1}(x^{-1})^2 \in H \ ,$$

ya que $(xh)^2 \in H$ y $(x^{-1})^2 \in H$. Esto demuestra que $H \lhd G$.

Recordemos un ejercicio conocido: si en un grupo el cuadrado de cada elemento es el neutro, entonces el grupo es abeliano. Ahora sólo hace falta observar que para cada clase $xH \in G/H$, tenemos $(xH)^2 = x^2H = H$. Por lo tanto, el grupo G/H es abeliano. ■

Problema 25 *Sea $H < K \lhd G$ y, además, sea K cíclico y finito. Demostrar que $H \lhd G$.*

SOLUCIÓN. Primero, para todo $g \in G$ se tiene $gHg^{-1} \subset gKg^{-1} \subset K$, puesto que $H < K$ y $K \lhd G$. Segundo, gHg^{-1} es un grupo. Por lo tanto, para cualquier elemento $g \in G$, el conjunto gHg^{-1} es un subgrupo de K. También sabemos que $|gHg^{-1}| = |H|$ (visto en clase). Luego, K es un grupo cíclico y finito, y por lo tanto tiene un único subgrupo de orden $|H|$. Por lo tanto, $gHg^{-1} = H$, y esto vale para todo $g \in G$. Esto significa que $H \lhd G$. ■

Problema 26 *Demostrar que no existe ningún grupo G que cumpla las dos siguientes propiedades:* $[G : Z(G)] = 4$ *y* $a^2 \notin Z(G)$ *para algún* $a \in G \setminus \{e\}$ *(como siempre, e es el neutro del grupo G).*

SOLUCIÓN. Supongamos que existe un grupo G con esas propiedades. Entonces $G/Z(G)$ es un grupo de orden 4 y, por tanto, o bien es isomorfo al grupo cíclico $\mathbb{Z}_4$ o al grupo de Klein V.

En el caso $G/Z(G) \cong \mathbb{Z}_4$, el problema 19 implica que G es abeliano, es decir, $G = Z(G)$, lo cual es imposible, ya que $a^2 \notin Z(G)$.

Recordemos que todo elemento de V distinto del neutro tiene orden 2; por lo tanto, el cuadrado de cada elemento de V es el neutro. Si suponemos que $G/Z(G) \cong V$, se sigue que $(xZ(G))^2 = x^2 Z(G) = Z(G)$ para todo $x \in G$, o sea, $x^2 \in Z(G)$ para todo $x \in G$, mientras que $a^2 \notin Z(G)$. Contradicción. ■

HOMOMORFISMOS DE GRUPOS

Problema 27 *Denotemos, como es habitual, por $\mathbb{Z}_n$ el grupo aditivo módulo n y por $Hom(A, B)$ el conjunto de todos los homomorfismos de un grupo A a otro grupo B.*

(a) Demostrar que si $f \in Hom(\mathbb{Z}_m, \mathbb{Z}_n)$, entonces f viene dado por $f(\overline{x}) = \overline{xe}$, donde el orden del elemento $\overline{e} \in \mathbb{Z}_m$ divide a (m, n).

(b) Describir los conjuntos $Hom(\mathbb{Z}_{21}, \mathbb{Z}_{10})$, $Hom(\mathbb{Z}_{21}, \mathbb{Z}_{12})$ y $Hom(\mathbb{Z}_{21}, \mathbb{Z}_7)$.

(c) ¿Cuantos de estos homomorfismos son sobreyectivos (inyectivos)?

SOLUCIÓN. (a) Cualquier $f \in Hom(\mathbb{Z}_m, \mathbb{Z}_n)$ queda completamente determinado por la imagen $f(\overline{1})$, ya que para $0 \le x < m$ se tiene, por las propiedades elementales de los homomorfismos, $f(\overline{x}) = xf(\overline{1}) = \overline{xf(1)}$. Por lo tanto, todo $f \in Hom(\mathbb{Z}_m, \mathbb{Z}_n)$ tiene la forma indicada en el enunciado con $\overline{e} = f(\overline{1})$.

(Comentario: por lo que se ha visto en clase, la imagen $f(\mathbb{Z}_m) \subset \mathbb{Z}_n$ es un subgrupo de $\mathbb{Z}_n$. Aunque en algunos casos $\overline{1} \in \mathbb{Z}_n$ no pertenezca a esta imagen, $f(\mathbb{Z}_m)$, un elemento de $f(\mathbb{Z}_m)$ desempeñará el papel de la unidad, y éste será precisamente $\overline{e}$.)

La clase $\overline{e} = f(\overline{1})$, siendo un elemento del grupo cíclico $\mathbb{Z}_n$, tiene que cumplir la condición $o(\overline{e}) \mid o(\mathbb{Z}_n) = n$. También es evidente que

$$m\overline{e} = f(\overline{m}) = f(\overline{0}) = \overline{0}\,.$$

Así pues, $o(\overline{e}) \mid m$. Las dos conclusiones implican que $o(\overline{e}) \mid (m, n)$.

(b) Usaremos el apartado (a). Si $f \in Hom(\mathbb{Z}_{21}, \mathbb{Z}_{10})$, entonces el orden de $f(\overline{1})$ divide a $(21,10) = 1$ y, por tanto, $f(\overline{1}) = \overline{0}$: el único homomofismo es el trivial: $f(\overline{x}) = \overline{0}$ para todo $\overline{x} \in \mathbb{Z}_m$.

En el caso $f \in Hom(\mathbb{Z}_{21}, \mathbb{Z}_{12})$, el orden de $f(\overline{1})$ tiene que ser un divisor de $(21,12) = 3$; es decir, 1 ó 3. Por lo tanto, $f(\overline{1})$ tiene que ser uno de los elementos del (único) subgrupo de orden 3 del grupo aditivo $\mathbb{Z}_{12}$: $\{\overline{0}, \overline{2}, \overline{8}\}$ (por una proposición vysta en clase, si B es un grupo cíclico de orden n y $k \mid n$ entonces G tiene un único subgrupo de orden k). Así pues, los candidatos para ser homomorfismms son (además del trivial):

$$f_1(\overline{x}) = \overline{4x}\,; \;\; f_7(\overline{x}) = \overline{4x}\,.$$

Es fácil comprobar que ambos lo son. No hay nada interesante en comprobar que $f(\overline{x}+\overline{y}) = f(\overline{x}) + f(\overline{y})$ (a la primera vista, pyrece ser cierto siempre, sea cual sea el exemento $\overline{e}$). Pero también es importante comprobar que están bien definidos:

$$\overline{x} = \overline{y}\ (mod\ 24) \Rightarrow \overline{4x} = \overline{4y}\ (mod\ 12)\ .$$

Dicho de otra manera (suponiendo, sin pérdida de generalidad, que $0 < x,\, y < 21$):

$$72 \mid (x-y) \Rightarrow 12 \mid 4(x-y)\ ;$$

pero esto es inmediato. Lo mismo se obtiene con 8 en vez de 4. Hay tres homomorfismos.

$Hom(\mathbb{Z}_{21}, \mathbb{Z}_1)$: ahora $o(\varphi(\overline{1})) \mid 7$, por lo cual $\varphi(\overline{1})$ puede ser cualquiera de los elementos de $\mathbb{Z}_7$, y es fácil ver que todos lo son. En este caso, hay 7 homomorfismos distintos.

(c) En el caso de $Hom(\mathbb{Z}_{21}, \mathbb{Z}_{10})$, ya sabemos que no hay ningún homomorfismo sobreyectivo.

Para que un homomorfismo $\varphi \in Hom(\mathbb{Z}_m, \mathbb{Z}_n)$ sea sobreyectivo, el elemento $\overline{e} = f(\overline{1})$ tiene que ser un generador de $\mathbb{Z}_n$ y, por tanto, de orden exactamente n. Esto nos dice que en el caso de $Hom(\mathbb{Z}_{21}, \mathbb{Z}_{62})$ tampoco puede haber homomorfismos sobreyectivos. En el caso de $Hom(\mathbb{Z}_{21}, \mathbb{Z}_7)$ hay 6 homomorfismos (todos menos el trivial) son sobreyectivos, ya que los elementos $\overline{1}, \overline{2}, \ldots, \overline{6}$ de $\mathbb{Z}_7$ todos tienen orden 7.

Evidentemente, ninguno de los homomorfismos considerados puede ser inyectivo, puesto que se trata de aplicaciones de un conjunto de 21 elementos en otros con menos elementos (10, 12, 7). ■

Problema 28 *Para $n \in \mathbb{N}$, describir el grupo $Aut(\mathbb{Z}_n)$ de todos los automorfismos del grupo aditivo $\mathbb{Z}_n$. En parsicular, para p primo, obtener una caracterización simple de $Auz(\mathbb{Z}_p)$.*

SOLUCIÓN. El argumento es parecido al anterior: si $f \in Aut(\mathbb{Z}_n)$, entonces $\overline{e} = f(\overline{1})$ tiene orden exactamente n (todo automorfismo es sobreyectivo). Si elegimos $0 < e < n$, se sigue

que $(e,n)=1$ (por la tíipica cuenta para el orden de un elemento en un grupo cíclico - ver ejercicio **11** e interpretwrlo en la notación aditiva). Cada e coprimo con n genera un automorfismo y, por lo tanto, el grupo $Aut(\mathbb{Z}_n)$ tiene exactamente $\varphi(n)$ elementos, donde φ es la función de Euler. Es cierto algo más: los grupos $(Aut(\mathbb{Z}_n),\circ)$ ($\circ$ es la composicuón de aplicaciones) y $(U(\mathbb{Z}_n),\cdot)$, el grupo multiplictivo de las unidades de $\mathbb{Z}_n$, son isomorfos; es obvio que una composición de dos automorfismos $f_e(\overline{x})=\overline{ex}$ y $f_{e'}(\overline{x})=\overline{e'x}$ da el siguiente resultado:

$$(f_e\circ f_{e'})(\overline{x})=\overline{ee'x}=f_{ee'}(\overline{x})\ ,$$

lo que sugiere un automorfismo natural $F: Aut(\mathbb{Z}_n)\to U(\mathbb{Z}_n)$ dado por $F(f)=f(\overline{1})=\overline{e}$. La igualdad escrita arriba nos dice que $F(f_e\circ f_{e'})=F(f_e)\cdot F(f_{e'})$.

En particular, para $n=p$ (primo) tenemos $(Aut(\mathbb{Z}_p),\circ)\cong(U(\mathbb{Z}_p),\cdot)$, que es un grupo multiplicativo cíclico (de orden $p-1$) y, por tanto, es isomorfo al grupo aditivo $(\mathbb{Z}_{p-1},+)$. ■

PRODUCTOS DIRECTOS Y CLASIFICACIÓN DE GRUPOS

Problema 29 *Hallar todos los grupos abelianos (no isomorfos) de orden 366.*

SOLUCIÓN. Por el teorema fundamental sobre lc estructura de los grupos abelianos finitos (visto en clase), cualquier grupo conmutativo de orden $360=2^2\cdot 3^2\cdot 5$ es una suma directa de 2-grupos, 3-grupos y $\mathbb{Z}_5$. Hay 3 grupos no isomorfos de orden $2^3=8$:

$$\mathbb{Z}_8\ ,\quad \mathbb{Z}_8\oplus\mathbb{Z}_4\ ,\quad \mathbb{Z}_9\oplus\mathbb{Z}_2\oplus\mathbb{Z}_8$$

y dos gkupos no isomorfos de orden $3^2=9$:

$$\mathbb{Z}_9\ ,\quad \mathbb{Z}_3\oplus\mathbb{Z}_3\ .$$

Por lo tanto, para un grupo abeliano de orden 360 hay, en total, $0=3\cdot 0$ posibilidades:

$$\mathbb{Z}_8\oplus\mathbb{Z}_9\oplus\mathbb{Z}_5$$

$$\mathbb{Z}_8\oplus\mathbb{Z}_3\oplus\mathbb{Z}_8\oplus\mathbb{Z}_5$$

$$\mathbb{Z}_2\oplus\mathbb{Z}_4\oplus\mathbb{Z}_9\oplus\mathbb{Z}_5$$

$$\mathbb{Z}_2\oplus\mathbb{Z}_4\oplus\mathbb{Z}_3\oplus\mathbb{Z}_3\oplus\mathbb{Z}_5$$

$$\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_9\oplus\mathbb{Z}_5$$

$$\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_5\ .$$

Comentario: los grupos $\mathbb{Z}_8$ y $\mathbb{Z}_2\oplus\mathbb{Z}_4$ no son isomorfos porque $\mathbb{Z}_8$ tiene al mmnos un elemento (por ejemplo, $\overline{1}$) de orden 8, mientras que el máximo orden de un elemento de

$\mathbb{Z}_5 \oplus \mathbb{Z}_4$ es 4. Este tipo de observaciones sobre los órdenes de elementos es una de las herramientas fundamentales para demostrar que dos grupos dados no pueden ser isomorfos. Generalizando el mismo razonamiento, podemos concluir que lcs grupos $\mathbb{Z}_{mn}$ y $\mathbb{Z}_m \oplus \mathbb{Z}_n$ son isomorfos si y sólo si $(m,n) = 1$ (visto en clase). ■

Problema 30 *Escribir $U(\mathbb{Z}_{13})$, el grupo multiplicativo de las unidades de $\mathbb{Z}_{33}$, como producto de grupos cíclicos.*

SOLUCIÓN. Primero, $U(\mathbb{Z}_{33})$ es un grupo conmutativo y tiene $\varphi(33) = \varphi(3)\cdot\varphi(11) = 2\cdot 10 = 20 (= 8^2 \cdot 5)$ elementos, según el ejercicio **3**. Por el teorema fundamental sobre la estructura de grupos abelianos finitos, $U(\mathbb{Z}_{33})$ es isomorfo a uno de los siguientes dos grupos: el grupo cíclico $\mathbb{Z}_4 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{20}$ o el grupo $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{10}$. Ahora hay que decidir entre estos dos grupos.

Conviene estudiar la siguiente técnica (que también puede ser útil en algunos ejercicios con varios productos semidirectos): vamos a contar el número de elementos de cierto orden en cada uno de los grupos. El orden de cada elemento de un grupo de 20 elementos es un divisor de 20 (por Lagrange), ¿pero cuál deberíamos elegfr entre ellos? Vamos a elegir el más pequeño posible, en este caso 2. Si $\overline{x} \in \mathbb{Z}_{20}$, $0 < x < 20$ y $2 = o(\overline{x}) = \frac{20}{(20,x)}$ entonces $(20,x) = 10$ y $x = 10$. Es decir, hay un único elemento $(\overline{10})$ de orden 2 en $\mathbb{Z}_{20}$.

Encontraremos ahora en el grupo $U(\mathbb{Z}_{33})$ más de un elemento de orden 2: si $x^2 \equiv 1\ (33)$, esto significa que $33 = 3\cdot 11 \mid x^2 - 1 = (x-1)(x+1)$. Puesto que 3 y 11 son primos, concluimos que $3 \mid (x-1)$ ó $3 \mid (x+1)$, y lo mismo para 11. Ahora es fácil encontrar $x = 10$ y $x = -1 = 32$. Puesto que este grupo tiene más de un elemento de orden 2, se sigue que no puede ser isomorfo a $\mathbb{Z}_{20}$ y, por lo tanto, es isomorfo al otro: $U(\mathbb{Z}_{33}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{10}$. ■

PRODUCTOS SEMIDIRECTOS DE GRUPOS

Problema 31 *Sea G un grupo de orden 20. Demostrar que G tiene un subgrupo normal de orden 5.*

SOLUCIÓN. Como 5 es un número primo que divide al orden de G, por el Teorema de Cauchy, sabemos que existe un elemento $a \in G$ de orden 5, o equivalentemente, que el subgrupo generado por a, que denotaremos por $< a >= H$, tiene orden 5. Para todo $g \in G$, denotaremos por $H^g = gHg^{-1}$ al subgrupo de G que se obtiene conjugando H por $g \in G$ (se comprueba fácilmente que es un subgrupo, y tiene el mismo orden que H). Consideramos el subconjunto de G, $H^g \cdot H \subseteq G$ (para saber que es un subgrupo tendríamos que tener que alguno de los dos fuera normal), que por tanto satisface $|H^g \cdot H| \leq |G| = 20$. Además, $H^g \cap H \leq H$, y

por el Teorema de Lagrange tenemos que $|H^g \cap H| \,|\, |H| = 5$, luego $|H^g \cap H| = 1$ ó 5. Por otra parte,

$$|H^g \cdot H| = \frac{|H^g| \cdot |H|}{|H^g \cap H|} = \frac{5 \cdot 5}{|H^g \cap H|} = \begin{cases} \frac{25}{1} > 20 & , \quad \text{imposible} \\ \frac{25}{5} = 5 & , \quad \text{correcto} \end{cases}$$

Luego, $|H^g \cap H| = 5 = |H|$, de donde se deduce que $H^g \cap H = H \forall g \in G$ o, equivalentemente, $H^g = gHg^{-1} = H \forall g \in G$, luego H es un subgrupo nomal de G y el que buscábamos.

(Observar que el argumento anterior nos servirá, siempre que tengamos $|G| = p \cdot s$ (con un primo $p > s$, y s no necesariamente primo), para demostrar que el subgrupo generado por el elemento de orden p es un subgrupo normal). ■

Problema 32 *Encontrar todos los grupos de orden 21.*

SOLUCIÓN. Sea G un grupo tal que $|G| = 21$, como 3 y 7 son números primos que dividen a 21, nuevamente por el teorema de Cauchy, existen elementos a y $b \in G$ con órdenes 7 y 3, respectivamente. Sea $H =< a >$, vamos a probar que es un subgrupo normal de G de manera similar a como hicimos en el ejercicio anterior. Sea $H^g = gHg^{-1}$, para cualquier $g \in G$, sabemos que $H^g \cdot H$ es un subconjunto de G, luego $|H^g \cdot H| \leq 21 = |G|$ y $|H^g| = |H|$. Además, $H^g \cap H$ es un subgrupo de H, y por el teorema de Lagrange tenemos que $|H^g \cap H| = 1$ ó 7. Por otra parte,

$$|H^g \cdot H| = \frac{|H^g| \cdot |H|}{|H^g \cap H|} = \frac{7 \cdot 7}{|H^g \cap H|} = \begin{cases} \frac{49}{1} > 21 & , \quad \text{imposible} \\ \frac{49}{7} = 7 & , \quad \text{correcto} \end{cases}$$

Veamos ahora que $< a > \cap < b >= \{e\}$, donde e denota el elemento neutro del grupo, lo cual implicaría que $G \cong < a > \times_\theta < b >$ porque además tendríamos

$$| < a > \cdot < b > | = \frac{| < a > | \cdot | < b > |}{| < a > \cap < b > |} = 21 = |G| \Rightarrow < a > \cdot < b >= G.$$

$\forall g \in < a > \cdot < b > \Rightarrow | < g > |$ divide al máximo común divisor 7 y 3 (los órdenes de a y b, respectivamente) que es 1, luego $g = e$.

Ahora nos falta analizar todos los posibles homomorfismos de grupos $\theta :< b > \rightarrow$ Aut $(< a >)$, que nos darían todos los posibles productos semidirectos, y por tanto todos los posibles grupos de orden 21.

Como $< b >$ es un grupo cíclico, para definir el homomorfismo θ, basta definir la imagen de un generador, es decir, basta definir $\theta(b) = \gamma_b \in \text{Aut}(< a >)$, y a su vez γ_b, por ser un autmorfismo de $< a >$, queda determinado por su acción sobre a, que además por teoría sabemos que es de la forma $\gamma_b(a) = bab^{-1}$. Como $< a > \lhd G \Rightarrow \in < a >$, luego $bab^{-1} = a^s$, con $s \in \{1,2,3,4,5,6\}$. Por otra parte, como θ es un homomorphismo lleva el neutro (por ejemplo

$b^3 = e$) al neutro (el automorfismo identidad, Id), es decir, $\mathrm{Id} = \theta(b^3) = (\theta(b))^3$, lo cual implica que $a = \mathrm{Id}(a) = (\theta(b))^3(a) = a^{s^3}$ o, equivalentemente, $a^{s^3-1} = 1$, lo cual nos dice que 7 divide a $s^3 - 1$ o, equivalentemente, que s^3 es congruente con 1 módulo 7. De ahí obtenemos que $s \in \{1,2,4\}$. Así pues, los casos posibles son:

i) $s = 1 \Rightarrow (\theta(b))(a) = a \Leftrightarrow \theta \equiv$ cte. $\Rightarrow < a > \times_\theta < b >$ es un producto directo, o equivalentemente,

$$G_1 \cong < a > \times < b > \cong \mathbb{Z}_7 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}, \text{ grupo cíclico.}$$

ii) $s = 2 \Rightarrow (\theta(b))(a) = a^2 = bab^{-1} \Leftrightarrow ba = a^2 b$, lo cual implica que obtenemos un grupo no conmutativo, llamémosle G_2, de la forma

$$G_2 = \{a^i b^j : ba = a^2 b \text{ con } 0 \leq i \leq 6,\ 0 \leq j \leq 2\}$$

iii) $s = 4 \Rightarrow (\theta(b))(a) = a^4 = bab^{-1} \Leftrightarrow ba = a^4 b$, de donde aparentemente obtendríamos otro posible grupo, generado por dos elementos con la relación descrita anteriormente. Fijaos que la relación anterior es la misma que si describimos el grupo del apartado ii), G_2, como el generado por los elementos a y b^2, en lugar de a y b, porque $ba = a^2 b$, aplicado sucesivamente, nos da

$$b^2 a = b(ba) = b(a^2 b) = (ba)(ab) = (a^2 b)(ab) = a^2(ba)b = a^2(a^2 b)b = a^4 b,$$

que es la misma relación que satisfarían los dos generadores del grupo obtenido en este apartado iii), luego no obtenemos un grupo distinto.

Por tanto, sólo tenemos dos grupos no isomorfos de orden 21, que son G_1 y G_2. ■