

“SOBRE UNAS CONJETURAS DE ISSAI SCHUR”

FLOR ÁNGELA DURÁN SANDOVAL

UNIVERSIDAD NACIONAL DE COLOMBIA
FACULTAD DE CIENCIAS
DEPARTAMENTO DE MATEMÁTICAS
BOGOTÁ
MAYO DE 2005

“SOBRE UNAS CONJETURAS DE ISSAI SCHUR”

FLOR ÁNGELA DURÁN SANDOVAL

PRESENTADO COMO REQUISITO
PARA OPTAR AL TÍTULO DE **Matemático**

DIRECTOR:
VÍCTOR SAMUEL ALBIS

UNIVERSIDAD NACIONAL DE COLOMBIA
FACULTAD DE CIENCIAS
DEPARTAMENTO DE MATEMÁTICAS
BOGOTÁ
MAYO DE 2005

Capítulo 1

Sobre unas conjeturas de Issai Schur

En [17] y [18] *Issai Schur* conjetura que si a_1, \dots, a_M son números enteros distintos entre sí, y si

$$P(x) = (x - a_1) \cdots (x - a_M) = \prod_{i=1}^M (x - a_i)$$

entonces los polinomios

$$P(x) - 1 \tag{1.1}$$

$$P(x) + 1 \tag{1.2}$$

$$P^2(x) + 1 \tag{1.3}$$

$$P^4(x) + 1 \tag{1.4}$$

(para $M > 4$) son irreducibles en $\mathbb{Q}[x]$. A partir de estas conjeturas (hechas en 1908 y 1909) y otras expresadas en sus ejercicios de álgebra, se da inicio a una sucesión importantísima de trabajos sobre la irreducibilidad de polinomios de coeficientes enteros, la cual aún no se detiene.

Una demostración inicial de la ecuación (1.1) la da W. FLÜGEL en [7], señalando en este trabajo que con excepciones también la ecuación (1.2) es irreducible.

G. PÓLYA en [15] da algunos criterios para $M \geq 7$ de la irreducibilidad de (1.1) y (1.2) y estableciendo otros criterios de irreducibilidad como

1.1 Teorema. *Sea $f(x) \in \mathbb{Z}[x]$ de Grado $n \geq 1$, y supongase que de estos n enteros*

existe k talque

$$0 < |f(k)| < \frac{(n - \lfloor \frac{n}{2} \rfloor)!}{2^{n - \lfloor \frac{n}{2} \rfloor}}$$

entonces $f(x)$ es irreducible sobre \mathbb{Q}

Una demostración de la ecuación (1.3) es más fácil de hacer (si $M \geq 7$).

La irreducibilidad de (1.4) y (1.5), fue demostrada por A. BRAUER, R. BRAUER & H. HOPF [1] y A. BRAUER & R. BRAUER [2].

El polinomio

$$P^8(x) + 1 \tag{1.5}$$

Los polinomios (1.2), (1.3), (1.4) y (1.5) son polinomios especiales de la forma $G(P(x))$. Donde $G(z) = z^r + 1$, y con r como una potencia de 2, de donde este es irreducible. I. Schur busca demostrar que si $r = 2^s$ el polinomio es irreducible; con $s > 3$.

Solución de I. Seres

Del polinomio planteado en las conjeturas de I. Schur, Seres presento una demostración de este problema en 1956 ver [19]. En el desarrollo de este, se dan algunos resultados de interes y sus demostraciones.

Para hacer la demostración del polinomio, Seres hace una concatenación de otros teoremas aún más generales que permiten llegar al teorema propuesto por I. Schur. Para entender un poco mejor la demostración ver la figura 1.1.

1.2 Teorema. Sea a_1, a_2, \dots, a_M números enteros racionales distintos entre sí, con $M \geq 1$; $n \geq 1$. El polinomio

$$F(x) = \prod_{k=1}^M (x - a_k)^{2^n} + 1$$

es irreducible en $\mathbb{Q}[x]$.

1.3 Teorema. Sean a_1, a_2, \dots, a_M números enteros racionales distintos entre sí.

Si $f_m(x)$ es el m -ésimo polinomio ciclotómico primitivo ($m > 2$).

Entonces el polinomio

$$f_m(P(x))$$

donde $P(x) = \prod_{k=1}^M (x - a_k)$ es irreducible si $M \geq 5$.

Es claro que para $M < 5$ también es cierto salvo algunas excepciones.

1.4 Teorema. Sean a_1, a_2, \dots, a_M números enteros racionales distintos, con $M \geq 6$. Sea $Q(x)$ un polinomio de coeficientes enteros racionales con coeficiente director igual a 1 y tal que el Grado $Q(x) < M$.

Si además $f_m(x)$ designa al m -ésimo polinomio ciclotómico ($m > 2$) y $R(x)$ al polinomio $Q(x) \prod_{k=1}^M (x - a_k)$, entonces el polinomio

$$f_m(R(x))$$

es irreducible en $\mathbb{Q}[x]$.

1.5 Teorema. El polinomio

$$\psi(x) = Q(x) \prod_{k=1}^M (x - a_k) - \xi \quad (\xi = e^{\frac{2\pi i}{m}})$$

es irreducible en $\mathbb{Q}(\xi)[x]$, si $Q(x), a_1, \dots, a_M, M$ y m satisfacen las condiciones del teorema 1.4.

Para demostrar estos teoremas necesitamos algunos lemas

1.6 Lema. Sea $f_m(x)$ el m -ésimo polinomio ciclotómico primitivo de coeficientes enteros racionales. Entonces el polinomio $\Phi_m(x) = f_m(R(x))$ es irreducible sobre $\mathbb{Q}[x]$ si y solo si $\psi(x) = R(x) - \xi$ es irreducible sobre $\mathbb{Q}(\xi)[x]$.

(Este es un caso los especial del **Teorema de Capelli**)

Demostración. Tenemos que $f_m(x)$ es el m -ésimo polinomio ciclotómico primitivo ($m > 2$), es irreducible en $\mathbb{Q}[x]$, es decir que

$$f_m(x) = (x - \xi_1) \cdots (x - \xi_s).$$

donde cada ξ_l es una de las raíces primitivas de la unidad, con $l = 1, \dots, s$.

Como

$$\begin{aligned} f_m(x) &= (x - \xi_1) \cdots (x - \xi_s) \\ f_m(R(x)) &= (R(x) - \xi_1) \cdots (R(x) - \xi_s). \end{aligned}$$

Supongamos $R(x) - \xi$ es irreducible en $\mathbb{Q}(\xi)[x]$, con ξ una de las raíces primitivas de la unidad, pero que $f_m(R(x))$ es reducible en $\mathbb{Q}[x]$ esto es

$$f_m(R(x)) = G(x) \cdot H(x)$$

con $G(x), H(x) \in \mathbb{Q}[x]$, luego $G(x) \mid f_m(R(x))$ así que $G(x) \mid (R(x) - \xi_1) \cdots (R(x) - \xi_s)$, es decir que $G(x) \mid (R(x) - \xi)$ con $\xi = \xi_l, l = 1, \dots, s$.

Lo cuál es contradictorio ya que $R(x) - \xi$ es irreducible en $\mathbb{Q}(\xi)[x]$; ($\mathbb{Q} \subset \mathbb{Q}(\xi)$). \square

En lo que sigue suponemos que el polinomio

$$\psi(x) = Q(x) \prod_{k=1}^M (x - a_k) - \xi \quad (1.6)$$

es reducible sobre $\mathbb{Q}(\xi)[x]$.

Es decir existen polinomios no constantes $\tau(x), \omega(x) \in \mathbb{Q}(\xi)[x]$, unitarios tales que

$$\psi(x) = \tau(x)\omega(x). \quad (1.7)$$

Donde los coeficientes de $\tau(x), \omega(x)$ son enteros de $\mathbb{Q}(\xi)$.

Es fácil ver que el anillo de los enteros $\mathbb{Q}(\xi)$ es $\mathbb{Z}[\xi]$.

Entonces $\tau(a_k)$ ($k = 1, \dots, M$) son enteros de $\mathbb{Q}(\xi)$ (esto es que $\tau(a_k) \in \mathbb{Z}[\xi]$) pues los $a_k \in \mathbb{Z}$ (lo mismo para $\omega(a_k)$)

De (1.6) resulta que

$$\psi(a_k) = -\xi$$

y de (1.7),

$$\psi(a_k) = \tau(a_k)\omega(a_k).$$

Luego en $\mathbb{Z}[\xi]$,

$$\tau(a_k) \mid \xi.$$

Pero ξ es una unidad de $\mathbb{Z}[\xi]$ (esto se tiene ya que ξ es una raíz primitiva de la unidad, es decir, $\xi^m = e^{2\pi i} = 1$). De donde, si $\xi = \lambda\tau(a_k)$ con $\lambda \in \mathbb{Z}[\xi]$, entonces

$$1 = |\xi| = |\lambda \cdot \tau(a_k)| = |\lambda| \cdot |\tau(a_k)| \Rightarrow |\tau(a_k)| = 1$$

luego $\tau(a_k)$ es una unidad de $\mathbb{Z}[\xi]$.

1.7 Lema. *Los coeficientes del polinomio $\tau(x)$ pertenecen a $\mathbb{Z}[\xi]$. Si $|a_k - a_l| > 2$, entonces $\tau(a_k)\tau^{-1}(a_l)$ es real.*

Demostración. Del **teorema de Kroneker** [7], tenemos:

$$\tau(a_k) = \eta_k \varepsilon_k, \quad \tau(a_l) = \eta_l \varepsilon_l,$$

donde las η_k, η_l son raíces de la unidad complejas y $\varepsilon_k, \varepsilon_l$ son unidades reales de $\mathbb{Z}[\xi]$.

Si hacemos $\tau(x) = \beta_0 + \beta_1 x + \cdots + \beta_r x^r$, vemos

$$\begin{aligned} \eta_k \varepsilon_k - \eta_l \varepsilon_l &= \tau(a_k) - \tau(a_l) \\ &= (\beta_0 + \beta_1 a_k + \beta_2 a_k^2 + \cdots + \beta_r a_k^r) - (\beta_0 + \beta_1 a_l + \beta_2 a_l^2 + \cdots + \beta_r a_l^r) \\ &= \beta_1 (a_k - a_l) + \beta_2 (a_k^2 - a_l^2) + \cdots + \beta_r (a_k^r - a_l^r) \\ &= (a_k - a_l) \cdot \Theta, \end{aligned} \tag{1.8}$$

donde $\Theta \in \mathbb{Z}[\xi]$, puesto que los $\beta_i \in \mathbb{Z}[\xi]$ y los $a_k, a_l \in \mathbb{Z}$.

Luego

$$a_k - a_l \mid \eta_k \varepsilon_k - \eta_l \varepsilon_l$$

De la ecuación (1.8) resulta sucesivamente

$$\begin{aligned} \eta_k \varepsilon_k - \eta_l \varepsilon_l &= (a_k - a_l) \Theta && (\text{con } \Theta \in \mathbb{Z}[\xi]) \\ \eta_k - \eta_l \varepsilon_l \varepsilon_k^{-1} &= (a_k - a_l) \Theta \varepsilon_k^{-1} && (\text{con } \Theta \varepsilon_k^{-1} \in \mathbb{Z}[\xi]) \\ \eta_k \eta_l^{-1} - \varepsilon_l \varepsilon_k^{-1} &= (a_k - a_l) \Theta \varepsilon_k^{-1} \eta_l^{-1} && (\text{con } \Theta \varepsilon_k^{-1} \eta_l^{-1} \in \mathbb{Z}[\xi]) \end{aligned} \tag{1.9}$$

es decir,

$$a_k - a_l \mid \eta_k \eta_l^{-1} - \varepsilon_l \varepsilon_k^{-1}.$$

Tomando conjugados en (1.9), tenemos

$$\eta_k^{-1} \eta_l - \varepsilon_l \varepsilon_k^{-1} = (a_k - a_l) \overline{(\Theta \varepsilon_k^{-1} \eta_l^{-1})} \tag{1.10}$$

Restando (1.9) y (1.10), obtenemos que

$$\eta_k \eta_l^{-1} - \eta_k^{-1} \eta_l = (a_k - a_l) \cdot \odot \tag{1.11}$$

con $\odot = \Theta \varepsilon_k^{-1} \eta_l^{-1} - \overline{\Theta \varepsilon_k^{-1} \eta_l^{-1}} \in \mathbb{Z}[\xi]$, por lo que de (1.11) se tiene que

$$a_k - a_l \mid \eta_k \eta_l^{-1} - \eta_k^{-1} \eta_l.$$

De (1.11), resulta

$$\begin{aligned}\eta_k \eta_l^{-1} (\eta_k \eta_l^{-1} - \eta_k^{-1} \eta_l) &= \eta_k \eta_l^{-1} ((a_k - a_l) \cdot \odot) \\ (\eta_k \eta_l^{-1})^2 - 1 &= (a_k - a_l) \cdot \Delta\end{aligned}$$

con $\Delta = \eta_k \eta_l^{-1} \cdot \odot \in \mathbb{Z}[\xi]$.

Si $(\eta_k \eta_l^{-1})^2 - 1 \neq 0$, tenemos que

$$0 < |(\eta_k \eta_l^{-1})^2 - 1| \leq |(\eta_k \eta_l^{-1})^2| + 1 = 1 + 1 = 2,$$

entonces $|(a_k - a_l) \cdot \Delta| = 2$, es decir que $|a_k - a_l| \leq 2$. Pero como por hipotesis $|a_k - a_l| > 2$, estamos ante una contradicción.

Luego

$$\begin{aligned}(\eta_k \eta_l^{-1})^2 - 1 &= 0 \\ (\eta_k \eta_l^{-1} + 1)(\eta_k \eta_l^{-1} - 1) &= 0\end{aligned}$$

por lo que $\eta_k = \pm \eta_l$.

Así que,

$$\tau(a_k) \tau(a_l)^{-1} = \frac{\eta_k \varepsilon_k}{\eta_l \varepsilon_l} = \pm \frac{\varepsilon_k}{\varepsilon_l}$$

Como $\pm \varepsilon_k, \pm \varepsilon_l$ son reales, entonces $\tau(a_k) \tau(a_l)^{-1}$ es real. \checkmark

1.8 Lema. Sean $a_1 < a_2 < \dots < a_M$ números enteros racionales, $M \geq 6$ y $\tau(x) \in \mathbb{Z}[\xi][x]$. Sean $\tau(a_k)$ ($k = 1, \dots, M$) unidades de $\mathbb{Z}[\xi]$. Entonces las proporciones: $\frac{\tau(a_k)}{\tau(a_l)}$ son números reales.

Demostración. Como $M \geq 6$, tenemos

$$2 < a_4 - a_1, \quad a_5 - a_1, \quad \dots, \quad a_M - a_1$$

y

$$2 < a_M - a_3, \quad a_M - a_2, \quad a_5 - a_2, \quad a_6 - a_3.$$

entonces se tiene que $|a_k - a_l| > 2$ y por tanto se cumple el lema 1.7.

Supongamos que $|a_k - a_l| \leq 2$ pero que $|a_r - a_k| > 2$ y $|a_r - a_l| > 2$ (esto se tiene ya que con lo anterior garantizamos esto), luego

$$\begin{aligned} \frac{\tau(a_k)}{\tau(a_l)} &= \frac{\tau(a_k)}{\tau(a_l)} \cdot 1 = \frac{\tau(a_k)}{\tau(a_l)} \cdot \frac{\tau(a_r)}{\tau(a_r)} \\ &= \frac{\tau(a_k)}{\tau(a_r)} \cdot \frac{\tau(a_r)}{\tau(a_l)} \\ &= \left(\pm \frac{\varepsilon_k}{\varepsilon_r} \right) \cdot \left(\pm \frac{\varepsilon_r}{\varepsilon_l} \right) = \pm \left(\frac{\varepsilon_k}{\varepsilon_r} \cdot \frac{\varepsilon_r}{\varepsilon_l} \right) \\ &= \pm \frac{\varepsilon_k}{\varepsilon_l} \end{aligned}$$

como ε_k y ε_l son números reales, así que este lema se cumple. \checkmark

Demostración. **Teorema 1.5.** Supongamos que el polinomio

$$\psi(x) = Q(x) \prod_{k=1}^M (x - a_k) - \xi,$$

es entonces reducible en $\mathbb{Q}(\xi)[x]$, y lo podemos descomponer en factores primos unitarios

$$\psi(x) = \tau_1(x) \cdots \tau_r(x),$$

donde todos los coeficientes de $\tau_l(x)$ son enteros de $\mathbb{Q}(\xi)$, con $l = 1, \dots, r$.

Además tenemos que

$$\text{Grado } \psi(x) = \text{Grado } Q(x) + M < 2M$$

Así que el grado de por lo menos uno de los $\tau_1(x), \dots, \tau_r(x)$ es menor que

$$0 < \frac{M + \text{Grado } Q(x)}{2} < M$$

Podemos suponer, sin pérdida de generalidad que

$$0 < s = \text{Grado } \tau_1(x) < M$$

Supongamos de ahora en adelante que $M \geq 6$.

De los anterior (vease el lema 1.8) tenemos que si las unidades de $\mathbb{Q}(\xi)$

$$\tau_1(a_k) \quad (k = 1, \dots, M)$$

son de la forma

$$\tau_1(a_k) = \eta \varepsilon_k \quad (k = 1, \dots, M)$$

donde η es una unidad de la raíz compleja y $\varepsilon_1, \dots, \varepsilon_M$ son unidades reales .

Tomemos el polinomio $\eta^{-1}\tau_1(x)$.

Por la fórmula de *interpolación de Lagrange* existe un único polinomio $L(x) \in \mathbb{R}[x]$, determinado por los valores $L(a_k)$, con $k = 1, \dots, s, s + 1$.

Luego $\tau_1(x) = \eta \cdot L(x)$. Como $\tau_1(x) \mid \psi(x)$, y $L(x) \mid \tau_1(x)$, entonces $L(x) \mid \psi(x)$. Es decir

$$\psi(x) = L(x) \cdot \tau(x)$$

Pero todos los coeficientes de $\psi(x)$ son reales, menos el término constante que es ξ , pero esto es una contradicción. \square

Demostración. Teorema 1.4. Supongamos que $\Phi_m(x) = f_m(R(x))$, donde $R(x) = Q(x) \prod_{k=1}^M (x - a_k)$, es reducible en $\mathbb{Q}[x]$. Es decir

$$\Phi_m(x) = G(x) \cdot H(x),$$

donde $G(x), H(x) \in \mathbb{Q}[x]$ (unitarios).

Por el lema (1.6), el polinomio

$$\psi(x) = Q(x) \prod_{k=1}^M (x - a_k) - \xi,$$

es entonces reducible en $\mathbb{Q}(\xi)[x]$, pero por la demostración anterior tenemos que $\psi(x)$ con $M \geq 6$ es irreducible en $\mathbb{Q}(\xi)[x]$, lo cual es contradictorio. De donde resulta que $\Phi_m(x)$ es irreducible sobre $\mathbb{Q}[x]$. \square

Demostración. **Del teorema 1.3**

Si $M \geq 6$, entonces tomando $Q(x) = 1$, tenemos el teorema 1.3 como corolario del teorema 1.4.

Si $M = 5$, entonces el Grado $\tau_1(x) \leq 2$ y por otro lado

$$2 < a_4 - a_1, \quad a_5 - a_1$$

y a_1, a_4, a_5 (por el lema 1.7) son tres puntos de interpolación adecuados, y por lo tanto el teorema es válido si $M = 5$. \square

Para demostrar el teorema 1.2 necesitamos el lema siguiente.

1.9 Lema. Sean a_1, \dots, a_n enteros racionales si el polinomio

$$K(x) = \prod_{k=1}^M (x - a_k) + 1$$

es irreducible mod 2 o es congruente a una potencia de un polinomio irreducible mod 2, entonces

$$F(x) = \prod_{k=1}^M (x - a_k)^{2^n} + 1$$

es irreducible en $\mathbb{Q}[x]$

Demostración. Supongamos que $F(x)$ es reducible en $\mathbb{Q}[x]$ esto es decir

$$F(x) = G(x) \cdot H(x)$$

Por otro lado

$$\begin{aligned} [K(x)]^{2^n} &\equiv \left[\prod_{k=1}^M (x - a_k)^{2^n} + 1 \right]^{2^n} \pmod{2} \\ &\equiv \prod_{k=1}^M (x - a_k)^{2^n} + 1 \pmod{2} \\ &\equiv F(x) \pmod{2} \end{aligned}$$

Por hipótesis

$$K(x) = \prod_{k=1}^M (x - a_k) + 1 \equiv \psi(x)^r \pmod{2} \quad (r \geq 1), \quad (1.12)$$

Luego

$$F(x) = G(x) \cdot H(x) \equiv [\psi(x)]^{2^n \cdot r} \pmod{2}$$

como el Grado $G(x) > 0$ y Grado $H(x) > 0$ esto es posible si

$$\begin{aligned} G(x) &\equiv \psi(x)^\alpha \pmod{2} & (\alpha > 0), \\ H(x) &\equiv \psi(x)^\beta \pmod{2} & (\beta > 0). \end{aligned}$$

de modo que

$$\left. \begin{aligned} G(x) &= \psi(x)^\alpha + 2A(x) \\ H(x) &= \psi(x)^\beta + 2B(x) \end{aligned} \right\} \quad (\alpha + \beta = 2^n r),$$

donde $A(x), B(x) \in \mathbb{Q}[x]$.

Considerando el producto $G(x) \cdot H(x) \pmod{4}$. Resuelta entonces

$$F(x) \equiv G(x) \cdot H(x) \equiv \psi(x)^{\alpha+\beta} + 2\psi(x)^\beta A(x) + 2\psi(x)^\alpha B(x) \pmod{4}. \quad (1.13)$$

En virtud de (1.12) tenemos

$$\begin{aligned} \prod_{k=1}^M (x - a_k) + 1 &\equiv \psi^r \pmod{2} \\ \prod_{k=1}^M (x - a_k) + 1 &= \psi(x)^r + 2K_1(x) \\ \prod_{k=1}^M (x - a_k) &= \psi(x)^r - 1 + 2K_1(x) \end{aligned}$$

donde $K_1(x)$ es un polinomio sobre \mathbb{Q} .

De la definición de $F(x)$ obtenemos

$$\begin{aligned} F(x) &= \prod_{k=1}^M (x - a_k)^{2^n} + 1 \\ &\equiv (\psi(x)^r - 1 + 2K_1(x))^{2^n} + 1 \\ &\equiv \left(\psi(x)^{r2^n} + 2\psi^{r2^{n-1}} + 1 \right) + 1 \pmod{4} \\ &\equiv \psi(x)^{r2^n} + 2\psi^{r2^{n-1}} + 2 \pmod{4}. \end{aligned} \quad (1.14)$$

De las congruencias en 1.13 y 1.14 tenemos

$$\begin{aligned}\psi(x)^{\alpha+\beta} + 2\psi(x)^\alpha B(x) + 2\psi(x)^\beta A(x) &= \psi(x)^{r^{2^n}} + 2\psi(x)^{r^{2^{n-1}}} + 2 && \text{mod } 4 \\ 2\psi(x)^\beta A(x) + 2\psi(x)^\alpha B(x) - 2\psi(x)^{r^{2^{n-1}}} &\equiv 2 && \text{mod } 4 \\ \psi(x)^\beta A(x) + \psi(x)^\alpha B(x) - \psi(x)^{r^{2^{n-1}}} &\equiv 1 && \text{mod } 2.\end{aligned}$$

Esto es sin embargo imposible, pues el lado izquierdo $\text{mod } 2$ es divisible por $\psi(x)$, mientras que el derecho no lo es. \square

Demostración. Final de la demostración del teorema 1.2.

Del teorema 1.3 en el caso especial de $m = 2^{n+1}$, este teorema resulta para $M \geq 5$. Además en el caso de $M = 1$ es trivial.

Veamos para $M = 4$.

Supongamos $a_k = a_1 + k - 1$ ($k = 1, 2, 3, 4$), son números enteros racionales consecutivos entonces 1.12 se transforma en

$$\begin{aligned}K(x) &= (x - a_1)(x - (a_1 + 1))(x - (a_1 + 2))(x - (a_1 + 3)) + 1 \\ &\equiv (x - a_1)(x - a_1 - 1)(x - a_1)(x - a_1 - 1) + 1 && \text{mod } 2 \\ &\equiv (x - a_1)^2(x - a_1 - 1)^2 + 1 && \text{mod } 2 \\ &\equiv ((x - a_1)(x - a_1 - 1) + 1)^2 && \text{mod } 2 \\ &\equiv (x^2 + x + a_1(a_1 + 1) + 1)^2 && \text{mod } 2 \\ &\equiv (x^2 + x + 1)^2 && \text{mod } 2\end{aligned}$$

Puesto que el polinomio $K(x) = x^2 + x + 1 \text{ mod } 2$ es irreducible, entonces $F(x)$ es irreducible por el lema 1.9.

Ahora si $M = 3$ y $a_k = a_1 + k - 1$ ($k = 1, 2, 3$), entonces

$$\begin{aligned}K(x) &= (x - a_1)(x - (a_1 + 1))(x - (a_1 + 2)) + 1 \\ &\equiv (x - a_1)(x - a_1 - 1)(x - a_1) + 1 && \text{mod } 2 \\ &\equiv (x - a_1)^2(x - a_1 - 1) + 1 && \text{mod } 2\end{aligned}$$

Si $a_1 \equiv 0 \text{ mod } 2$, entonces $x^3 - x^2 + 1$ es irreducible $\text{mod } 2$.

Si $a_1 \equiv 1 \text{ mod } 2$, entonces $x^3 - x + 1$ es irreducible $\text{mod } 2$.

Entonces, $K(x) \equiv (x - a_1)^2(x - a_1 - 1) + 1 \pmod{2}$ es irreducible módulo 2.

Si $M = 2$ y $|a_1 - a_2| \leq 2$, entonces se tiene dos casos

1. Si $a_1 \equiv a_2 \pmod{2}$ con lo cual

$$K(x) \equiv (x - a_1)^2 + 1 \equiv (x - a_1 + 1)^2 \pmod{2}$$

el cuál es irreducible.

2. o bien que $a_1 \equiv a_2 + 1 \pmod{2}$, esto es

$$\begin{aligned} K(x) &\equiv (x - a_1)(x - a_1 - 1) + 1 \\ &\equiv x^2 + x + a_1(a_1 + 1) + 1 \pmod{2} \\ &\equiv x^2 + x + 1 \pmod{2} \end{aligned}$$

que también es irreducible.

De aquí resulta que el teorema 1.2 es válido en todos los otros casos. \checkmark

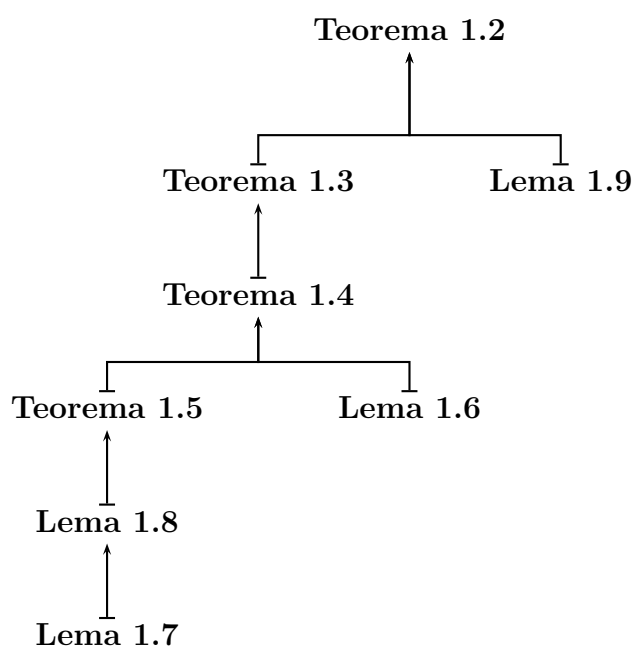


Figura 1.1: Esquema de la demostración

Bibliografía

- [1] BRAUER, A., BRAUER, R. & HOPF, H., *Über Irreduzibilität einiger speziellen Klassen von Polynomen*. Jahresbericht d. Deutschen Math. Ver. **35** (1926), 99–112.
- [2] BRAUER, A. & BRAUER, R., *Über Irreduzibilitätskriterien von I. Schur und G. Pólya*. Math. Zeitschrift. **40** (1936), 242–265.
- [3] CASTRO, I., *Temas de teoría de cuerpos, teoría de anillos y números algebraicos*. Bogotá., Universidad Nacional de Colombia. Tomo. **2** (1986).
- [4] EISENSTEIN, G., *Über die Irreduzibilität und einige andere Eigenschaften der Gleichung, von welcher die theilung der ganzen Lemniscate abhängt*. J. f. reine. u. angew. Math. **39** (1850), 160-182.
- [5] FADDIEEV, D. & SOMINSKI, I., *Problemas de álgebra superior*. Moscú: Mir, (1971).
- [6] FILASETA, M., *Irreducible polynomials*. Notas Mimeografiadas. South Carolina University. (2003).
- [7] FLÜGEL, W., *Lösung der Aufgabe 226*. Archiv Math. Phys. **15** (1909), 271–272.
- [8] FRALEIGH, J., *Álgebra abstracta*. Addison-Wesley Iberoamericana, S.A., E.U.A. (1987).
- [9] HARDY, G., & WRIGHT, E., *An introduction to the theory of numbers*. Oxford Universite press. Quinta edición., (1979).
- [10] HERSTEIN, I. N., *Álgebra moderna*. 2ª edición., Editorial Trillas., México. (1990).
- [11] LANG, S., *Algebra*. 2ª Edición.

- [12] MACLANE, S., & BIRKHOFF, G., *Algebra*. The Macmillan Company. New York., (1967).
- [13] NIVEN, I., & ZUCKERMAN, H., *Introducción a la teoría de números*. Editorial Limusa–Wiley., S. A., México (1969).
- [14] PÓLYA, G. & SZEGÖ, G., *Aufgaben und Lehrsätze der Analysis. II*. Berlin, 1925, 347–350 = *Problems and Theorems in Analysis II*, Berlin: Springer–Verlag, 1976.
- [15] PÓLYA, G., *Verschiedene Bemerkungen zur Zahlentheorie*. Jahresber. d. Deutsch. Math. Ver. 28 (1919), S.66–67.
- [16] SCHÖNEMANN, *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*. J. f. reine. u. angew. Math. **32** (1846), 93–105.
- [17] SCHUR, I., *Aufgabe 226*. Archiv. Math. Phys. **13** (1908), 367.
- [18] SCHUR, I., *Aufgabe 275*. Archiv. Math. Phys. **15** (1909), 259.
- [19] SERES, I., *Lösung und verallgemeinerung eines Schurschen Irreduzibilitätsproblems für Polynome*. Acta Mathematica Academic Scienc Hungar. **VII**, (1956), 151–157.
- [20] SERES, I., *Über die Irreduzibilität gewisser Polynome*. Acta Arithmetica **VIII**. (1963), 321–341.