1
2ej.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

SOLUBILIDAD POR RADICALES: UNA EXPOSICIÓN MODERNA DE RESULTADOS DE ABEL

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

M A T E M Á T I C O

P R E S E N T A:

CARLOS EDUARDO ÁLVAREZ SALAS

DIRECCIÓN GENERAL DE ESTUDIOS PROFESIONALES

DIRECTOR DE TESIS: **DR. FRANCISCO RAGGI CÁRDENAS**
ASESOR DE TESIS: **DR. EMILIO LLUIS RIERA**

FACULTAD DE CIENCIAS
SECCIÓN ESCOLAR

PRIMAVERA 1997

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

VNIVERSIDAD NACIONAL
AVPNOMA DE
MEXICO

M. en C. Virginia Abrín Batule
Jefe de la División de Estudios Profesionales de la
Facultad de Ciencias
P r e s e n t e

Comunicamos a usted que hemos revisado el trabajo de Tesis:

Solubilidad por radicales: Una exposición moderna de resultados de Abel.

realizado por Carlos Eduardo Álvarez Salas

con número de cuenta 8913788-8 , pasante de la carrera de Matemático

Dicho trabajo cuenta con nuestro voto aprobatorio.

Atentamente

Dr. Francisco Raggi Cárdenas
Director de Tesis

Propietario

Dr. Emilio Lluis Riera
Propietario

Dr. José Ríos Montes
Propietario

Dr. Rodolfo San Agustín Chi
Suplente

Dr. Carlos José Enrique Signoret Poillon
Suplente

M.A. Virginia Abrín Batule
Consejo Departamental de Matemáticas

Solubilidad por radicales: Una exposición moderna de resultados de Abel

Carlos Eduardo Álvarez Salas

Director de Tesis
Dr. Francisco Raggi Cárdenas

Asesor de Tesis
Dr. Emilio Lluis Riera

Primavera 1997.

Investigación auspiciada por Fundación UNAM a través de un proyecto apoyado por el Instituto de Matemáticas UNAM.

Contenido

1	**Grupos**	**3**
2	**Anillos.**	**11**
3	**Polinomios.**	**21**
4	**Extensiones de Campos.**	**25**
5	**La insolubilidad de la quíntica.**	**29**

Prefacio

En la antigüedad se encontraron expresiones radicales para las raíces de polinomios de segundo grado, es decir, a partir de los coeficientes del polinomio y aplicando un número finito de operaciones de campo y extracción de raíces se obtenían las soluciones a la ecuación que resulta de igualar el polinomio con cero. En el siglo XVI se encontraron expresiones radicales para las raíces de polinomios de tercero y cuarto grados. A estos descubrimientos siguió un siglo y medio de verdaderos esfuerzos por encontrar expresiones radicales para los polinomios de quinto grado. En 1799, Paolo Ruffini afirma que tal expresión no existe y ofrece una prueba que, aunque no está completa, es un gran descubrimiento; aparentemente, Ruffini tiene razón y sólo falta completar la prueba. Entre 1824 y 1826, el gran matemático noruego Niels Hendrik Abel ofrece una prueba completa de este hecho. Unos cuatro años después, el joven Evariste Galois descubre un criterio de solubilidad por radicales del cual puede obtenerse el resultado de Abel.

Es interesante preguntarse cómo pudo Abel obtener su resultado sin el uso de grupos solubles, aspecto importante en el criterio de Galois; pero es asombroso cómo pudo Galois obtener su criterio cuando ni siquiera había una definición precisa de grupo. En este trabajo, se expone el resultado de Abel haciendo uso de definiciones actuales de conceptos que seguramente él tenía en mente, pero en ningún momento se mencionan grupos solubles, ni siquiera subgrupos normales. En los primeros capítulos se expone una teoría elemental de grupos, anillos y campos; todo lo necesario para llegar al resultado de Abel en el último capítulo. Si usted sólo quiere saber cómo obtener el resultado de Abel con una teoría elemental, puede leer sólo el último capítulo; los primeros capítulos no obstante, contienen resultados y observaciones tan útiles que algunos ejercicios sobre polinomios resultan ser sus consecuencias inmediatas.

Capítulo 1

Grupos

Definición. Un grupo $(G, *)$ es un conjunto G, junto con una operación binaria $*$ en G, tal que satisface los siguientes axiomas:

1) La operación $*$ es asociativa, es decir, $\forall a, b, c \in G\ (a*b)*c = a*(b*c)$.

2) Existe un elemento e en G tal que para cada $a \in G$, $e * a = a$. El elemento e se llama elemento neutro del grupo $(G, *)$.

3) Para cada $a \in G$ existe un elemento $a' \in G$ tal que $a' * a = e$. El elemento a' se llama inverso de a con respecto a $*$.

Notación. Frecuentemente denotaremos al grupo $(G, *)$ simplemente G y $a * b$ simplemente ab, siempre que tengamos claro cuál es la operación $*$. Gracias a la asociatividad, podremos escribir $(ab)c\ [= a(bc)]$ simplemente abc.

Observaciones. 1) La ley de cancelación izquierda es válida en G : Si $ab = ac$, entonces $b = eb = a'ab = a'ac = ec = c$.

2) Para cada $a \in G$, $aa' = e = a'a$, veamos: $aa' = eaa' = (a')'a'aa' = (a')'ea' = (a')'a' = e$.

3) Para cada $a \in G$, $ae = ea$, veamos: $ae = aa'a = ea$.

4) La ley de cancelación derecha también es válida en G, como en 1), usando 2) y 3).

5) Para cada $a \in G$, el inverso a' es único, si $a'a = e$ y $a''a = e$, entonces $a'a = a''a$ así $a' = a''$.

6) El elemento neutro es único, si e_1 es neutro, $e_1 = ee_1 = e_1e = e$.

Notación. El inverso de a se llama a^{-1}. Debido a 2) y 5), $(a^{-1})^{-1} = a$. Si n es un entero positivo, $a^0 = e$, $a^1 = a$ y $a^{n+1} = a^n a$ y $a^{-n} = (a^{-1})^n$.

Con esta notación, tenemos que $a^{m+n} = a^m a^n$, además $a^{-n} = (a^n)^{-1}$.

Ejemplo. Sea $I_n = \{1, \ldots, n\}$ y sea S_n el conjunto de las funciones biyectivas de I_n en él mismo: $S_n = \{\alpha : I_n \longrightarrow I_n : \alpha \text{ es biyectiva}\}$ y definimos la operación en S_n como la composición de funciones : $\forall \alpha, \beta \in S_n, a \in I_n$, $\beta\alpha(a) = \beta(\alpha(a))$. La composición de funciones siempre es asociativa, la función que deja fijos a todos los elementos de I_n es biyectiva y además cualquier función biyectiva tiene inversa, la cual también es biyectiva, así que S_n es un grupo, llamado el grupo de permutaciones de n elementos ó grupo simétrico.

Definición. Sea G un grupo y $H \subseteq G$, H es un subgrupo de G si cumple:
1) Si $a, b \in H$, entonces $ab \in H$.
2) $e \in H$.
3) Si $a \in H$ entonces $a^{-1} \in H$.

Teorema. Sea G un grupo, $\{H_\alpha : \alpha \in J\}$ una familia de subgrupos de G y sea $H = \bigcap_{\alpha \in J} H_\alpha$. Entonces H es un subgrupo de G.

Demostración. Sean $a, b \in H$, así para cada $\alpha \in J$, $a, b \in H_\alpha$, como H_α es subgrupo, para cada $\alpha \in J$ $ab \in H_\alpha$, así que $ab \in H$. Además, para cada $\alpha \in J$, $e \in H_\alpha$, así que $e \in H$. Ahora, si $a \in H$, para cada $\alpha \in J$ tenemos $a \in H_\alpha$ así que para cada $\alpha \in J$ tenemos $a^{-1} \in H_\alpha$ y finalmente $a^{-1} \in H$. Así que H es un subgrupo de G. ■

Ahora, sea G un grupo, $A \neq \phi$ un subconjunto de G y definimos H_A como $H_A = \{a_1^{r_1} a_2^{r_2} \cdots a_s^{r_s} \mid a_i \in A, r_i \in \mathbb{Z}, 1 \leq i \leq s\}$, claramente $A \subseteq H_A$, veamos que H_A es un subgrupo de G :

1) Claro que si $a_1^{r_1} a_2^{r_2} \cdots a_s^{r_s}, b_1^{t_1} b_2^{t_2} \cdots b_u^{t_u} \in H_A$,
entonces $a_1^{r_1} a_2^{r_2} \cdots a_s^{r_s} b_1^{t_1} b_2^{t_2} \cdots b_u^{t_u} \in H_A$.

2) Como $A \neq \phi$, sea $a \in A$, entonces $a^0 = e \in H_A$.

3) Si $a_1^{r_1} a_2^{r_2} \cdots a_s^{r_s} \in H_A$, también $a_s^{-r_s} \cdots a_1^{-r_1} \in H_A$, y
$a_s^{-r_s} \cdots a_1^{-r_1} a_1^{r_1} a_2^{r_2} \cdots a_s^{r_s} = e$, así que H_A es un subgrupo de G.

Además, si H es un subgrupo de G y $A \subseteq H$, entonces $H_A \subseteq H$, pues si
$a_1^{r_1} a_2^{r_2} \cdots a_s^{r_s} \in H_A$ donde $a_i \in A$, entonces $a_i \in H$ y $a_i^{r_i} \in H$,
así que $a_1^{r_1} a_2^{r_2} \cdots a_s^{r_s} \in H$ y $H_A \subseteq H$.
Ahora sea $\Gamma = \{H \mid H \text{ es subgrupo de } G \text{ y } A \subseteq H\}$, por un lado $H_A \in \Gamma$,
así que $\cap\Gamma \subseteq H_A$, por otro lado $\cap\Gamma$ es un subgrupo de G y además $A \subseteq \cap\Gamma$
así que $H_A \subseteq \cap\Gamma$ y entonces $H_A = \cap\Gamma$.
El subgrupo H_A se llama el subgrupo de G generado por A y decimos que A genera al subgrupo H_A .

Veamos a continuación algunas de las propiedades que tiene el grupo simétrico S_n, pues son muy útiles para poder lograr algunos de los teoremas en el último capítulo.

Definición. Sea $\sigma \in S_n$, el soporte de σ es $\sup \sigma = \{k \in I_n \mid \sigma(k) \neq k\}$. Dos permutaciones son ajenas si sus soportes son ajenos.

Definición. Sea $\sigma \in S_n$, si $\sup \sigma = \{a_1, a_2, \ldots, a_r\}$, $\sigma(a_i) = a_{i+1}$ si $1 \leq i < r$, y $\sigma(a_r) = a_1$, entonces σ se llama ciclo de longitud r ó $r - ciclo$, y si $r = 2$, σ se llama transposición.

Notación. El $r - ciclo$ σ se denota $\sigma = (a_1 a_2 \ldots a_r)$, $e = (1)$.

Observaciones. 1) $(a_1 a_2 \ldots a_r) = (a_2 a_3 \ldots a_r a_1)$.

Si $\sigma, \tau \in S_n$,

2) $a \in \sup \sigma \Leftrightarrow \sigma(a) \in \sup \sigma^{-1}$, pues
$a \in \sup \sigma \Leftrightarrow \sigma(a) \neq a \Leftrightarrow \sigma(a) \neq \sigma^{-1}\sigma(a) \Leftrightarrow \sigma(a) \in \sup \sigma^{-1}$.

3) $a \in \sup \sigma \Leftrightarrow \sigma(a) \in \sup \sigma$, pues
$a \in \sup \sigma \Leftrightarrow \sigma(a) \neq a \Leftrightarrow \sigma(\sigma(a)) \neq \sigma(a)$ pues σ es una función inyectiva,
y $\sigma(\sigma(a)) \neq \sigma(a) \Leftrightarrow \sigma(a) \in \sup \sigma$.

4) Usando 2) y 3), tenemos que $\sup \sigma = \sup \sigma^{-1}$.

5) Si σ y τ son ajenas, $a \in \sup \tau \Leftrightarrow \sigma(a) \in \sup \tau$, pues si $a \in \sup \tau$,
entonces $a \notin \sup \sigma$, así que $a = \sigma(a) \in \sup \tau$; ahora, si $\sigma(a) \in \sup \tau$,
entonces $\sigma(a) \notin \sup \sigma$ así que $a \notin \sup \sigma$ y $\sigma(a) = a \in \sup \tau$.

6) Si σ, τ son ajenas, y si $a \in \sup \sigma$, entonces $a \notin \sup \tau$, y por 5),
$\sigma(a) \notin \sup \tau$ de manera que $\sigma\tau(a) = \sigma(a) = \tau\sigma(a)$,
análogamente si $a \in \sup \tau$, $\tau\sigma(a) = \tau(a) = \sigma\tau(a)$; y si $a \notin \sup \sigma \cup \sup \tau$,
entonces $\sigma\tau(a) = \sigma(a) = a = \tau(a) = \tau\sigma(a)$.
Así obtenemos que $\sigma\tau = \tau\sigma$ y $\sup \sigma\tau = \sup \sigma \cup \sup \tau$.

Después de estas observaciones, estamos listos para el primer gran teorema acerca del grupo simétrico S_n y los ciclos ajenos:

Teorema. Toda permutación es el producto de ciclos ajenos, más aún, la factorización en ciclos ajenos de cada permutación es única salvo el orden (suponiendo que no aparecen ciclos triviales).

Demostración. Sea $\sigma \in S_n$, por el segundo principio de inducción sobre el número de elementos de $\sup \sigma$, si $\sup \sigma = \phi$, $\sigma = e = (1)$.
Ahora, sea $\sigma \neq e$, así $\sup \sigma \neq \phi$. Sea $k \in \sup \sigma$, notamos que
$k, \sigma(k), \sigma^2(k), \ldots, \sigma^n(k)$ son $n + 1$ elementos de I_n, así que debe haber al menos dos iguales. Así, entendiendo k como $k = \sigma^0(k)$, tenemos que
$\sigma^i(k) = \sigma^j(k)$ con $0 \leq i < j \leq n$, así que $\sigma^{j-i}(k) = k$ con $j - i$ un entero positivo, entonces hay un mínimo entero positivo l tal que $\sigma^l(k) = k$,

$l > 1$ pues $k \in \sup\sigma$. Sea τ el $l-ciclo$ $\tau = (k\,\sigma(k)\ldots\sigma^{l-1}(k))$, recordando la observación 4), $\sup\tau = \sup\tau^{-1}$ y observamos que: si $r \notin \sup\tau$, $\sigma\tau^{-1}(r) = \sigma(r)$, y si $r \in \sup\tau$, $\sigma\tau^{-1}(r) = r$, por la construcción de τ. Así que sea $\eta = \sigma\tau^{-1}$, así $\eta\tau = \sigma$ además $\sup\eta \subseteq \sup\sigma$, y dado que $k \in \sup\tau$, $k \notin \sup\eta$ pero $k \in \sup\sigma$, así que la inclusión es propia y por la hipótesis de inducción tenemos $\eta = \tau_1\tau_2\cdots\tau_s$ donde τ_i es un ciclo para $1 \leq i \leq s$ con τ_i y τ_j ajenos si $i \neq j$, hemos visto también que si $r \in \sup\tau$, entonces $r \notin \sup\eta$ así que τ y η son ajenas, por la observación 6), $\sup\eta = \bigcup_{i=1}^{s} \sup\tau_i$, así que para cada $1 \leq i \leq s$, τ y τ_i son ajenos y $\sigma = \tau_1\tau_2\cdots\tau_s\tau$.

Veamos que la factorización en ciclos ajenos es única (salvo el orden) por inducción sobre el número de ciclos en alguna factorización. Sea $\sigma = \tau_1\tau_2\cdots\tau_s$ producto de ciclos ajenos, así que $\sup\sigma = \bigcup_{i=1}^{s} \sup\tau_i$. Si $\sigma = e$, dado que $\sup e = \phi$, cada τ_i es un ciclo trivial. Ahora supongamos que $\sigma \neq e$, $\sigma = \sigma_1\sigma_2\cdots\sigma_r$ el producto de ciclos ajenos no triviales, digamos que σ_1 es un $l-ciclo$ $\sigma_1 = (a_1\ldots a_l)$, así que para algún i, $a_1 \in \sup\tau_i$, sin perder generalidad podemos suponer que $a_1 \in \sup\tau_1$, usando las observaciones 3) y 6) tenemos que $a_1, \ldots, a_l \in \sup\tau_1$, y por la observación 6), $\tau_1(a_i) = \sigma(a_i) = \sigma_1(a_i)$ así que $\sigma_1 = \tau_1$ y $\sigma_2\cdots\sigma_r = \tau_2\cdots\tau_s$, y por la hipótesis de inducción tenemos que $r-1 = s-1$ y $\{\sigma_2, \ldots, \sigma_r\} = \{\tau_2, \ldots, \tau_s\}$ y de aquí que $r = s$ y $\{\sigma_1, \ldots, \sigma_r\} = \{\tau_1, \ldots, \tau_s\}$. ■

Ahora, cualquier ciclo es producto de transposiciones:
$(a_1\ldots a_r) = (a_1a_r)\cdots(a_1a_3)(a_1a_2)$, así que un $r-ciclo$ es el producto de $r-1$ transposiciones, de aquí que si $\alpha \in S_n$ es el producto de ciclos ajenos $\alpha = (i_1i_2\ldots i_r)(j_1j_2\ldots j_s)\cdots(l_1l_2\ldots l_u)$ entonces α es el producto de $(r-1)+(s-1)+\cdots+(u-1)$ transposiciones. Hemos probado el siguiente

Corolario. *S_n está generado por transposiciones.* ■

Sabemos que $(ab)^{-1} = (ab)$ y cada elemento de S_n es producto de transposiciones, pero la expresión como producto de transposiciones no es única, ni siquiera el número de transposiciones, por ejemplo
$(123) = (13)(12) = (12)(23) = (13)(23)(12)(13)$. Sabemos que $\alpha \in S_n$ tiene una descomposición en ciclos ajenos $\alpha = (i_1i_2\ldots i_r)(j_1j_2\ldots j_s)\cdots(l_1l_2\ldots l_u)$ y es única, de allí se obtiene una expresión como el producto de $(r-1)+(s-1)+\cdots+(u-1)$ transposiciones, este número de transposiciones sólo depende de la descomposición en ciclos ajenos de α, la cual es única, así que podemos definir
$N(\alpha) = (r-1)+(s-1)+\cdots+(u-1)$ y $N(e) = N(1) = 0$. Ahora tenemos

unas

Observaciones. Si $\sigma \in S_n$, $\sigma = \sigma_1\sigma_2 \cdots \sigma_s$ el producto de ciclos ajenos, y $(ab) \in S_n$,

1) Si (ab) y σ son ajenas, $(ab)\sigma = (ab)\sigma_1\sigma_2 \cdots \sigma_s$ es un producto de ciclos ajenos y $N((ab)\sigma) = N(\sigma) + 1$.

2) Si $a \in \sup\sigma$ y $b \notin \sup\sigma$, supongamos que $a \in \sup\sigma_1$ y $\sigma_1 = (ac_1 \ldots c_h)$, así $(ab)\sigma_1 = (ac_1 \ldots c_h b)$ y $(ab)\sigma = (ac_1 \ldots c_h b)\sigma_2 \cdots \sigma_s$ es un producto de ciclos ajenos, de donde $N((ab)\sigma) = N(\sigma) + 1$.

3) Si $a, b \in \sup\sigma_1$, $\sigma_1 = (ac_1 \ldots c_h b d_1 \ldots d_k)$ y entonces
$(ab)\sigma_1 = (ac_1 \ldots c_h)(bd_1 \ldots d_k)$, obteniendo que
$(ab)\sigma = (ac_1 \ldots c_h)(bd_1 \ldots d_k)\sigma_2 \ldots \sigma_s$ es un producto de ciclos ajenos y $N((ab)\sigma) = N(\sigma) - 1$.

4) Si $a \in \sup\sigma_1, b \in \sup\sigma_2$, $\sigma_1 = (ac_1 \ldots c_h)$ y $\sigma_2 = (bd_1 \ldots d_k)$, así que $(ab)\sigma_1\sigma_2 = (ac_1 \ldots c_h b d_1 \ldots d_k)$ y $(ab)\sigma = (ac_1 \ldots c_h b d_1 \ldots d_k)\sigma_3 \ldots \sigma_s$ es un producto de ciclos ajenos, de donde $N((ab)\sigma) = N(\sigma) + 1$.

Nuevamente estamos listos para un gran teorema, pues tendrá consecuencias muy útiles.

Teorema. Sea $\alpha \in S_n$. Si $N(\alpha)$ es par, cualquier descomposición de α en transposiciones tiene un número par de ellas; si $N(\alpha)$ es impar, cualquier descomposición de α en transposiciones tiene un número impar de ellas.

Demostración. Sea $\alpha \in S_n$, $\alpha = \tau_1 \cdots \tau_r$ producto de r transposiciones, como $N(e) = 0$ entonces, por las últimas observaciones, $N(\alpha) = \sum_{i=1}^{r} \varepsilon_i$ donde $\varepsilon_i = \pm 1$, si hacemos $\delta_i = \varepsilon_i$ si $\varepsilon_i = 1$ y $\delta_i = \varepsilon_i + 2$ si $\varepsilon_i = -1$, entonces $\delta_i = 1$ para cada $1 \leq i \leq r$, así $\sum_{i=1}^{r} \delta_i = r$ es par sí y sólo sí $N(\alpha) = \sum_{i=1}^{r} \varepsilon_i$ es par, y r es impar sí y sólo sí $N(\alpha)$ es impar. ■

Definición. Sea $\alpha \in S_n$. Decimos que α es par si $N(\alpha)$ es par, y α es impar si $N(\alpha)$ es impar. $A_n = \{\alpha \in S_n \mid \alpha \text{ es par}\}$.

Así que los elementos de A_n son las permutaciones que pueden expresarse como producto de un número par de transposiciones. Ahora, si $\alpha, \beta \in A_n$, $\alpha = \alpha_1 \cdots \alpha_{2r}$ y $\beta = \beta_1 \cdots \beta_{2s}$ con α_i, β_i transposiciones, entonces $\alpha\beta = \alpha_1 \cdots \alpha_{2r}\beta_1 \cdots \beta_{2s}$ es el producto de $2(r+s)$ transposiciones, así que $\alpha\beta \in A_n$, $e = (12)(12) \in A_n$, y si hacemos $\gamma = \alpha_{2r} \cdots \alpha_1$, $\gamma \in A_n$ y $\gamma\alpha = e$, así que $\gamma = \alpha^{-1} \in A_n$; en otras palabras, A_n es un subgrupo de S_n.

Teorema. Si $n \geq 3$, A_n está generado por los $3-$*ciclos*.

Demostración. Sea (abc) un $3-ciclo$, $(abc)=(ac)(ab)\in A_n$, así que el subgrupo generado por los $3-ciclos$ es un subconjunto de A_n. Veamos que el producto de 2 transposiciones también es producto de $3-ciclos$: si son iguales, $(ab)(ab)=(123)(123)(123)$, si sus soportes tienen un elemento en común, $(ab)(ac)=(acb)$, si son ajenas, $(ab)(cd)=(acb)(acd)$. Ahora sea $\tau\in A_n$, $\tau=\tau_1\tau_2\cdots\tau_{2r}$, podemos tomar $\tau_1\tau_2,\tau_3\tau_4,\ldots,\tau_{2r-1}\tau_{2r}$ y substituir la igualdad adecuada de las 3 anteriores obteniendo así a τ como producto de $3-ciclos$, de aquí que el subgrupo A_n está generado por los $3-ciclos$. ■

Teorema. Si m es un número impar tal que $3\leq m\leq n$, entonces A_n está generado por los $m-ciclos$.

Demostración. Sea m un número impar tal que $3\leq m\leq n$, un $m-ciclo$ es producto de $m-1$ transposiciones,
$(a_1a_2\ldots a_m)=(a_1a_m)\cdots(a_1a_3)(a_1a_2)\in A_n$, así que el subgrupo generado por los $m-ciclos$ es un subconjunto de A_n.

Ahora, $(a_1a_2a_3)=(a_2a_1a_3a_4\ldots a_m)(a_ma_{m-1}\ldots a_4a_3a_2a_1)$ y usando el teorema anterior tenemos que si $\tau\in A_n$, τ es producto de $m-ciclos$. Así que el subgrupo A_n está generado por los $m-ciclos$. ■

Esto es todo lo que necesitamos del grupo simétrico S_n y su subgrupo A_n, particularmente este último teorema tendrá un uso asombroso en el último capítulo, yo diría que este es el ensamble entre el trabajo de Abel y la explicación moderna de su resultado. Veamos ahora otra de las herramientas poderosas de los grupos.

Definición. Sea G un grupo y sea X un conjunto, una acción de G en X es una función $T:G\times X\to X$ tal que:

1) Para cada $s\in X$, $T(e,s)=s$.

2) Para cada $s\in X$, y para cada $g_1,g_2\in G$, $T(g_1g_2,s)=T(g_1,T(g_2,s))$.

Observación. Si tenemos una acción T de G en X y para cada $g\in G$ definimos $T_g:X\to X$ tal que para cada $s\in X$, $T_g(s)=T(g,s)$, tenemos que $T_e=Id_X$, y para cada $g_1,g_2\in G$, $T_{g_1g_2}=T_{g_1}\circ T_{g_2}$, pues sea $s\in X$,

$$\begin{aligned}T_{g_1g_2}(s)&=T(g_1g_2,s)\\&=T(g_1,T(g_2,s))=T(g_1,T_{g_2}(s))=T_{g_1}(T_{g_2}(s))=T_{g_1}\circ T_{g_2}(s).\end{aligned}$$

Ahora, si tenemos un grupo G y un conjunto X, y para cada elemento $g\in G$ tenemos una función $T_g:X\to X$ tal que: $T_e=Id_X$ y para cada $g_1,g_2\in G$, $T_{g_1g_2}=T_{g_1}\circ T_{g_2}$ y definimos una función $T:G\times X\to X$ tal que para cada $g\in G$ y para cada $s\in X$, $T(g,s)=T_g(s)$, entonces T es una acción de G en X : pues sea $s\in X$, y $g_1,g_2\in G$, $T(e,s)=T_e(s)=Id_X(s)=s$, y $T(g_1g_2,s)=T_{g_1g_2}(s)=T_{g_1}\circ T_{g_2}(s)=T_{g_1}(T_{g_2}(s))=T(g_1,T(g_2,s))$. Así que

una acción de un grupo G en un conjunto X transforma cada elemento de G en una función de X en él mismo, además cada una tiene inversa, pues $T_g \circ T_{g^{-1}} = T_{g^{-1}} \circ T_g = T_e = Id_X$ y por tanto cada T_g es biyectiva.

Teorema. Sea G un grupo, X un conjunto y $T : G \times X \longrightarrow X$ una acción de G en X. El conjunto $G_s = \{g \in G \mid T(g,s) = s\}$ es un subgrupo de G para cada $s \in X$.

Demostración. Sea $s \in X$, si $g_1, g_2 \in G_s$,
$T(g_1g_2, s) = T(g_1, T(g_2, s)) = T(g_1, s) = s$, así que $g_1g_2 \in G_s$. $T(e,s) = s$, así que $e \in G_s$. Ahora, si $g \in G_s$,
$T(g^{-1}, s) = T(g^{-1}, T(g,s)) = T(g^{-1}g, s) = T(e,s) = s$, así que $g^{-1} \in G_s$. De aquí que G_s es un subgrupo de G. ■

Definición. El subgrupo $G_s = \{g \in G \mid T(g,s) = s\}$ se llama el subgrupo de isotropía de s.

Corolario. Si $A \subseteq X$, $G_A = \{g \in G \mid \text{para cada } s \in A, T(g,s) = s\}$ es un subgrupo de G.

Demostración. $G_A = \bigcap_{s \in A} G_s$. ■

Definición. Sean G, G' dos grupos, un homomorfismo de G en G' es una función $f : G \longrightarrow G'$ tal que para cada $a, b \in G$, $f(ab) = f(a)f(b)$. Si f es inyectiva, se llama monomorfismo. Si f es suprayectiva, se llama epimorfismo. Si f es biyectiva, se llama isomorfismo.

Observaciones. Si $f : G \longrightarrow G'$ es un homomorfismo de grupos,

1) Si e es el elemento neutro de G y e' el elemento neutro de G', entonces $e'f(e) = f(e) = f(ee) = f(e)f(e)$, así que $e' = f(e)$.

2) Si $a \in G$, $f(a^{-1})f(a) = f(a^{-1}a) = f(e) = e'$, así que $f(a)^{-1} = f(a^{-1})$.

Definición. Un grupo G es abeliano si su operación es conmutativa.

Notación. Cuando G es abeliano, denotamos $+$ a la operación, $-a$ el inverso de a, y $a - b = a + (-b)$.

Sea G un grupo abeliano y H un subgrupo de G, definimos una relación $\sim$ entre los elementos de G de la siguiente manera: $a \sim b$ si y solamente si $a - b \in H$. Esta relación es de equivalencia: Sean $a, b, c \in G$. Tenemos $a - a = e \in H$ así que $a \sim a$. Si $a \sim b$, $a - b \in H$ así que $-(a - b) \in H$, además $a - b + b - a = e$ así que $-(a - b) = b - a \in H$, de donde $b \sim a$. Si $a \sim b$ y $b \sim c$, $a - b \in H$ y $b - c \in H$, así que $a - b + b - c = a - c \in H$ y entonces $a \sim c$.

Notación. Para cada $b \in G$, $H + b = \{h + b \mid h \in H\}$.

Observaciones. 1) La clase de equivalencia de b es $H+b$: Sea $a \in G$. Si $a \in H+b$, $a = h+b$ para algún $h \in H$ y $a-b = h+b-b = h \in H$ de donde $a \sim b$. Si $a \sim b$, entonces $a-b \in H$, así que $(a-b)+b = a \in H+b$.

2) Debido a la conmutatividad de $+$ en G, $H+b = b+H$. Así que, $a+H = b+H$ si y solamente si $a \sim b$.

3) Si $a_1+H = a+H$ y $b_1+H = b+H$, entonces $(a_1+b_1)+H = (a+b)+H$, pues $a_1+b_1-(a+b) = a_1+b_1-b-a = (a_1-a)+(b_1-b) \in H$.

Si ahora definimos $G/H = \{a+H \mid a \in G\}$ el conjunto de clases de equivalencia de $\sim$ y definimos una operación en G/H inducida por la operación de G de la siguiente manera: para cada $a+H, b+H \in G/H$, $(a+H)+(b+H) = (a+b)+H$. La observación 3) nos asegura que la operación de G/H está bien definida.

Teorema. Sea G un grupo abeliano y H un subgrupo de G, G/H con la operación inducida por la de G es un grupo. Más aún, $f : G \longrightarrow G/H$ tal que para cada $a \in G$, $f(a) = a+H$ es un homomorfismo de grupos.

Demostración. Las propiedades de grupo de G/H son debidas a las propiedades de grupo de G, verifiquemos que f es un homomorfismo: sean $a, b \in G$, $f(a+b) = (a+b)+H = (a+H)+(b+H) = f(a)+f(b)$. ■

Observación. Dado que el grupo G es abeliano, G/H también es abeliano.

Capítulo 2

Anillos.

Definición. Un anillo conmutativo y con unitario es un conjunto A junto con dos operaciones binarias $+$ (llamada suma) y $\cdot$ (llamada producto) en A tales que:
1. $\langle A, + \rangle$ es un grupo abeliano. Tal grupo se llama el grupo aditivo del anillo, y el neutro se denota 0 y se llama cero.
2. La operación $\cdot$ es asociativa y conmutativa.
3. Se satisface la ley distributiva $a \cdot (b + c) = a \cdot b + a \cdot c$ para todos los $a, b, c \in A$.
4. Existe un elemento $1 \in A$ neutro para el producto.

Observaciones.
1. El elemento neutro del producto es único y se llama el unitario de A.
2. $\forall a \in A$, $a \cdot 0 = 0$ y $(-1) \cdot a = -a$.
3. Si A es un anillo donde $1 = 0$, entonces $A = \{0\}$ pues si $a \in A$, $a = a \cdot 1 = a \cdot 0 = 0$.

De ahora en adelante, estudiaremos solamente anillos donde $1 \neq 0$ y conmutativos con unitario.

Definición. Sea A un anillo, $I \subseteq A$ y $a \in A$:
1. a es un divisor de cero si existe $b \in A$, $b \neq 0$ tal que $ab = 0$.
2. a es una unidad si existe un $b \in A$ tal que $ab = 1$.
3. A es un dominio entero si el único divisor de cero es el mismo cero, es decir, $ab = 0 \Rightarrow (a = 0 \text{ ó } b = 0)$.
4. A es un campo si cada elemento distinto de cero es una unidad, es decir, $\langle A - \{0\}, \cdot \rangle$ es un grupo.

5. I es un ideal de A si I es subgrupo del grupo aditivo de A y $\forall b \in A, \forall c \in I(bc \in I)$, es decir, $AI \subseteq I$.
6. El ideal I es *primo* si $I \neq A$ y $\forall a, b \in A(ab \in I \Rightarrow (a \in I \text{ ó } b \in I))$.
7. El ideal I es *máximo* si $I \neq A$ y para cualquier J ideal de A, $I \subseteq J \subseteq A \Rightarrow (I = J \text{ ó } J = A)$.

Observaciones.

1. La intersección de una familia de ideales es un ideal.
2. Si $B \subseteq A$, entonces $\cap\{I : I \text{ es ideal de } A \text{ y } B \subseteq I\}$ $= \{a_1b_1 + \cdots + a_rb_r : a_1, \ldots, a_r \in A, b_1, \ldots, b_r \in B\}$ además de ser un ideal.

Notación. Tal ideal se llama el ideal generado por B y se denota $\langle B \rangle$.

4. Si A es un anillo, I un ideal de A, tenemos que $1 \in I$ si y solamente si $I = A$.
3. Cero no es unidad y el producto de dos unidades es una unidad. Así que un campo también es un dominio entero.

Ahora, sea A un anillo, I un ideal de A, al formar el grupo abeliano cociente A/I, tenemos la siguiente

Observación. Si $r+I = r_1+I$ y $s+I = s_1+I$ entonces $rs+I = r_1s_1+I$ pues $rs - r_1s_1 = rs - rs_1 + rs_1 - r_1s_1 = r(s - s_1) + (r - r_1)s_1 \in I$ dado que $s - s_1 \in I$ y $r - r_1 \in I$.

Así que podemos definir una operación producto en A/I como: $\forall a, b \in A, (a + I)(b + I) = ab + I$, dando a A/I una estructura de anillo conmutativo con elemento unitario $1 + I$.

Teorema 1. Sea A un anillo conmutativo y con unitario, $I \neq A$ un ideal de A.

i) A/I es un dominio entero$\Leftrightarrow$ I es un ideal primo.

ii) A/I es un campo $\Leftrightarrow$ I es un ideal máximo.

Demostración. *i)* $\Rightarrow$⌋ Supongamos que A/I es un dominio entero, sean $a, b \in A$. Si $ab \in I$, $(a + I)(b + I) = ab + I = I$ así que $a + I = I$ ó $b + I = I$ y entonces $a \in I$ ó $b \in I$ así que I es un ideal primo.

$\Leftarrow$⌋ Supongamos que I es un ideal primo, sean $a + I, b + I$ tales que $(a + I)(b + I) = 0 + I = I$ así, $ab \in I$ de donde $a \in I$ ó $b \in I$ y de aquí que $a + I = I$ ó $b + I = I$.

ii) $\Rightarrow$⌋ Supongamos que A/I es campo, y sea J un ideal tal que $I \subset J$, $I \neq J$ así $\exists a \in J$ tal que $a \notin I$, entonces $a + I \neq I$ y $\exists b \in A$ tal que $(a+I)(b+I) = 1+I$ y así $1-ab \in I \subset J$. Dado que $a \in J$, $1-ab+ab = 1 \in J$ así que $J = A$.

$\Leftarrow\rfloor$ Supongamos que I es un ideal máximo, y sea $a + I \neq I$, así que $a \notin I$. Ahora, $\langle I, a\rangle = \{b + ac \mid b \in I, c \in A\}$ es el ideal generado por $I \cup \{a\}$, $I \subset \langle I, a\rangle$ pero $I \neq \langle I, a\rangle$ entonces $\langle I, a\rangle = A$ así que $1 = b + ac$ para algunos $b \in I, c \in A$ y $1 - ac = b \in I$, así $1 + I = ac + I = (a + I)(c + I)$ y A/I es un campo. ■

Corolario 2. Si I es un ideal máximo, entonces I es un ideal primo. ■

En cuanto al inverso de este corolorio, el anillo $\mathbb{Z}$ es un dominio entero de donde el ideal $I = \{0\}$ es primo; pero dado que $\mathbb{Z}$ no es campo, I no es un ideal máximo.

Definición. Sea D un dominio entero, I un ideal de D :

Si existe $a \in D$ tal que $I = \langle a\rangle$, I se llama ideal principal.

Si todos los ideales de D son principales, D se llama Dominio de Ideales Principales (DIP).

Si $a, b \in D$ y existe $c \in D$ tal que $b = ac$ entonces a divide a b.

Notación. a divide a b se denota $a \mid b$.

Definición. Sea D un dominio entero, $p \in D$, $p \neq 0$ y p no unidad,

p es primo si: $\forall a, b \in D$, $p \mid ab \Rightarrow p \mid a$ ó $p \mid b$.

p es irreducible si: $\forall a, b \in D$, $p = ab \Rightarrow a$ es unidad ó b es unidad.

Observaciones. 1. Si p es primo y $p \mid a_1 a_2 \cdots a_r$ entonces $p \mid a_i$ para algún $1 \leq i \leq r$.

2. Si p es primo, p es irreducible: Si $p = ab$, $p \mid ab$ y de allí que $p \mid a$ ó $p \mid b$. Supongamos que $p \mid a$, así $\exists c \in D$ tal que $pc = a$, así $pcb = ab = p$. Dado que D es dominio entero, $cb = 1$ y b es unidad.

Teorema 3. Sea D un dominio entero, $p \in D$.

i) p es primo $\Leftrightarrow p \neq 0$ y $\langle p\rangle$ es un ideal primo.

ii) Si D es un DIP, p es irreducible$\Leftrightarrow p \neq 0$ y $\langle p\rangle$ es un ideal máximo.

Demostración. *i)* $\Rightarrow\rfloor$ Si p es primo, $p \neq 0$; como p no es unidad, $\langle p\rangle \neq D$ pues $1 \notin \langle p\rangle$. Ahora, si $ab \in \langle p\rangle$, $p \mid ab$ y así $p \mid a$ ó $p \mid b$ y entonces $a \in \langle p\rangle$ ó $b \in \langle p\rangle$.

$\Leftarrow\rfloor$ $p \neq 0$ y p no es unidad pues $\langle p\rangle \neq D$. Ahora, si $p \mid ab$, $ab \in \langle p\rangle$ así que $a \in \langle p\rangle$ ó $b \in \langle p\rangle$ y entonces $p \mid a$ ó $p \mid b$.

ii) $\Rightarrow\rfloor$ Si p es irreducible, $p \neq 0$ y $\langle p\rangle \neq D$ pues p no es unidad. Ahora, si $\langle p\rangle \subseteq \langle a\rangle \subseteq D$, $p \in \langle a\rangle$ así que $p = ab$ con $b \in D$, entonces a es unidad ó b es unidad

—Si a es unidad, $1 \in \langle a\rangle$ y $\langle a\rangle = D$.

⇒ Si b es unidad, $\exists c \in D$ tal que $bc = 1$, así $pc = abc = a \cdot 1 = a$ de donde $a \in \langle p \rangle$ y $\langle a \rangle \subseteq \langle p \rangle$ así que $\langle p \rangle = \langle a \rangle$. De esta manera, $\langle p \rangle$ es un ideal máximo.

⇐ Supongamos que $p \neq 0$ y $\langle p \rangle$ es un ideal máximo, así que por el corolario anterior $p \neq 0$ y $\langle p \rangle$ es un ideal primo, y por $i)$ tenemos que p es primo, y por la observación 2., p es irreducible. ■

Corolario 4. Si D es un DIP, cada elemento irreducible es primo y cada ideal primo diferente de cero es máximo. ■

Este corolario, a pesar de no ser un inverso para el Corolario 2, nos proporciona condiciones bajo las cuales un ideal primo es también un ideal máximo.

Definición. Una valuación euclidiana en un dominio entero D es una función v que transforma a los elementos distintos de cero de D, en los enteros no negativos tal que satisface las siguientes condiciones:
1. Para todos los $a, b \in D$ con $b \neq 0$ existen q y r en D tales que $a = bq + r$, donde $r = 0$ ó $v(r) < v(b)$.
2. Para todos los $a, b \in D$, donde ni a ni b es cero, $v(a) \leq v(ab)$.

Si existe una valuación euclidiana en D, decimos que D es un dominio euclidiano.

Teorema 5. Todo dominio euclidiano es un DIP.

Demostración. Sea D un dominio euclidiano y sea I un ideal de D,
Si $I = \{0\}$, $I = \langle 0 \rangle$.
Si $I \neq \{0\}$, $I \setminus \{0\} \neq \emptyset$ y el conjunto de valores que toma la valuación euclidiana en $I \setminus \{0\}$ tiene mínimo. Sea $b \in I$, $b \neq 0$ un elemento que tome ese valor mínimo. Veamos que $\langle b \rangle = I$.

Es claro que $\langle b \rangle \subseteq I$. Ahora, sea $a \in I$, como D es euclidiano, existen $q, r \in D$ tales que $a = bq + r$ donde $v(r) < v(b)$ ó $r = 0$, además $a - bq = r \in I$ así que $v(b) \leq v(r)$ ó $r = 0$; de allí que $r = 0$ y $a \in \langle b \rangle$, así $I \subseteq \langle b \rangle$ y entonces $\langle b \rangle = I$ y D es un DIP. ■

Teorema 6. Sea D un dominio euclidiano, $a, b, u \in D$, $a \neq 0, b \neq 0$.
$i)$ Si $\langle a \rangle \subseteq \langle b \rangle$, entonces $v(b) \leq v(a)$ y si $\langle a \rangle = \langle b \rangle$ entonces $v(a) = v(b)$.
$ii)$ Si u es una unidad, entonces $\forall c \in D$ $c \neq 0$, $v(u) \leq v(c)$.
$iii)$ u es una unidad $\Leftrightarrow$ $u \neq 0$ y $v(u) = v(1)$.

Demostración. $i)$ Si $\langle a \rangle \subseteq \langle b \rangle$, $a \in \langle b \rangle$ así $a = bc$ y $v(b) \leq v(bc) = v(a)$. Si $\langle a \rangle = \langle b \rangle$, $\langle a \rangle \subseteq \langle b \rangle$ y $\langle b \rangle \subseteq \langle a \rangle$, así $v(b) \leq v(a)$ y $v(a) \leq v(b)$, se sigue que $v(a) = v(b)$.

ii) Si u es unidad, $1 \in \langle u \rangle$ y $D = \langle u \rangle$, así $\langle c \rangle \subseteq \langle u \rangle$ y por $i)$, $v(u) \leq v(c)$.

iii) $\Rightarrow\rfloor$ Si u es unidad, $u \neq 0$ y $\langle u \rangle = D = \langle 1 \rangle$ así por $i)$, $v(u) = v(1)$.

$\Leftarrow\rfloor$ Dado que $u \neq 0$, existen $q, r \in D$ tales que $1 = uq + r$ con $r = 0$ ó $v(r) < v(u)$, pero 1 es unidad, así que si $r \neq 0$, $v(u) = v(1) \leq v(r)$ de aquí que $r = 0$ y u es una unidad. ■

Teorema 7. Sea D un dominio euclidiano y sea $I \neq \{0\}$ un ideal de D. $I = \langle a \rangle$ con $a \in D$, $a \neq 0$ y para cualquier elemento $b + I \in D/I$ tal que $b \notin I$ existe $b_0 \in b + I$ tal que $v(b_0) < v(a)$.

Demostración. Como D es euclidiano, D es un DIP, $I = \langle a \rangle$, como $I \neq \{0\}$, $a \neq 0$ así que existen $q, r \in D$ tales que $b = aq + r$ con $r = 0$ ó $v(r) < v(a)$, $b - aq = r \in b + I$ pero $0 \notin b + I$ pues $b \notin I$ así que $r \neq 0$ y $v(r) < v(a)$, así $r = b_0$. ■

Si D es un dominio euclidiano y $a = bc$, $a \neq 0$ entonces $v(b) \leq v(bc) = v(a)$. Más aún,

Teorema 8. Sea D un dominio euclidiano, $a \in D$, $a \neq 0$.

i) Si $a = bc$, entonces $v(b) < v(a) \Leftrightarrow c$ no es unidad.

ii) a no es irreducible $\Leftrightarrow \exists b, c \in D$ tales que $a = bc$ donde $v(b) < v(a)$ y $v(c) < v(a)$.

Demostración. *i)* $\Rightarrow\rfloor$ Por contrapositiva, si c es unidad, $\exists d \in D$ tal que $cd = 1$, así $ad = bcd = b$ y $v(a) \leq v(ad) = v(b)$ y entonces $v(a) = v(b)$.

$\Leftarrow\rfloor$ Dado que $a \neq 0$, existen $q, r \in D$ tales que $b = aq + r$ con $v(r) < v(a)$ ó $r = 0$, ahora como $b - aq = r$ y $a = bc$, $r = b - bcq = b(1 - cq)$, $b \neq 0$ y dado que c no es unidad, $1 - cq \neq 0$ así que $r \neq 0$ y $v(b) \leq v(b(1 - cq)) = v(r) < v(a)$, y $v(b) < v(a)$.

ii) $\Rightarrow\rfloor$ Como a no es irreducible, $a = bc$ donde ni b ni c es unidad, por $i)$ tenemos que $v(c) < v(a)$ y $v(b) < v(a)$.

$\Leftarrow\rfloor$ Si $a = bc$ con $v(b) < v(a)$ y $v(c) < v(a)$, por $i)$ tenemos que b no es unidad y c no es unidad, entonces a no es irreducible. ■

Definición. Un dominio entero D es un Dominio de Factorización Única (DFU) si se satisfacen las siguientes condiciones:

i) Todo elemento de D que no sea cero ni unidad es producto de elementos irreducibles.

ii) Para cada $a \in D$, si $a = p_1 \cdots p_r = q_1 \cdots q_s$ con p_i, q_j irreducibles, entonces $r = s$ y los q_j pueden ser renumerados de tal manera que existen unidades $u_1, \ldots, u_r \in D$ tales que $q_i = p_i u_i$.

Teorema 9. Todo dominio euclidiano D es un DFU.

Demostración. Sea $a \in D$, $a \neq 0$, veamos que a es un producto de irreducibles utilizando el segundo principio de inducción sobre $v(a)$. Si a es irreducible, a es producto de irreducibles. Ahora, si a no es irreducible, por el teorema anterior, existen $b, c \in D$ tales que $a = bc$ con $v(b) < v(a)$ y $v(c) < v(a)$, por la hipótesis de inducción b y c son productos de irreducibles, así que a también lo es.

Supongamos que $a = p_1 \cdots p_r = q_1 \cdots q_s$ con p_i, q_j irreducibles, así $p_1 \mid q_1 \cdots q_s$ y como D es euclidiano, D es un DIP (teorema 5). Como p_1 es irreducible, p_1 es primo y $p_1 \mid q_i$ para alguna $i \leq s$, supongamos que $i = 1$, así $p_1 t_1 = q_1$ y dado que q_1 es irreducible, p_1 es unidad ó t_1 es unidad, pero p_1 es irreducible así que t_1 es unidad. Entonces $a = p_1 \cdots p_r = p_1 t_1 q_2 \cdots q_s$, veamos la propiedad $ii)$ por inducción sobre r.
Si $r = 1$, $a = p_1 = q_1 \cdots q_s = p_1 t_1 q_2 \cdots q_s$ y cancelando p_1, $t_1^{-1} = q_2 \cdots q_s$ pero como los q_j son irreducibles, no pueden ser unidades así que $s = 1$. Ahora, sea $r \in \mathbb{N}$, $r > 1$, tenemos que $p_2 \cdots p_r = t_1 q_2 \cdots q_s$dado que t_1 es unidad y q_2 es irreducible, $t_1 q_2$ es un irreducible, así que por hipótesis de inducción, $r - 1 = s - 1$ de donde $r = s$ y existen unidades $u_2, \ldots, u_r \in D$ tales que $p_2 u_2 = t_1 q_2$ (de donde $p_2 u_2 t_1^{-1} = q_2$ y $u_2 t_1^{-1}$ también es unidad) y $p_i u_i = q_i$ si $3 \leq i \leq r$. ■

Construcción del Campo de Cocientes de un Dominio Entero

Sea D un dominio entero y $S = \{(a,b) \in D \times D \mid b \neq 0\}$, definimos una relación en S así: $(a,b) \sim (c,d) \Leftrightarrow ad = bc$. Veamos que $\sim$ es de equivalencia: Reflexividad. $ab = ba$, así que $(a,b) \sim (b,a)$. Simetría. Si $(a,b) \sim (c,d)$, entonces $ad = bc$ así $cb = da$ y $(c,d) \sim (a,b)$. Transitividad. Si $(a,b) \sim (c,d)$ y $(c,d) \sim (r,s)$, entonces $ad = bc$ y $cs = dr$ así que $asd = sad = sbc = bcs = bdr = brd$, dado que $d \neq 0$ y D es dominio entero, $as = br$ y $(a,b) \sim (r,s)$.

Ahora, sea F el conjunto de clases de equivalencia de $\sim$ y denotemos $\frac{a}{b}$ la clase de equivalencia de (a,b). Definamos tentativamente operaciones de suma y producto en F como sigue: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ y $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. Los miembros derechos de las igualdades anteriores son realmente elementos de F pues si $b \neq 0$ y $d \neq 0$, $bd \neq 0$. Veamos que las operaciones no dependen de representantes:

Supongamos que $\frac{a}{b} = \frac{a_1}{b_1}$ y $\frac{c}{d} = \frac{c_1}{d_1}$ así que $ab_1 = ba_1$ de donde $ab_1d_1d = ba_1d_1d$ y $cd_1 = dc_1$ de donde $cd_1b_1b = dc_1b_1b$, y sumando miembro a miembro tenemos $ab_1d_1d + cd_1b_1b = ba_1d_1d + dc_1b_1b$ es decir, $(ad + bc)b_1d_1 = bd(a_1d_1 + b_1c_1)$ así $(ad + bc, bd) \sim (a_1d_1 + b_1c_1, b_1d_1)$, $\frac{ad+bc}{bd} = \frac{a_1d_1+b_1c_1}{b_1d_1}$ y la suma está bien definida.

Ahora, multiplicando miembro a miembro $ab_1 = ba_1$ y $cd_1 = dc_1$ tenemos $ab_1cd_1 = ba_1dc_1$ así que $acb_1d_1 = bda_1c_1$ de aquí que $(ac, bd) \sim (a_1c_1, b_1d_1)$ y la multiplicación está bien definida.

Observaciones:

1. $\frac{0}{1} = 0$ es el neutro aditivo.
2. $\frac{-a}{b}$ es el inverso aditivo de $\frac{a}{b}$.
3. $\frac{1}{1}$ es el unitario.
4. Si $\frac{a}{b} \in F$ no es el neutro aditivo, entonces $a \neq 0$, $a \in D$ y $\frac{b}{a} \in F$ es el inverso multiplicativo de $\frac{a}{b}$.
5. $\langle F, +, \cdot \rangle$ es un campo.

El campo F se llama el campo de cocientes del dominio entero D.

Definición. *i)* Un subanillo de un anillo A es un subconjunto S tal que $1 \in S$, S es subgrupo del grupo aditivo de A y S es cerrado bajo productos.

ii) Un subcampo de un campo F es un subanillo de F que es campo.

Observaciones.

1. La intersección de una familia de subanillos de un anillo A es un subanillo de A.

2. La intersección de una familia de subcampos de un campo F es un subcampo de F.

Definición. Sean A, B dos anillos, un homomorfismo de A en B es una función $\varphi : A \longrightarrow B$ tal que:

1.$\varphi(1) = 1$.

2.φ es un homomorfismo de los grupos aditivos de A y B.

3. $\forall r, s \in A\ (\varphi(rs) = \varphi(r)\varphi(s))$.

Si A y B son campos, φ se llama homomorfismo de campos, si φ es inyectiva se llama monomorfismo, si φ es suprayectiva se llama epimorfismo, si φ es biyectiva se llama isomorfismo.

Notación. Si φ es un isomorfismo, decimos que A y B son isomorfos y escribimos $A \cong B$.

El núcleo de φ es $Núc\varphi = \{r \in A \mid \varphi(r) = 0\}$.

Observaciones.

1.La imagen inversa de un ideal de B es un ideal de A, es decir, si I es un ideal de B, $J = \varphi^{-1}(I) = \{a \in A \mid \varphi(a) \in I\}$ es un ideal de A. Además, si I es un ideal primo, J también es un ideal primo. Particularmente $Núc\varphi$ es un ideal de A.

Veamos que J es un ideal, sean $a, b \in J, t \in A$, así $\varphi(a), \varphi(b) \in I$ y $\varphi(a+b) = \varphi(a) + \varphi(b) \in I$, por eso $a+b \in J$. Ahora, $\varphi(ta) = \varphi(t)\varphi(a) \in I$ pues $\varphi(a) \in I$, así que $ta \in J$ y J es un ideal de A. Ahora, supongamos que I es un ideal primo y que $cd \in J$, así $\varphi(cd) \in I$ y como $\varphi(cd) = \varphi(c)\varphi(d) \in I$ entonces $\varphi(c) \in I$ ó $\varphi(d) \in I$ pues I es un ideal primo, así que $c \in J$ ó $d \in J$ y entonces J también es un ideal primo.

2.φ es un monomorfismo si y sólo si $Núc\varphi = \{0\}$.

3.La imagen de φ, $\operatorname{Im}\varphi$ es un subanillo de B.

Ejemplos.

1.Si D es un dominio entero y F su campo de cocientes, $f : D \longrightarrow F$ tal que para cada $a \in D$ $f(a) = \frac{a}{1}$ es un monomorfismo de anillos.

Ahora, si E es un campo, $\sigma : D \longrightarrow E$ un monomorfismo, y tenemos que $\tau : F \longrightarrow E$ es un homomorfismo tal que $\tau \circ f = \sigma$, entonces para cada $a \in D$, $\sigma(a) = \tau(f(a)) = \tau(\frac{a}{1})$. Y para cada $b \in D$, $b \neq 0$, dado que $\sigma(b) \neq 0$, $\frac{b}{1} \in F$, $\frac{b}{1} \neq 0$ y $\frac{1}{b}$ es el inverso multiplicativo de $\frac{b}{1}$, tenemos que

$\tau(\frac{1}{b}) = \tau(\frac{b}{1})^{-1} = \sigma(b)^{-1}$. Finalmente, dado que $\tau(\frac{a}{1}) = \sigma(a)$ y $\tau(\frac{1}{b}) = \sigma(b)^{-1}$ para cada $a, b \in D$, $b \neq 0$, $\tau(\frac{a}{b}) = \tau(\frac{a}{1} \cdot \frac{1}{b}) = \tau(\frac{a}{1})\tau(\frac{1}{b}) = \sigma(a)\sigma(b)^{-1}$. Es decir, τ sólo depende de σ y por eso es único.

Inversamente, si E es un campo, $\sigma : D \longrightarrow E$ un monomorfismo y definimos una función $\tau : F \longrightarrow E$ tal que para cada $\frac{a}{b} \in F$, $\tau(\frac{a}{b}) = \sigma(a)\sigma(b)^{-1}$; tenemos que τ es un homomorfismo y $\tau \circ f = \sigma$.

Así que si tenemos un monomorfismo $\sigma : D \longrightarrow E$, podemos enviar a los elementos de D dentro de su campo de cocientes F y extender σ a un homomorfismo $\tau : F \longrightarrow E$ tal que el diagrama

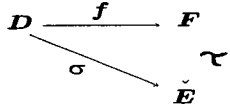

Figura 2.1:

es conmutativo.

2.Si A es un anillo, para cada ideal I de A, $\varphi : A \longrightarrow A/I$ tal que para cada $a \in A$ $\varphi(a) = a + I$ es un epimorfismo de anillos llamado el homomorfismo canónico.

3.Si $f : A \longrightarrow B$ es un homomorfismo de anillos, $Núcf = I$ y J es un ideal de A tal que $J \subseteq I$, entonces f induce un homomorfismo de anillos $f_J : A/J \longrightarrow B$ dado por $f_J(a + J) = f(a)$. Veamos que f_J está bien definida, supongamos que $a + J = b + J$, entonces $a - b \in J \subseteq I$ y así $0 = f(a - b) = f(a) - f(b)$ de donde $f(a) = f(b)$ y f_J está bien definida. Es inmediato comprobar que f_J es un homomorfismo de anillos, además $f = f_J \circ \varphi$ donde φ es el homomorfismo canónico, es decir, el diagrama

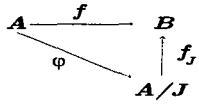

Figura 2.2:

conmuta. Más aún, f_I es un monomorfismo: Si $f_I(a + I) = 0$, entonces $f(a) = 0$ así que $a \in I$ y $a + I = I$ de donde f_I es un monomorfismo. Así que $A/Núcf \cong \operatorname{Im} f$, esta última parte es el llamado *Primer Teorema del Isomorfismo para anillos.*

Capítulo 3

Polinomios.

En este capítulo establecemos algunos resultados acerca de polinomios que usaremos en el siguiente capítulo y un teorema importante para poder aplicar los teoremas del capítulo anterior exhibiendo a algunos anillos de polinomios como dominios euclidianos.

Definición. Sea A un anillo, un polinomio en una variable sobre A es una función $P : \mathbb{N} \cup \{0\} \longrightarrow A$ tal que el conjunto $\sup P = \{n \in \mathbb{N} \cup \{0\} \mid P(n) \neq 0\}$, llamado el soporte de P, es finito.

Notación.El valor de P en n se denota P_n, es decir, $P(n) = P_n$.

Definamos operaciones de suma y producto de polinomios de la siguiente manera:

Si P, Q son polinomios sobre A,

$P + Q : \mathbb{N} \cup \{0\} \longrightarrow A$ es tal que para cada $n \in \mathbb{N} \cup \{0\}$,
$(P + Q)_n = P_n + Q_n$ la suma común de funciones.

$P \cdot Q : \mathbb{N} \cup \{0\} \longrightarrow A$ es tal que para cada $n \in \mathbb{N} \cup \{0\}$,

$(PQ)_n = \sum_{i=0}^{n} P_i Q_{n-i} (= \sum_{i+j=n} P_i Q_j)$ el llamado producto convolución.

Notación. Denotamos mediante $x : \mathbb{N} \cup \{0\} \longrightarrow A$ el polinomio tal que $(x)_1 = 1$ y $(x)_r = 0$ si $r \neq 1$,El conjunto de los polinomios en una variable sobre A se denota $A[x]$.

Teorema. $A[x]$ es un anillo con las operaciones arriba definidas, $0 \in A[x]$ es tal que para cada $n \in \mathbb{N} \cup \{0\}$, $0_n = 0 \in A$ y $1 \in A[x]$ es tal que $1_0 = 1 \in A$ y si $n \geq 1$, $1_n = 0 \in A$.

Demostración. Tal vez lo único que necesite una explicación detallada sea la asociatividad del producto, las demás propiedades de anillo son con-

secuencias muy directas de las propiedades de A dada la forma en que las operaciones en $A[x]$ fueron definidas. Así, sean $P, Q, R \in A[x]$, veamos que $(PQ) \cdot R = P \cdot (QR)$. Así que para cada $n \in \mathbb{N} \cup \{0\}$,

$$\begin{aligned}((PQ)\cdot R)_n &= \sum_{i=0}^{n} (PQ)_i R_{n-i} \\ &= \sum_{i=0}^{n} \left(\sum_{j=0}^{i} P_j Q_{i-j}\right) R_{n-i} \\ &= P_0Q_0R_n + \\ &\quad + P_0Q_1R_{n-1} + P_1Q_0R_{n-1} + \\ &\quad + \\ &\quad \vdots \\ &\quad + P_0Q_nR_0 + P_1Q_{n-1}R_0 + \cdots + P_nQ_0R_0 \\ &= \sum_{i=0}^{n} P_i \sum_{j=0}^{n-i} Q_j R_{n-(i+j)} \\ &= \sum_{i=0}^{n} P_i (QR)_{n-i} = (P \cdot (QR))_n\end{aligned}$$

de donde $(PQ) \cdot R = P \cdot (QR)$ y el producto es asociativo en $A[x]$. ■

Observaciones.1) El anillo de polinomios en m variables $A[x_1, \ldots, x_m]$ puede definirse de manera similar como el anillo de funciones de $\mathbb{N} \cup \{0\}^m$ en A con soporte finito, con el producto convolución.

2) Si definimos $i : A \longrightarrow A[x]$ tal que para cada $a \in A$, $(i(a))_0 = a$ y $(i(a))_r = 0$ si $r \geq 1$, entonces i es un monomorfismo. Así, podemos pensar en A dentro de $A[x]$ identificando cada elemento $a \in A$ con $i(a)$, estos elementos son llamados polinomios constantes.

3) Para cada $n \in \mathbb{N} \cup \{0\}$, $(x^n)_n = 1$ y $(x^n)_r = 0$ si $r \neq n$. Por inducción:

Es claro para $n = 0$ y $n = 1$. Supongamos que $(x^m)_m = 1$ y $(x^m)_r = 0$ si $r \neq m$, así $(x^{m+1})_r = (x \cdot x^m)_r = \sum_{i=0}^{r} (x_i)(x^m)_{r-i}$, así $(x^{m+1})_0 = 0$ y $(x^{m+1})_r = (x^m)_{r-1}$ si $r \geq 1$, de allí que $(x^{m+1})_{m+1} = 1$ y $(x^{m+1})_r = 0$ si $r \neq m+1$. Así, cada $P \in A[x]$ puede escribirse de manera única como $P = \sum_{i \in \mathbb{N} \cup \{0\}} P_i \cdot x^i$. Dado que $\sup P$ es finito, la suma de arriba en realidad es finita, $P = a_0 + a_1x + \cdots + a_nx^n$ donde $P_i = a_i$ si $0 \leq i \leq n$ y $P_i = 0$ si $i > n$.

4) A cada polinomio P se le puede asociar una función $P(\cdot) : A \longrightarrow A$ tal que si $P = a_0 + a_1x + \cdots + a_nx^n$, para cada $a \in A$ definimos $P(a) = a_0 + a_1a + \cdots + a_na^n$. De hecho, esta regla de correspondencia funciona para cualquier elemento que pueda multiplicarse por él mismo y por elementos de A, por ejemplo, $P(x) = P$ donde $x \in A[x]$ de la observación

elementos de A, por ejemplo, $P(x) = P$ donde $x \in A[x]$ de la observación anterior. Si $a \in A$, la función $e_a : A[x] \longrightarrow A$ tal que para cada $P \in A[x]$, $e_a(P) = P(a)$ es un epimorfismo llamado el homomorfismo de evaluación en a.

5) $A[x]$ es un dominio entero $\Leftrightarrow$ A es un dominio entero
$\Leftrightarrow A[x_1, \ldots x_m]$ es un dominio entero,
pero $A[x]$ y $A[x_1, \ldots, x_m]$ nunca son campos.

Definición. Sea $P \in A[x]$, $P \neq 0$.

1) Definimos el grado de P como el máximo del conjunto finito $\sup P$.

2) Si n es el grado de P, definimos el coeficiente principal de P como P_n.

3) Decimos que P es mónico si su coeficiente principal es el unitario de A.

4) Si $P(a) = 0$, decimos que a es una raíz de P.

Notación. El grado de P se denota $\deg P$.

Observación. Si D es un dominio entero, $P, Q \in D[x]$ diferentes de cero, entonces:

1) El coeficiente principal del producto PQ es el producto de los coeficientes principales de P y Q.

2) $\deg(PQ) = \deg P + \deg Q$ y así $\deg P \leq \deg(PQ)$.

Teorema. Sea A un anillo, $g \in A[x]$, $g \neq 0$ y tal que su coeficiente principal es una unidad. Entonces para cualquier $f \in A[x]$ existen $q, r \in A[x]$ tales que $f = qg + r$ donde $r = 0$ ó $\deg r < \deg g$.

Demostración. Sea $g \in A[x]$, $g \neq 0$ y de grado n,
digamos $g = a_n x^n + \cdots + a_1 x + a_0$ con a_n unidad. Sea $f \in A[x]$, si $f = 0$ ó si $\deg f < n$, entonces $q = 0$ y $r = f$ satisfacen.

Ahora, supongamos que $f \neq 0$ y que $\deg f \geq n$, veamos el resultado por el segundo principio de inducción sobre el grado de f. Digamos que
$f = b_m x^m + \cdots + b_1 x + b_0$ con $\deg f = m \geq n$, recordando que a_n es unidad, tenemos $b_m a_n^{-1} x^{m-n} g = b_m x^m + \cdots + b_m a_n^{-1} a_0 x^{m-n}$ así que
$\deg(\ f - b_m a_n^{-1} x^{m-n} g) < \deg f$ ó $f - b_m a_n^{-1} x^{m-n} g = 0$ y en cualquier caso, por hipótesis de inducción ó por el primer caso, existen $s, t \in A[x]$ tales que
$f - b_m a_n^{-1} x^{m-n} g = sg + t$ con $t = 0$ ó $\deg t < \deg g$, y entonces
$f = (s + b_m a_n^{-1} x^{m-n}) g + t$. ■

Corolario. Si F es un campo, $F[x]$ es un dominio euclidiano.

Demostración. Por el teorema anterior y por la observación anterior al teorema, el grado es una valuación euclidiana para el anillo de polinomios $F[x]$. ■

Observaciones.1) Aún cuando D sea un dominio euclidiano, no necesariamente lo es $D[x]$ pues en $\mathbb{Z}[x]$, el ideal $\langle x, 2\rangle$ no es principal y dado que $\mathbb{Z}[x]$ no es un DIP tampoco puede ser un dominio euclidiano.

2) Las unidades de $F[x]$ son los elementos de grado cero, es decir, los polinomios constantes diferentes de cero. Esto también explica por qué $F[x]$ no es un campo.

Corolario. Sea F un campo, $f \in F[x]$ y $a \in F$. Entonces existe $q \in F[x]$ tal que $f = q(x-a) + f(a)$.

Demostración. Por ser $F[x]$ un dominio euclidiano, existen $q, r \in F[x]$ tales que $f = q(x-a) + r$ donde $r = 0$ ó $\deg r = 0$, pues $\deg(x-a) = 1$. Aplicando el homomorfismo de evaluación en a y dado que r es un polinomio constante, $f(a) = q(a)(a-a) + r(a) = r$. ■

Corolario. Sea F un campo, y $f \in F[x]$. Entonces $a \in F$ es una raíz de f si y solamente si $x - a$ divide a f.

Demostración. Si a es una raíz de f, del corolario anterior y $f(a) = 0$ resulta $f = q(x-a)$.

Si $x - a$ divide a f, $f = q(x-a)$, evaluamos en a y $f(a) = 0$, así que a es una raíz de f. ■

Teorema. Si F es un campo y $f \in F[x]$ tiene grado n, entonces F contiene a lo más n raíces de f.

Demostración. Por inducción sobre n. Si $n = 0$, f tiene grado cero, así que es un polinomio constante diferente de cero y no tiene raíces. Supongamos el resultado verdadero para polinomios de grado n. Sea $f \in F[x]$, f de grado $n+1$ y supongamos que f tiene alguna raíz $a \in F$. Así, $x - a$ divide a f, $f = (x-a)g$ donde g tiene grado n pues $x - a$ tiene grado 1. Así, g tiene a lo más n raíces. Ahora, si b es raíz de f, $f(b) = 0$ y $(b-a)g(b) = 0$ así que b es raíz de $x - a$ (es decir, $a = b$) ó b es raíz de g. Finalmente, f tiene a lo más $n+1$ raíces. ■

Capítulo 4

Extensiones de Campos.

Definición. Sean E y F dos campos, decimos que E es una extensón de F si E contiene un subcampo isomorfo a F.

Notación. Denotamos $E : F$ al campo E visto como extensión del campo F.

Siempre que es posible, identificamos a F con el subcampo isomorfo contenido en E.

Definición. 1) Sea $E : F$ una extensión de campo y sean $\alpha_1, \ldots, \alpha_n \in E$, $F(\alpha_1, \ldots, \alpha_n)$ es el mínimo subcampo de $E : F$ que contiene a F y a $\{\alpha_1, \ldots, \alpha_n\}$.

2) La extensión $E : F$ se llama simple si existe $\alpha \in E$ tal que $E = F(\alpha)$.

3) Sea $\alpha \in E : F$, α se llama algebráico sobre F si α es raíz de algún polinomio diferente de cero $f \in F[x]$, en otro caso α se llama trascendente.

4) Sean $\alpha_1, \ldots, \alpha_n \in E : F$, $\alpha_1, \ldots, \alpha_n$ son algebráicamente dependientes sobre F si $(\alpha_1, \ldots, \alpha_n)$ es raíz de algún polinomio $f \in F[x_1, \ldots, x_n]$, en otro caso, $\alpha_1, \ldots, \alpha_n$ son algebráicamente independientes sobre F.

Ejemplos. 1) Si F es un campo, el campo de cocientes de $F[x]$ es $F(x)$ y el campo de cocientes de $F[x_1, \ldots, x_n]$ es $F(x_1, \ldots, x_n)$. El elemento $x \in F(x)$ es trascendente sobre F y $x_1, \ldots, x_n \in F(x_1, \ldots, x_n)$ son algebráicamente independientes sobre F.

2) Sea F un campo y $p \in F[x]$, p irreducible, así que $E = F[x]/\langle p \rangle$ es un campo. Ahora, si $i : F \longrightarrow F[x]$ es la inclusión, y $\varphi : F[x] \longrightarrow F[x]/\langle p \rangle$ el homomorfismo canónico, $\varphi \circ i : F \longrightarrow F[x]/\langle p \rangle$ es un monomorfismo, pues si $a \in F$ es tal que $\varphi \circ i(a) = 0$ entonces $a + \langle p \rangle = \langle p \rangle$ así que $a \in \langle p \rangle$, dado que $a \in F$ y $p \in F[x]$ es irreducible (ó $\langle p \rangle$ máximo) $a = 0$, $\varphi \circ i$ es

un monomorfismo y la imagen de $\varphi \circ i$ es un subcampo de $F[x]/\langle p\rangle = E$ isomorfo a F, en otras palabras, $E : F$ es una extensión de campo. Más aún, si denotamos $\alpha = x + \langle p\rangle \in E$, $E = F(\alpha)$ y $p(\alpha) = p + \langle p\rangle = \langle p\rangle = 0 \in E : F$, así que α es una raíz de p y α es algebráico sobre F.

3) Sea $\alpha \in E : F$, si α es algebráico sobre F y $f_\alpha : F[x] \longrightarrow E$ es la evaluación en α, tenemos que $\operatorname{Im} f_\alpha \subseteq F(\alpha)$, además $Núcf_\alpha$ es un ideal diferente de cero de $F[x]$. Dado que $F[x]$ es un DIP, existe un $p \in F[x]$ tal que $Núcf_\alpha = \langle p\rangle$. Ahora, $F[x]/\langle p\rangle \cong \operatorname{Im} f_\alpha$ y como $\operatorname{Im} f_\alpha$ es un subanillo del campo E, $\operatorname{Im} f_\alpha$ es un dominio entero y $F[x]/\langle p\rangle$ también lo es, así que $\langle p\rangle$ es un ideal primo de $F[x]$ y por tanto un ideal máximo, de allí que $F[x]/\langle p\rangle$ es un campo y también $\operatorname{Im} f_\alpha$ es un campo, y como $\alpha \in \operatorname{Im} f_\alpha$, $F(\alpha) \subseteq \operatorname{Im} f_\alpha$; así que $\operatorname{Im} f_\alpha = F(\alpha) \cong F[x]/\langle p\rangle$.

Observación. El polinomio p es de grado mínimo en $Núcf_\alpha$, además, como cualquier múltiplo por unidad del polinomio p genera el mismo ideal, podemos pedir que p sea mónico y así ya es único. Por otro lado, dado que $\langle p\rangle \neq \{0\}$ es un ideal máximo, p es irreducible y además α es raíz de p.

Definición. Sea $E : F$ una extensión de campo y $\alpha \in E : F$, α algebráico sobre F. El único polinomio mónico irreducible $p \in F[x]$ tal que α es raíz de p se llama el polinomio irreducible de α sobre F.

Definición. Sea $f \in F[x]$, f un polinomio no constante.

1) f se descompone sobre F si es producto de factores lineales (de grado 1) en $F[x]$.

2) Un campo de descomposición para f es una extensión $E : F$ sobre la cual f se descompone pero f no se descompone sobre ningún subcampo propio de E que contenga a F.

Observación. El polinomio f se descompone sobre F si todas las raíces de f son elementos de F.

Teorema. Sea $f \in F[x]$ un polinomio no constante.

1) Hay una extensión $E : F$ sobre la cual f se descompone.

2) Hay un campo de descomposición para f.

Demostración. 1) Por inducción sobre el grado de f. Si f es de grado 1, f ya es lineal y se descompone sobre F. Supongamos que para cada polinomio de grado n hay una extensión de F sobre la cual se descompone. Supongamos que f es un polinomio de grado $n+1$ y sea $p \in F[x]$ uno de sus factores irreducibles. Construimos como en el ejemplo 2) una extensión $B : F$ que contenga a una raíz α de p, así que $\alpha \in B$ es también una raíz de f y $f = (x-\alpha)g$ con $g \in B[x]$ donde g tiene grado n. Por hipótesis de inducción,

hay una extensión $E : B$ sobre la cual g se descompone y por tanto f también se descompone sobre E.

2) Sea E un campo sobre el cual f se descompone (el campo existe por la parte 1)), es decir, si $\alpha_1, \ldots, \alpha_n$ son las raíces de f, $\alpha_1, \ldots, \alpha_n \in E$. Claramente, f se descompone sobre $F(\alpha_1, \ldots, \alpha_n)$ pero no sobre algún subcampo propio de $F(\alpha_1, \ldots, \alpha_n)$ que contenga a F. ■

Definición. 1) Una extensión de campo $B : F$ es una extensión pura si existe un $\alpha \in B$, $\alpha \neq 0$ tal que $B = F(\alpha)$ y α^p es un elemento de F (del subcampo de B isomorfo a F) para algún número primo p.

2) Una extensión de campo $E : F$ es una extensión radical si hay una serie de campos intermedios $F = B_0 \subset B_1 \subset \cdots \subset B_t = E$ tal que cada extensión $B_{i+1} : B_i$ es pura.

3) Sea $f \in F[x]$, f es soluble por radicales si hay una extensión radical $E : F$ tal que f se descompone sobre E.

Ejemplo. El polinomio $x^2 + 1$ es un irreducible en $\mathbb{R}[x]$, así que $\mathbb{R}[x]/\langle x^2 + 1\rangle$ es una extensión de $\mathbb{R}$ que contiene una raíz α del polinomio $x^2 + 1$ tal que $\mathbb{R}(\alpha) = \mathbb{R}[x]/\langle x^2 + 1\rangle$. Ahora, como α es raíz de $x^2 + 1$, $\alpha^2 + 1 = 0$ y $\alpha^2 = -1 \in \mathbb{R}$, así que $\mathbb{R}[x]/\langle x^2 + 1\rangle$ es una extensión pura de $\mathbb{R}$.

Notación. Denotamos $\mathbb{C} = \mathbb{R}[x]/\langle x^2 + 1\rangle$ y le llamamos el campo de los números complejos, $i = x + \langle x^2 + 1\rangle = \alpha$, así,$\mathbb{R}(i) = \mathbb{C}$.

Definición. 1) Si F es un campo y $g : F \longrightarrow F$ es un isomorfismo, g se llama un automorfismo de F.

2) Si $E : F$ es una extensión de campo y $g : E \longrightarrow E$ es un automorfismo de E tal que para cada $a \in F$, $g(a) = a$; g se llama un $F - automorfismo$ de $E : F$.

Capítulo 5

La insolubilidad de la quíntica.

Sea F un campo de característica cero y que contenga a todas las raíces de la unidad, es decir, raíces de los polinomios de la forma $x^m - 1$ (por ejemplo $\mathbb{C}$ tiene esa propiedad). Sean $x_1, \ldots, x_n$ elementos algebráicamente independientes sobre F (por ejemplo variables en el campo de cocientes del anillo de polinomios sobre F).

Sea $P = (x - x_1)(x - x_2)\cdots(x - x_n)$
$= x^n - a_1x^{n-1} + a_2x^{n-2} - \cdots + (-1)^n a_n$

donde

$a_1 = x_1 + x_2 + \cdots + x_n$
$a_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n$
$\vdots$
$a_n = x_1x_2\cdots x_n$

El polinomio P se llama el polinomio genérico de grado n sobre F.

Sean $K = F(a_1, a_2, \ldots, a_n)$ y $L = K(x_1, x_2, \ldots, x_n)$

Observaciones.

1) $L = F(x_1, \ldots, x_n)$. Es claro que $a_1, a_2, \ldots, a_n \in F(x_1, \ldots, x_n)$. así que $F(a_1, a_2, \ldots, a_n) \subseteq F(x_1, \ldots, x_n)$; ahora, dado que $x_1, \ldots, x_n \in F(x_1, \ldots, x_n)$ y $F(a_1, a_2, \ldots, a_n) = K$, $K(x_1, x_2, \ldots, x_n) \subseteq F(x_1, \ldots, x_n)$., es decir, $L \subseteq F(x_1, \ldots, x_n)$. Ahora, $F \subseteq K$ y $K \subseteq L$, además $x_1, \ldots, x_n \in L$ así que $F(x_1, \ldots, x_n) \subseteq L$. Finalmente $L = F(x_1, \ldots, x_n)$.

2) $P \in K[x]$

3) L es el campo de descomposición de P.

Debido a las observaciones de que un polinomio en n variables tiene una expresión única como suma de productos de potencias de las variables, pode-

mos definir un homomorfismo del anillo A en otro anillo y extender el homomorfismo a uno de $A[x_1,\ldots,x_n]$ solamente definiéndolo en $x_1,\ldots,x_n$.

Ahora, sea $Id : F \longrightarrow F$ el homomorfismo identidad, que deja fijo todo F. Para cada $\sigma \in S_n$ el grupo de permutaciones, definimos el homomorfismo $\bar{\sigma} : F[x_1,\ldots,x_n] \longrightarrow L$ tal que

$\bar{\sigma}(a) = a$ si $a \in F$ y $\bar{\sigma}(x_i) = x_{\sigma(i)}$ para cada $i = 1,\ldots,n$.

$\operatorname{Im}\bar{\sigma} \subseteq F[x_1,\ldots,x_n]$

Debido a la independencia algebráica de $x_1,\ldots,x_n$ sobre F, $\bar{\sigma}$ es un monomorfismo; de manera que $\bar{\sigma}$ se extiende de manera única a un homomorfismo $\sigma^* : F(x_1,\ldots,x_n) \longrightarrow L$ pues $F(x_1,\ldots,x_n)$ es el campo de cocientes de $F[x_1,\ldots,x_n]$.

Ahora, si $\sigma \in S_n$ es el neutro del grupo, $\bar{\sigma}(x_i) = x_i$ y de allí que $\sigma^* = Id_L$.

Y, sean $\sigma, \tau \in S_n$,

$$\begin{aligned}\bar{\sigma} \circ \bar{\tau}(x_i) &= \bar{\sigma}(x_{\tau(i)}) \\ &= x_{\sigma(\tau(i))} \\ &= x_{\sigma\circ\tau(i)} \\ &= \overline{\sigma \circ \tau}\ (x_i)\end{aligned}$$

así que $\bar{\sigma} \circ \bar{\tau} = \overline{\sigma \circ \tau}$ y también $\sigma^* \circ \tau^* = (\sigma \circ \tau)^*$ y por la observación a la definición de acción de grupo, el grupo S_n actúa en L de la siguiente manera:

$T : S_n \times L \longrightarrow L$ es tal que $T(\sigma, a) = \sigma^*(a)$.

Observaciones.

1)Dado que T es una acción del grupo S_n, para cada $\sigma \in S_n$, σ^* es biyectiva; es decir, $\sigma^* : L \longrightarrow L$ es un automorfismo.

2)Los coeficientes del polinomio P, $a_1,\ldots,a_n$ permanecen fijos bajo la acción de S_n; es decir, el subgrupo de isotropía de a_i es S_n.

3)Dado que F permanece fijo bajo la acción de S_n, todo $F(a_1,\ldots,a_n) = K$ permanece fijo; así que para cada $\sigma \in S_n$, σ^* es un $K - automorfismo$ de L.

Definición.

1)La expresión de a_i en términos de $x_1,\ldots,x_n$ se llama el $i - ésimo$ polinomio simétrico elemental en $x_1,\ldots,x_n$.

2)Un polinomio $p(x_1,\ldots,x_n) \in F[x_1,\ldots,x_n]$ es simétrico si para cada $\sigma \in S_n$,

$p(x_{\sigma(1)},\ldots,x_{\sigma(n)}) = p(x_1,\ldots,x_n)$; es decir,

$\bar{\sigma}(p) = p$.

3)Un elemento $\frac{p}{q} \in F(x_1,\ldots,x_n)$ es una fracción racional simétrica si para cada $\sigma \in S_n$, $\sigma^*(\frac{p}{q}) = \frac{p}{q}$.

Teorema. *(Fundamental de los Polinomios Simétricos)*
Sean $s_1, \ldots, s_n$ los polinomios simétricos elementales en $t_1, \ldots, t_n$. Cada polinomio simétrico en $t_1, \ldots, t_n$ tiene una expresión polinomial en $s_1, \ldots, s_n$; es decir, si $p \in F[t_1, \ldots, t_n]$ es simétrico, entonces $p(t_1, \ldots, t_n) = q(s_1, \ldots, s_n)$ para algún $q \in F[x_1, \ldots, x_n]$.

Demostración. Por inducción sobre n.
Si $n = 1$, el resultado es claro porque $s_1 = t_1$.
Sea $n \in \mathbb{N}$, $n > 1$ y supongamos el resultado verdadero para $n - 1$.
Sea p simétrico en $t_1, \ldots, t_n$ y ordenémoslo con respecto a t_n,
$p(t_1, \ldots, t_n) = P_0 + P_1 t_n + P_2 t_n^2 + \cdots + P_k t_n^k$
donde cada P_i es un polinomio en $t_1, \ldots, t_{n-1}$. Al intercambiar los $t_1, \ldots, t_{n-1}$ de alguna manera, p sigue igual por ser simétrico, así, cada P_i debe quedar igual pues t_n no ha sido movido, así que cada P_i es simétrico en $t_1, \ldots, t_{n-1}$.
Por hipótesis de inducción, cada P_i es un polinomio en términos de los polinomios simétricos elementales en $t_1, \ldots, t_{n-1}$, sean $u_1, \ldots, u_{n-1}$ tales polinomios simétricos elementales, así que
$p(t_1, \ldots, t_n) = q_0 + q_1 t_n + q_2 t_n^2 + \cdots + q_k t_n^k$
donde cada q_i es un polinomio en $u_1, \ldots, u_{n-1}$.
Notamos que cada s_i puede expresarse en términos de u_{i-1}, u_i y t_n así:

$$\begin{aligned} s_1 &= u_1 + t_n \\ s_2 &= u_2 + u_1 t_n \\ &\vdots \\ s_{n-1} &= u_{n-1} + u_{n-2} t_n \\ s_n &= u_{n-1} t_n \end{aligned}$$

Despejando cada u_i y substituyendo el despeje de u_{i-1},

$$\begin{aligned} u_1 &= s_1 - t_n \\ u_2 &= s_2 - u_1 t_n = s_2 - s_1 t_n + t_n^2 \\ &\vdots \\ u_{n-1} &= s_{n-1} - u_{n-2} t_n = s_{n-1} - s_{n-2} t_n + \cdots + (-1)^{n-1} t_n^{n-1} \end{aligned}$$

y también
$0 = s_n - u_{n-1} t_n = s_n - s_{n-1} t_n + \cdots + (-1)^n t_n^n$ de donde
$t_n^n = (-1)^{n-1} s_n + (-1)^{n-2} s_{n-1} t_n + \cdots + s_1 t_n^{n-1}$
Ahora, sustituyendo en cada q_i las expresiones anteriores de $u_1, \ldots, u_{n-1}$, resulta
$p(t_1, \ldots, t_n) = r_0 + r_1 t_n + r_2 t_n^2 + \cdots + r_k t_n^k$

donde cada r_i se expresa en términos de $s_1, \ldots, s_{n-1}$ y t_n, así que ordenando nuevamente con respecto a t_n, resulta

$$p(t_1, \ldots, t_n) = g_0 + g_1 t_n + \cdots + g_m t_n^m$$

donde cada g_i es una expresión polinomial en términos de $s_1, \ldots, s_{n-1}$.

Si resulta $m \geq n$, podemos reducir el grado en t_n usando la expresión de t_n^n en términos de $s_1, \ldots, s_n, t_n, \ldots, t_n^{n-1}$. Así,

$$p(t_1, \ldots, t_n) = h_0 + h_1 t_n + \cdots + h_{n-1} t_n^{n-1}$$

donde cada h_i es una expresión polinomial en términos de $s_1, \ldots, s_n$ y por eso cada h_i es simétrico en $t_1, \ldots, t_n$, y dado que p también lo es, al intercambiar t_i y t_n en esta última expresión, obtenemos

$$p(t_1, \ldots, t_n) = h_0 + h_1 t_i + \cdots + h_{n-1} t_i^{n-1}$$

válido para cada $i = 1, \ldots, n$. Así, observamos el polinomio

$$P(x) = h_0 + h_1 x + \cdots + h_{n-1} x^{n-1} - p(t_1, \ldots, t_n) \qquad P \in F(t_1, \ldots, t_n)\,[x]$$

y tiene a lo más, grado $n-1$, pero $t_1, \ldots, t_n$ son n raíces de P, así que P solamente puede ser el polinomio cero. Así, $h_i = 0$ para $i \geq 1$ y $p(t_1, \ldots, t_n) = h_0 = h_0(s_1, \ldots, s_n)$ como afirma el teorema. ■

Teorema *(Fundamental de las Fracciones Simétricas).* Sea $\frac{p}{q} \in F(t_1, \ldots, t_n)$. Si $\frac{p}{q}$ es simétrica, entonces $\frac{p}{q}$ tiene una expresión como cociente de dos expresiones polinomiales en términos de $s_1, \ldots, s_n$.

Demostración. Sea $\frac{p}{q}$ simétrica, y sea $S_n = \{\sigma_1, \ldots, \sigma_r\}$ (de hecho, $r = n!$), definimos $q_s = \sigma_s^*(q)$ y supongamos que σ_1 es el neutro de S_n sólo para que $q_1 = q$. Si $\tau \in S_n$, $\{\tau\sigma_1, \ldots, \tau\sigma_r\} = S_n$ así , el producto $q_1 \cdots q_r$ es simétrico y como $\frac{p}{q} = \frac{pq_2 \cdots q_r}{qq_2 \cdots q_r}$ y $\frac{p}{q}$ es simétrico, $pq_2 \cdots q_r$ también es simétrico. Ahora, por el teorema fundamental de los polinomios simétricos, existen dos polinomios f, g tales que

$$pq_2 \cdots q_r = f(s_1, \ldots, s_n) \text{ y } q_1 \cdots q_r = g(s_1, \ldots, s_n) \text{ así, } \frac{p}{q} = \frac{f(s_1, \ldots, s_n)}{g(s_1, \ldots, s_n)}$$ ■

Teniendo en mente las últimas observaciones y, manteniendo la notación inicial, tenemos la siguiente:

Observación. Si $a \in L$ y el subgrupo de isotropía de a bajo la acción de S_n en L es todo S_n, entonces $a \in K$.

Ahora, sea $\delta = \prod_{i<j} (x_i - x_j)$, $\delta \in L$; en cuanto a la acción de S_n en δ tenemos las siguientes

Observaciones:

1. La transposición $(m\ m+1)$ envía δ en $-\delta$.

2. Dado que $(m\ n) = (m\ m+1)(m+1\ m+2)(\cdots)(n-1\ n)(n-2\ n-1)(\cdots)(m\ m+1)$ es el producto de un número impar de transposiciones,

cualquier transposición $(m\ n)$ envía δ en $-\delta$.

3. El subgrupo de isotropía de $\delta \in L$ es el grupo alternante A_n y los demás elementos de S_n simplemente le cambian el signo. Así, el subgrupo de isotropía de δ^2 es S_n y $\delta^2 \in K$.

Notación. Si $\sigma \in S_n$, sabemos que $\sigma^* : L \longrightarrow L$, pero para simplificar y dado que no habrá confusión, denotemos a σ^* simplemente σ y $\sigma^*(a) = \sigma(a)$ donde $a \in L$.

Observaciones:

4. Si $\alpha \in L$ es tal que para cualquier transposición σ, $\sigma(\alpha) = -\alpha$ entonces $\frac{\alpha}{\delta}$ es fijo por todas las transposiciones y así, fijo por todo S_n, de donde $\frac{\alpha}{\delta} = b \in K$ y $\alpha = b\delta$.

5. Si α es fijo por A_n y $\sigma, \tau \in S_n$ son dos transposiciones, dado que $\sigma = \tau\tau\sigma$, $\sigma(\alpha) = \tau(\alpha)$.

Recordando que el campo K contiene todas las raíces de la unidad (que sean necesarias) y que para cada $\sigma \in S_n$, $\sigma : L \longrightarrow L$ es un $K-$ *automorfismo* de L, veamos el

Teorema. Si $n \geq 5$, $L : K$ no es una extensión radical.

Demostración. Sean $K_0, \ldots, K_r$ campos tales que $K = K_0 \subset K_1 \subset \cdots \subset K_r = L$. Supongamos para empezar, que $K_1 : K$ es una extensión pura. Entonces existe un primo p y $\alpha \in K_1$ tal que $K_1 = K(\alpha)$ y $\alpha^p \in K$. Sea $a = \alpha^p \in K$. Sea $\tau \in S_n$ una transposición, aplicando τ en ambos miembros de la ecuación $\alpha^p = a$, tenemos $\tau(\alpha)^p = a$ y así $\left(\frac{\tau(\alpha)}{\alpha}\right)^p = 1$ así que $\tau(\alpha) = \zeta\alpha$ donde $\zeta^p = 1$. Aplicando nuevamente τ tenemos $\alpha = \tau\tau(\alpha) = \tau(\zeta\alpha) = \zeta\tau(\alpha) = \zeta^2\alpha$. Ahora,

Si α es fijo por todas las transposiciones, α es fijo por todo S_n y $\alpha \in K$ así que $K(\alpha) = K$ y no hay extensión.

Si hay algún τ transposición tal que $\tau(\alpha) \neq \alpha$, entonces $\tau(\alpha) = -\alpha$ y $p = 2$. Además, para cada transposición τ, $\tau(\alpha) = \pm\alpha$ así que para cada $\sigma \in S_n$, $\sigma(\alpha) = \pm\alpha$. Ahora, dado que un $3-ciclo$ $(a\ b\ c) = (a\ c\ b)(a\ c\ b)$, α es fijo por todos los $3-ciclos$ y así α es fijo por todo A_n. Por la observación 5 y dado que hay alguna transposición τ tal que $\tau(\alpha) = -\alpha$, cada transposición σ es tal que $\sigma(\alpha) = -\alpha$; por la observación 4 tenemos que $\frac{\alpha}{\delta} = b \in K$ y $\alpha = b\delta$ obteniendo también $K_1 = K(\alpha) = K(\delta)$.

Dado que α satisface un polinomio de grado 2 en $K[x]$, cada elemento en $K_1 = K(\alpha)$ es de la forma $c + d\alpha$ con $c, d \in K$. Así, si $\gamma \in K_1$, γ es fijo por A_n y A_n es el mayor subgrupo que deja fijos a todos los elementos de K_1. Veamos ahora que, si $\gamma \in L$ es fijo por A_n entonces $\gamma \in K_1$:

Sea $\gamma \in L$ fijo por A_n y sea $\tau \in S_n$ una transposición, los elementos $\gamma + \tau(\gamma)$ y $\gamma - \tau(\gamma)$ también son fijos por A_n; además

$\tau(\gamma+\tau(\gamma)) = \tau(\gamma)+\tau\tau(\gamma) = \gamma+\tau(\gamma)$ y por la observación 5, $\gamma+\tau(\gamma) \in K$. y

$\tau(\gamma-\tau(\gamma)) = \tau(\gamma)-\tau\tau(\gamma) = -(\gamma-\tau(\gamma))$ por la observación 5 y por la 4, $\gamma-\tau(\gamma)$ es el producto de δ por un elemento de K, y como $\gamma = \frac{\gamma+\tau(\gamma)}{2} + \frac{\gamma-\tau(\gamma)}{2}$ donde $2 = 1+1$, entonces $\gamma \in K_1$.

Ahora, veamos que K_1 no puede extenderse radicalmente en L si $n \geq 5$. Supongamos que $K_2 : K_1$ es una extensión pura, entonces existe un primo q y $\beta \in K_2$ tal que $K_2 = K_1(\beta)$ y $\beta^q \in K_1$. Sea $c = \beta^q \in K_1$.

Sea $\rho \in A_n$ un $3-ciclo$, entonces $\rho(\beta)^q = c$ y se deduce que $\rho(\beta) = \zeta\beta$ donde $\zeta^q = 1$, y aplicando ρ dos veces más, tenemos $\beta = \rho^3(\beta) = \zeta^3\beta$. Ahora,

Si β es fijo por todos los $3-ciclos$, β es fijo por todo A_n y $\beta \in K_1$, así que $K_1(\beta) = K_1$ y no hay extensión.

Si hay algún $3-ciclo$ ρ tal que $\rho(\beta) \neq \beta$, entonces $q = 3$.

Ahora, dado que $n \geq 5$, podemos comenzar con un $5-ciclo$ y al poder generar A_n con $5-ciclos$, se deduce que $q = 5$ ó no hay extensión radical de K_1 en L. En este momento hemos visto que K_1 no puede extenderse radicalmente en L a menos que q fuera 3 y 5 simultáneamente.

Tenemos que $L : K$ no es una extensión radical. ■

Vale la pena notar que la suposición de que $n \geq 5$ no fue usada sino hasta en las últimas líneas de la demostración para poder usar aquel teorema sobre A_n demostrado en el primer capítulo. ¡Cómo el hecho de que A_n puede generarse con $3-ciclos$ y también con $5-ciclos$ es una razón poderosa para que $L : K$ no sea una extensión radical!

La siguiente tarea será mostrar que $L : K$ no está contenido en ninguna extensión radical de K.

Observación 1. Si α es una raíz de $x^p - a$ y $\zeta_1, \ldots, \zeta_p$ son las raíces $p-ésimas$ de la unidad, $\zeta_1\alpha, \ldots, \zeta_p\alpha$ son las raíces de $x^p - a$.

Ahora veamos los siguientes lemas. Este primer lema es un resultado general y muy conocido.

Lema 1. Sea F un campo, p un número primo y $a \in F$ tal que a no es una potencia $p-ésima$ en F ($x^p - a$ no tiene raíces en F).

i) Para $k = 1, \ldots, p-1$, a^k tampoco es una potencia $p-ésima$ en F.

ii) El polinomio $x^p - a$ es irreducible sobre F.

Demostración. *i)* Sea $k \in \{1, \ldots, p-1\}$, k es primo relativo con p así que hay unos enteros l ,q tales que $pq + kl = 1$ y $a = (a^q)^p \cdot (a^k)^l$ Ahora,

supongamos que a^k es una potencia $p-$ *ésima* en F, así que $a^k = b^p$ con $b \in F$,

de allí que $(a^q b^l)^p = (a^q)^p \cdot (b^l)^p = (a^q)^p \cdot (b^p)^l = (a^q)^p \cdot (a^k)^l = a$ así que $a \in F$ también es una potencia $p-$ *ésima* y el resultado se obtiene por contrapositiva.

ii) Sean $P, Q \in F[x]$ tales que $x^p - a = PQ$. Podemos suponer que P y Q son mónicos, veamos que uno de los dos es el polinomio constante 1.

Sea K una extensión de F donde $x^p - a$ se descompone, y sea $u \in K$ una de las raíces de $x^p - a$, por la observación 1, tenemos en $K[x]$, $\prod_{i=1}^{p} (x - \zeta_i u) = PQ$. Así que P y Q se descomponen en $K[x]$ como productos de factores lineales, digamos $P = \prod_{i=1}^{k} (x - \zeta_i u)$ y $Q = \prod_{i=k+1}^{p} (x - \zeta_i u)$.

Observando el término independiente en $P \in F[x]$, tenemos que $\left(\prod_{i=1}^{k} \zeta_i\right) u^k = b \in F$, elevando a la potencia p y dado que $(\zeta_i)^p = 1$, $b^p = (u^k)^p = a^k$, por la parte i) del lema, $k = 0$ ó $k = p$ de donde $P = 1$ ó $Q = 1$ y así $x^p - a$ es irreducible sobre F. ■

Observación 2. Si $R = F(u)$ donde u es algebráico sobre F con polinomio irreducible de grado n, para cada $v \in R$, existen $v_0, \ldots, v_{n-1} \in F$ tales que $v = v_0 + v_1 u + \cdots + v_{n-1} u^{n-1}$.

El siguiente lema nos permite obtener expresiones más sencillas que nos simplificarán el trabajo en el caso de que tengamos el elemento v de antemano fuera de F. Nuevamente es un resultado general sobre una extensión pura de un campo.

Lema 2. Sea F un campo, p un número primo y $a \in F$ tal que a no es una potencia $p-$*ésima* en F. Sea α una raíz del polinomio $x^p - a$ y $F(\alpha) = R$. Sea $v \in R$, si $v \notin F$ entonces existe $u \in R$ tal que $F(u) = R$, $u^p \in F$ y existen $v_0, v_2, \ldots, v_{p-1} \in F$ tales que $v = v_0 + u + v_2 u^2 + \cdots + v_{p-1} u^{p-1}$.

Demostración. Tenemos que $\alpha^p = a \in F$ la cual no es potencia $p-$ *ésima* en F, por la observación 2), $v = v'_0 + v'_1 \alpha + \cdots + v'_{p-1} \alpha^{p-1}$ con $v'_0, \ldots, v'_{p-1} \in F$. Como $v \notin F$, hay algún $v'_k \neq 0$ con $1 \leq k \leq p-1$, sea $u = v'_k \alpha^k$ y elevando a la potencia p, $u^p = v'^p_k a^k \in F$, y como a no es potencia $p-$*ésima* en F, a^k tampoco lo es por el lema 1.*i*), entonces u^p tampoco es una potencia $p-$ *ésima* en F ($u \notin F$). Dado que $u \in R$, claramente $F(u) \subseteq R$. Ahora, veamos como u genera a R sobre F empezando por generar a las potencias de α :

Elevando ambos miembros de la ecuación $u = v'_k\alpha^k$ a la potencia i para cada $i = 0, \ldots, p-1$ tenemos $u^i = v'^i_k\alpha^{ki}$. Ahora, definimos $\sigma_k : \{0, \ldots, p-1\} \to \{0, \ldots, p-1\}$ tal que para cada $i \in \{0, \ldots, p-1\}$, tomamos el residuo de ik al dividir por p, es decir, $\sigma_k(i)$ es el único entero elemento de $\{0, \ldots, p-1\}$ tal que $\sigma_k(i) \equiv ik (\mathrm{mod}\ p)$. Dado que k es primo relativo con p, σ_k es inyectiva, si $i, j \in \{0, \ldots, p-1\}$ son tales que $\sigma_k(i) = \sigma_k(j)$, entonces $ik \equiv jk (\mathrm{mod}\ p)$ así que $i \equiv j (\mathrm{mod}\ p)$ y así $i = j$. Además como $\{0, \ldots, p-1\}$ es finito, σ_k es una permutación del conjunto $\{0, \ldots, p-1\}$. Ahora, $ik - \sigma_k(i) = p \cdot m$ para algún $m \in \mathbb{Z}$ (que depende de i y de k) así que $\alpha^{ik} = (\alpha^p)^m\alpha^{\sigma_k(i)}$ y como $\alpha^p = a$, denotando $b_i = (v'^i_k a^m)^{-1}$, $b_i \in F$ para cada i, tenemos que

$b_i u^i = (v'^i_k a^m)^{-1} v'^i_k \alpha^{ki} = (a^m)^{-1}(a)^m \alpha^{\sigma_k(i)} = \alpha^{\sigma_k(i)}$ para cada i.

Esto muestra que u genera a las potencias de α sobre F y por eso genera a R, explícitamente:

Cada $x \in R$ tiene una expresión de la forma

$$x = \sum_{i=0}^{p-1} x_i\alpha^i \text{ con } x_i \in F \text{ para } i = 0, \ldots, p-1.$$

$$= \sum_{i=0}^{p-1} x_{\sigma_k(i)}\alpha^{\sigma_k(i)} \text{ pues } \sigma_k \text{ es una permutación de } \{0, \ldots, p-1\}$$

$$= \sum_{i=0}^{p-1} x_{\sigma_k(i)} b_i u^i \text{ con } x_{\sigma_k(i)} b_i \in F \text{ para } i = 0, \ldots, p-1.$$

Esto prueba que $F(u) = R$. En cuanto a $v = v'_0 + v'_1\alpha + \cdots + v'_{p-1}\alpha^{p-1}$, calculando el coeficiente de u en la expresión anterior para v, tenemos que $\sigma_k(1) = k$ así que $m = 0$ y $b_1 = (v'_k)^{-1}$ así que para v, $x_{\sigma_k(1)} b_1 = 1$ y entonces hay $v_0, v_2, \ldots, v_{p-1} \in F$ tales que $v = v_0 + u + v_2u^2 + \cdots + v_{p-1}u^{p-1}$. ■

El siguiente lema nos ayudará a simplificar unas grandes sumas; es también un resultado general, válido en cualquier campo.

Lema 3. Sea p un número primo, y ζ una raíz $p-ésima$ primitiva de la unidad. Entonces, para cada $i \in \mathbb{Z}$,

$$1 + \zeta^i + \zeta^{2i} + \cdots + \zeta^{(p-1)i} = \begin{cases} 0 & \text{si } p \text{ no divide a } i \\ p & \text{si } p \text{ divide a } i \end{cases}$$

Demostración. Si p divide a i, $1 + \zeta^i + \zeta^{2i} + \cdots + \zeta^{(p-1)i} = 1 + 1 + 1^2 + \cdots + 1^{p-1} = p$.

Si p no divide a i, tenemos $(1 - \zeta^i)(1 + \zeta^i + \cdots + (\zeta^i)^{p-1}) = 1 - (\zeta^i)^p = 0$

y dado que p no divide a i, $1 - \zeta^i \neq 0$, de manera que

$1 + \zeta^i + \zeta^{2i} + \cdots + \zeta^{(p-1)i} = 0$. ■

El siguiente lema es específicamente acerca de nuestra extensión $L : K$ definida al inicio del capítulo, nuevamente usamos algunas propiedades del grupo simétrico S_n.

Lema 4. La extensión $L : K$ es algebráica, es decir, cada elemento de L es algebráico sobre K. Más aún, para cada $y \in L$, el polinomio irreducible de y sobre K se descompone sobre L.

Demostración. Sea $y \in L$, si $\sigma \in S_n$, tenemos un $K-automorfismo$ de L que podemos extender a un homomorfismo de anillos $\sigma : L[x] \longrightarrow L[x]$ (σ denota al elemento de S_n, al $K - automorfismo$ de L y al endomorfismo de $L[x]$) definiendo $\sigma(x) = x$, así que si $h \in L[x]$, $h = a_0 + a_1x + \cdots + a_mx^m$, $\sigma(h) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_m)x^m$. Sea $\{\sigma_1, \ldots, \sigma_r\} = S_n$ (de hecho $r = n!$) y definimos $\sigma_s(y) = y_s$, supongamos que σ_1 es el neutro de S_n para que $y_1 = y$.

Sea $g \in L[x]$ el polinomio $g(x) = (x - y_1)(x - y_2)\cdots(x - y_r)$ del cual y es una raíz, para cualquier $\tau \in S_n$, $\{\tau\sigma_1, \ldots, \tau\sigma_r\} = S_n$ de donde $\tau(g) = g$ y de aquí que los coeficientes de g están fijos bajo la acción del grupo S_n y por eso están en K y $g \in K[x]$, así que y es algebráico sobre K. Ahora, el polinomio irreducible de y sobre K debe ser uno de los factores irreducibles de g en $K[x]$, así que también se descompone en L. ■

El siguiente lema también es específicamente acerca de los campos K y L, hacemos uso de los 4 lemas anteriores para demostrar este.

Lema 5. Sea $E : K$ una extensión del campo K, p un número primo y $a \in E$ tal que a no es una potencia $p - ésima$ en E. Sea α una raíz de $x^p - a \in E[x]$, $M = E(\alpha) \cap L$ y $M_0 = E \cap L$ y supongamos que $E(\alpha)$ y L están contenidos en una extensión común del campo K. Si $M \neq M_0$ entonces $M : M_0$ es una extensión pura, es decir, hay un $\beta \in M$ tal que $\beta^p \in M_0$ y β genera a M sobre M_0 ($M_0(\beta) = M$).

Demostración. Sea $y \in M$ tal que $y \notin M_0$, así que $y \in E(\alpha) \cap L$ y por eso $y \in L$, pero dado que $y \notin E \cap L$, $y \notin E$; además $y \in E(\alpha)$, así que por Lema 2 existe $\beta \in E(\alpha)$ tal que $E(\beta) = E(\alpha)$, $\beta^p = b \in E$ pero b no es potencia $p - ésima$ en E y $y = b_0 + \beta + b_2\beta^2 + \cdots + b_{p-1}\beta^{p-1}$ donde $b_0, b_2, \ldots, b_{p-1} \in E$. Como $y \in L$, ahora por el Lema 4, y es algebráico sobre K, sea $g \in K[x]$
el polinomio irreducible de y sobre K y además g se descompone sobre L.

Sea $G(x) = g(b_0 + x + b_2x^2 + \cdots + b_{p-1}x^{p-1})$, $G \in E[x]$ y β es una raíz de G. Por el Lema 1.*ii*), $x^p - b \in E[x]$ es irreducible, entonces $x^p - b$ divide a G. Sea ζ una raíz $p-ésima$ primitiva de la unidad, como β es raíz de $x^p - b$, $\zeta^i\beta$ es raíz de $x^p - b$ para cualquier $i \in \mathbb{Z}$ y $\zeta^i\beta$ es raíz de G, así que los números

$$\begin{aligned} y = y_1 &= b_0 + \beta + b_2\beta^2 + \cdots + b_{p-1}\beta^{p-1} \\ y_2 &= b_0 + \zeta\beta + b_2\zeta^2\beta^2 + \cdots + b_{p-1}\zeta^{p-1}\beta^{p-1} \\ y_3 &= b_0 + \zeta^2\beta + b_2\zeta^{2(2)}\beta^2 + \cdots + b_{p-1}\zeta^{(p-1)(2)}\beta^{p-1} \\ &\vdots \\ y_p &= b_0 + \zeta^{p-1}\beta + b_2\zeta^{2(p-1)}\beta^2 + \cdots + b_{p-1}\zeta^{(p-1)(p-1)}\beta^{p-1} \end{aligned}$$

son raíces de g, el cual se descompone sobre L y así $y_1, \ldots, y_p \in L$, multiplicando cada y_i por ζ^{1-i} tenemos que

$$\begin{aligned} y = y_1 &= b_0 + \beta + b_2\beta^2 + \cdots + b_{p-1}\beta^{p-1} \\ \zeta^{-1}y_2 &= \zeta^{p-1}b_0 + \beta + b_2\zeta\beta^2 + \cdots + b_{p-1}\zeta^{p-2}\beta^{p-1} \\ \zeta^{-2}y_3 &= \zeta^{p-2}b_0 + \beta + b_2\zeta^2\beta^2 + \cdots + b_{p-1}\zeta^{(p-2)(2)}\beta^{p-1} \\ &\vdots \\ \zeta^{1-p}y_p &= \zeta b_0 + \beta + b_2\zeta^{p-1}\beta^2 + \cdots + b_{p-1}\zeta^{(p-2)(p-1)}\beta^{p-1} \end{aligned}$$

y al sumar teniendo en cuenta el Lema 3., tenemos que

$\beta = \frac{1}{p}\sum_{i=1}^{p} \zeta^{1-i}y_i \in L$. Así que $\beta \in E(\alpha) \cap L = M$ y $\beta^p = b \in E \cap L = M_0$. Así, $M_0(\beta) \subseteq M$ pues $M_0 \subseteq M$ y $\beta \in M$. Falta ver que $M \subseteq M_0(\beta)$, es decir, que β genera a M sobre M_0.

Sea $\gamma \in M$, así que $\gamma \in L$ y $\gamma \in E(\alpha)$, y como $E(\alpha) = E(\beta)$ entonces existen $c_0, \ldots, c_{p-1} \in E$ tales que $\gamma = c_0 + c_1\beta + c_2\beta^2 + \cdots + c_{p-1}\beta^{p-1}$. Ahora, como $\gamma \in L$, por el Lema 4 γ es algebráico sobre K, sea $f \in K[x]$ el polinomio irreducible de γ sobre K y además f se descompone sobre L. Sea $H(x) = f(c_0 + c_1x + c_2x^2 + \cdots + c_{p-1}x^{p-1})$, $H \in E[x]$ y β es una raíz de H, recordando que $x^p - b \in E[x]$ es irreducible y $\beta^p = b$ tenemos que $x^p - b$ divide a H y nuevamente $\zeta^i\beta$ es raíz de H para cualquier $i \in \mathbb{Z}$ y los números

$\gamma_i = c_0 + c_1\zeta^{i-1}\beta + \cdots + c_{p-1}\zeta^{(i-1)(p-1)}\beta^{p-1}$

$i = 1, \ldots, p$, son raíces de f, el cual se descompone sobre L y entonces $\gamma_1, \ldots, \gamma_p \in L$.

Ahora, sea $k \in \{0, \ldots, p-1\}$. Multiplicamos cada γ_i por $\zeta^{k(1-i)}$ y

$$\begin{aligned}
\gamma = \gamma_1 &= c_0 + c_1\beta + c_2\beta^2 + \cdots + c_k\beta^k + \cdots + c_{p-1}\beta^{p-1} \\
\zeta^{k(1-2)}\gamma_2 &= c_0\zeta^{-k} + c_1\zeta^{1-k}\beta + c_2\zeta^{2-k}\beta^2 + \cdots + c_k\beta^k + \cdots + c_{p-1}\zeta^{p-1-k}\beta^{p-1} \\
\zeta^{k(1-3)}\gamma_3 &= c_0\zeta^{-2k} + c_1\zeta^{2(1-k)}\beta + c_2\zeta^{2(2-k)}\beta^2 + \cdots + c_k\beta^k + \cdots + c_{p-1}\zeta^{2(p-1-k)}\beta^{p-1} \\
&\vdots \\
\zeta^{k(1-p)}\gamma_p &= c_0\zeta^{(1-p)k} + c_1\zeta^{(p-1)(1-k)}\beta + \cdots + c_k\beta^k + \cdots + c_{p-1}\zeta^{(p-1)(p-1-k)}\beta^{p-1}
\end{aligned}$$

y sumando los $\zeta^{k(1-i)}\gamma_i$ teniendo en mente el Lema 3. obtenemos $c_k\beta^k = \frac{1}{p}\sum_{i=1}^{p} \zeta^{k(1-i)}\gamma_i \in L$.

Dado que $\beta \in L$, $c_k \in L$ así que $c_0, \ldots, c_{p-1} \in E \cap L = M_0$ y entonces $\gamma \in M_0(\beta)$. Así que $M_0(\beta) = M$ y $M : M_0$ es una extensión pura. ■

Este último lema contiene el argumento fuerte para el siguiente teorema, es la sencilla razón de ser del teorema.

Teorema. Si L está contenido en una extensión radical de K, entonces $L : K$ es una extensión radical.

Demostración. Supongamos que $L \subseteq E$ y que $E : K$ es una extensión radical, digamos que $E_0, \ldots, E_m$ son tales que $K = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_m = E$ y para cada $i = 0, \ldots, m-1$, $E_{i+1} : E_i$ es una extensión pura, en otras palabras, existe $\alpha_i \in E_{i+1}$ tal que $E_{i+1} = E_i(\alpha_i)$ y $\alpha_i^{p_i} \in E_i$ para algún número primo p_i. Ahora, observamos $K = E_0 \cap L \subseteq E_1 \cap L \subseteq \cdots \subseteq E_{m-1} \cap L \subseteq L$:

Si $E_{i+1} \cap L = E_i \cap L$, podemos eliminar una; si $E_{i+1} \cap L \neq E_i \cap L$ entonces, por el Lema 5, $E_{i+1} \cap L : E_i \cap L$ es una extensión pura, mostrando que $L : K$ es una extensión radical. ■

Observaciones.

1. Al enunciar la contrapositiva del teorema y, dado que si $n \geq 5$ la extensión de campo $L : K$ no es radical, podemos concluir que el campo L no está contenido en ninguna extensión radical de K.

2. Dado que L es el campo de descomposición de $P \in K[x]$, el polinomio P no es soluble por radicales si $n \geq 5$.

ESTA TESIS NO DEBE
SALIR DE LA BIBLIOTECA

Bibliografía

1. M. F. Atiyah, Introduction to Commutative Algebra, Addison-Wesley, Reading-Mass.; 1969.
2. H. M Edwards, Galois Theory, Springer Verlag, New York-Berlin-Heidelberg,1984.
3. J. B. Fraleigh, Álgebra Abstracta, Addison-Wesley Iberoamericana, 1987.
4. N. Jacobson, Basic Algebra I, W. H. Freeman and Co., San Francisco 1974.
5. S. Roman, Field Theory, Springer Verlag, New York-Berlin-Heidelberg-London, 1995.
6. M. I. Rosen, Niels Hendrik Abel and Equations of the Fifth Degree, The American Mathematical Monthly, June-July 1995, pp. 495-505, 1995.
7. J. Rotman, Galois Theory, Springer Verlag, New York-Berlin-Heidelberg-London-Paris, 1990.
8. R. Y. Sharp, Steps in Commutative Algebra, Cambridge University Press, 1990.
9. I. Stewart, Galois Theory, Chapman and Hall, London, 1973.
10. J. P. Tignol, Galois Theory of Algebraic Equations, Longman Scientific Technical co-published with John Wiley and Sons, New York, 1987.