0.1. Extensiones algebraicas.

Teorema y definición 1. *(Parecido a ejercicio 4 de la sec 4.2) Sea F una extensión del campo ky sea $a \in F$ tal que a es algebraico sobre K. Entonces existe un único polinomio mónico en $K[x]$ de grado mínimo que tiene a a como raíz. Dicho polinomio se llama el* ***polinomio mínimo*** *de a sobre K, y se denota $irr_K(a)$. Además, para todo $f(x) \in K[x]$ se tiene que $f(a) = 0$ si y sólo si el polinomio mínimo de a sobre K divide a $f(x)$ en $K[x]$.*

Demostración: El conjunto I de todos los polinomios en $K[x]$ que anulan a a es un ideal de $K[x]$, por lo que tiene un único generador mónico de grado mínimo, denotémoslo $p(x)$ por el momento. Note que para $f(x)$ en $K[x]$, $f(x)$ anula a a si y solamente $f(x)$ está en I, que ocurre si y solamente si $p(x)$ divide a $f(x)$. Finalmente, si $p(x) = q(x)h(x)$ con $q(x)$ y $h(x)$ de grado menor que $p(x)$, evaluando en a tendríamos que $0 = p(a) = q(a)h(a)$, de donde $q(a) = 0$ o $h(a) = 0$, contradiciendo la minimalidad del grado de $p(x)$ (que es el polinomio de menor grado en $K[x]$ que anula a a).

0.2. Generadores de una extensión.

Ejercicio 1. Sea F una extensión del campo ky sea $a \in F$ algebraico sobre K. Demuestre que $K(a)$ es isomorfo al anillo cociente $K[x]/ < irr_K(a) >$. Concluya que si a y b son elementos en sendas extensiones de K tales que a y b tienen el mismo polinomio irreducible sobre K, entonces $K(a)$ es isomorfo a $K(b)$ (con un único isomorfismo que manda a en b). Muestre con un contraejemplo que $K(a)$ puede ser isomorfo a $K(b)$ sin que a y b tengan el mismo polinomio irreducible sobre K (note que el isomorfismo no puede mandar a en b).

0.3. Extensiones separables.

Definición 2. Sea k un campo y sea $f(x) \in k[x]$. Decimos que $f(x)$ es un polinomio **separable** sobre k si ninguno de sus factores irreducibles en $k[x]$ tiene raíces múltiples (en el campo de descomposición de $f(x)$).

Ejercicio 2. Sea k un campo y sea $f(x) \in k[x]$ un polinomio. Demuestre que si $f(x)$ no tiene raíces múltiples entonces $f(x)$ es separable sobre k. Muestre con un ejemplo que el inverso no es cierto.

Ejercicio 3. Sea k un campo y sea $f(x) \in k[x]$ un polinomio. Demuestre que $f(x)$ es separable sobre k si y sólo si para cualesquiera polinomios irreducibles $p(x)$ y $q(x)$ no asociados que dividan a $f(x)$ en $k[x]$ se tiene que p y q son primos relativos en $k[x]$.

Ejercicio 4. ¿Falso o verdadero? Demostrar o dar contraejemplo. *Sea k un campo y F una extensión de k. Sea $f(x) \in k[x]$. Entonces $f(x)$ es separable sobre k si y solamente si $f(x)$ es separable sobre F.*

Definición 3. Sea k un campo y sea F una extensión de k. Sea $a \in F$. Decimos que a es un **elemento separable** sobre k si a es trascendente sobre k o si su polinomio mínimo sobre k es separable sobre k. Decimos que F es una **extensión separable** de k si todo elemento en F es separable sobre k.

Ejercicio 5. Sea k un campo de característica p, y sea $f(x) = x^p - a$ para algún $a \in k$. Demuestre que $f(x)$ tiene una única raíz de multiplicidad p en su campo de descomposición. Concluya que dos factores irreducibles cualesquiera de $f(x)$ tienen que ser asociados. Demuestre que o bien $f(x)$ es irreducible en $k[x]$, o se factoriza como $(x-b)^p$ para algún $b \in k$.

Ejercicio 6. Sea $k = \mathbb{F}_p(t)$, y sea $f(x) \in k[x]$ el polinomio $f(x) = x^p - t$. Demuestre que $f(x)$ es irreducible sobre k, y que el campo de descomposición de $f(x)$ es una extensión no separable de k.

Ejercicio 7. Muestre un ejemplo de un polinomio $f(x)$ en $k[x]$ tal que $f(x)$ no sea separable sobre k, pero que sea separable para una extensión algebraica de k.

0.4. Grupo de Galois.

Ejercicio 8. Calcule $Gal(\mathbb{C}, \mathbb{R})$.

Ejercicio 9. Calcule $Gal(\mathbb{Q}(\sqrt{2}), \mathbb{Q})$, $Gal(\mathbb{Q}(\sqrt{3}), \mathbb{Q})$ y $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q})$.

Ejercicio 10. Calcule $Gal(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q})$,

Ejercicio 11. Sean k y k' campos y sea $\sigma : k \longrightarrow k'$ un isomorfismo de campos. Sea $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in k[x]$ un polinomio irreducible, y sea $q(x) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n$ el correspondiente polinomio irreducible en $k'[x]$. Sean β una raíz de $p(x)$ y β' una raíz de $q(x)$. Demuestre

que existe un único isomorfismo $\tau : k(\beta) \longrightarrow k'(\beta')$ que extiende a σ y tal que $\tau(\beta) = \beta'$. (Sugerencia: ya antes había demostrado la existencia de dicho isomorfismo, por lo que solamente debe demostrar la unicidad).

Ejercicio 12. Sea $k = \mathbb{Q}$, y sean $f(x) = x^3 - 5$, $g(x) = x^2 - 7$ y $h(x) = f(x)g(x)$ polinomios en $\mathbb{Q}[x]$. Sean F el campo de descomposición de $f(x)$ sobre $\mathbb{Q}$, y H el campo de descomposición de $g(x)$ sobre F. Demuestre que H es el campo de descomposición de $h(x)$ sobre $\mathbb{Q}$. Calcule el orden de $Gal(F, k)$, $Gal(H, F)$ y $Gal(H, k)$. Calcule el grado $[F : k]$, $[H : F]$ y $[H : k]$.

Esquema de solución: Tanto $g(x)$ como $f(x)$ se factorizan totalmente en H, por lo que H contiene un campo de descomposición de $h(x)$. Observe que dicho campo de descomposición de $h(x)$ debe contener a F. Los grados son: $[F : k] = 6$, $[H : F] = 2$ y $[H : k] = 12$. Los órdenes de los grupos de Galois son los grados de las correspondientes extensiones.

Proposición 4. *Sean k un campo, $f(x) \in k[x]$ y F el campo de descomposición de $f(x)$. Entonces el orden de $Gal(F, k)$ es menor o igual al grado de F sobre k. Además, se tiene igualdad si $f(x)$ es separable.*

Demostración: Ya se demostró antes.

Proposición 5. *Sea F un campo y G un subgrupo del grupo de automorfismos de F. Sea k el campo fijo de G. Entonces $[F : k] \leq |G|$.*

Demostración: Ya se demostró antes.

0.5. Extensiones normales.

Definición 6. Sea F una extensión del campo k. Decimos que F es una extensión **normal** de k si todo polinomio irreducible en $k[x]$ que tenga una raíz en F se factoriza totalmente en F.

Ejercicio 13. Sea F una extensión algebraica de k. Demuestre que F es una extensión normal de k si y sólo si para todo $a \in F$, F tiene todas las raíces del polinomio mínimo de a sobre k.

Ejemplo 7. El campo $\mathbb{Q}(\sqrt[3]{2})$ no es una extensión normal de $\mathbb{Q}$. El elemento $\sqrt{2}$ está en dicha extensión, y su polinomio mínimo sobre $\mathbb{Q}$ es $x^3 - 2$, que no tiene todas sus raíces en $\mathbb{Q}(\sqrt[3]{2})$, puesto que le faltan las dos raíces complejas.

Teorema 8. *Sea F una extensión del campo k. Las tres condiciones siguientes son equivalentes:*

(a) F es el campo de descomposición de un polinomio separable $f(x) \in k[x]$.

(b) k es el campo invariante de un grupo finito de automorfismos G de F.

(c) F es de grado finito, normal y separable sobre k.

Más aún, si k y F son como en (a) y $G = Gal(F, k)$, entonces $k = Inv(G)$; si G y k son como en (b), entonces $G = Gal(F, k)$.

Demostración: (a) implica (b): Sea G el grupo de Galois de F sobre k, y sea k' el campo fijo de G. Entonces k' es un subcampo de F que contiene a k. Además tenemos que F es campo de descomposición de $f(x)$ sobre k' (ya sabemos que F es campo de descomposición de $f(x)$ sobre k), y G es también el grupo de Galois de F sobre k'. Por un resultado anterior, el orden de G es $[F : k]$, pero también es $[F : k']$. Puesto que $k \leq k' \leq F$, esto implica que $k = k'$, por lo que (b) se cumple (para el grupo de Galois G). Además, demostramos el primero de los enunciados suplementarios.

(b) implica (c): Por un resultado anterior, $[F : k] \leq G$, por lo que F es de grado finito sobre k. Sea $f(x)$ un polinomio irreducible mónico en $k[x]$ que tiene una raíz en F. Debemos demostrar que $f(x)$ se factoriza totalmente sobre F como producto de factores lineales distintos (para concluir que F es normal y separable sobre k). Sea R el conjunto de todas las imágenes de r bajo los elementos del grupo G dado en (b), y sea $g(x) = \prod_{s \in R}(x - s)$. Afirmamos que $g(x)$ es un polinomio en $k[x]$ que anula a r y divide a $f(x)$ en $F[x]$, y como $f(x)$ es el polinomio irreducible de r sobre k, esto concluirá que $f(x)$ divide a $g(x)$ sobre k (y sobre F), por lo que $f(x) = g(x)$, es decir, $f(x)$ es como deseamos. Para ver que $g(x)$ divide a $f(x)$ sobre F, note que $f(s) = 0$ para toda $s \in R$, pues los elementos de G son automorfismos que fijan a los coeficientes de $f(x)$, y mandan a r (que es una raíz de $f(x)$) en otras raíces de $f(x)$. Así tenemos que $f(x)$ es divisible por todos los $x - s$ con $s \in R$, por lo que es divisible (en $F[x]$) por su producto, que es $g(x)$. Para ver que $g(x)$ tiene coeficientes en k, basta notar que los coeficientes de $g(x)$ son invariantes bajo todos los elementos de G (pues el campo fijo de G es k). Observe que dado un automorfismo σ en G, este induce un automorfismo en $F[x]$ que manda a $g(x)$ en $\sigma(g(x)) = \sigma(\prod_{s \in R}(x - s)) = \prod_{s \in R}(x - \sigma(s)) = \prod_{s \in R}(x - s) = g(x)$, por lo que los coeficientes de $g(x)$ quedan fijos bajo σ, por lo que $g(x) \in k[x]$.

(c) implica (a): Puesto que $[f : k]$ es finito, sabemos que F es una ex-

tensión algebraica de k, digamos $F = k(r_1, \ldots, r_t)$. Sean $f_i(x)$ el polinomio irreducible de r_i sobre k, y sea $f(x)$ el producto de todos los $f_i(x)$. Afirmamos que $f(x)$ es separable sobre k, y que su campo de descomposición sobre k es F, lo que establecerá (a). Por hipótesis, $f_i(x)$ debe ser separable (pues es el irreducible de un elemento en F, que es una extensión separable de k), y $f_i(x)$ debe tener todas sus raíces en F (pues F es una extensión normal de k, y $f_i(x)$ es un irreducible en $k[x]$ que tiene al menos una raíz en F). De esto se sigue que el producto de los $f_i(x)$ es separable, y que se factoriza totalmente en F, que debe ser el campo de descomposición de $f(x)$ (pues F tiene todas las raíces de $f(x)$, y F se obtiene de k agregando algunas raíces de $f(x)$).

Solamente resta demostrar el segundo enunciado complementario. Vimos que bajo las hipótesis de (b) se tiene que $[F : k] \leq G$, y como se cumple (c), se tiene que el orden del grupo de Galois de F sobre k es $[F : k]$. Puesto que $G \leq Gal(F, k)$ y $|G| \geq [F : k] = |Gal(F, k)|$, se sigue que $G = Gal(F, k)$.

0.6. Teorema fundamental de la teoría de Galois.

Teorema 9. *(Teorema Fundamental de la Teoría de Galois) Sea F una extensión normal, separable y de dimensión finita sobre k. Sea $G = Gal(F, k)$, y sea Λ la familia de los subgrupos de G. Sea Σ la familia de los campos intermedios entre k y F. Las funciones $H \mapsto Inv(H)$ y $E \mapsto Gal(F, E)$ con $H \in \Lambda$ y $E \in \Sigma$ son inversas, y por tanto son biyecciones entre Λ y Σ. Más aún, tenemos las siguientes propiedades:*

(1) $H_2 \leq H_1$ si y sólo si $Inv(H_1) \leq Inv(H_2)$

(2) $|H| = [F : Inv(H)]$, $[G : H] = [Inv(H) : k]$

(3) H es normal en G si y sólo si $Inv(H)$ es normal sobre k. En este caso, $Gal(Inv(H), k) \cong G/H$.

Demostración: Veamos primero que los mapeos $H \mapsto Inv(H)$ y $E \mapsto Gal(F, E)$ son inversos. Sea H un subgrupo de G. Sea $E = Inv(H)$. Note que $k \leq E \leq F$. Por la parte suplementaria del Teorema 8 para H en vez de G, vemos que H es el grupo de Galois de F sobre E, por lo que la primera composición de los mapeos dados es la identidad. Observe que también se tiene que $|H| = [F : Inv(H)]$, por un resultado anterior, y puesto que H es el grupo de Galois de F sobre $Inv(H)$.

Ahora sea E un campo intermedio entre k y F, y sea H el grupo de Galois de F sobre E. Es claro que H es un subgrupo de G. Note también que F es campo de descomposición sobre E de un polinomio separable (pues lo era sobre k, que está contenido en E). La parte suplementaria del Teorema 8 para F y E nos dice que el campo fijo de H es E. Esto termina la demostración de que los mapeos $H \mapsto Inv(H)$ y $E \mapsto Gal(F, E)$ son inversos.

La parte (1) es clara, pues mientras mayor sea el subgrupo de G, menor será su campo fijo, e inversamente, mientras menor sea el campo intermedio, mayor será su grupo de Galois asociado (pues más automorfismos de F lo fijan).

La primera parte de (2) ya se había establecido en lo que va de la demostración. Puesto que $|G| = [F : k] = [F : Inv(H)][Inv(H) : k] = |H|[Inv(H) : k]$, se tiene que $[G : H] = [Inv(H) : k]$, lo que completa (2).

Resta demostrar la parte (3). Sea H un subgrupo de G, y sea E su campo fijo. Para cualquier automorfismo σ en G, note que el campo fijo de $\sigma H \sigma^{-1}$ es la imagen $\sigma(E)$, puesto que la condición $\tau(a) = a$ es equivalente a pedir que $(\sigma\tau\sigma^{-1})(\sigma(a)) = \sigma(a)$. Se sigue entonces que H es un subgrupo normal de G si y solamente si $\sigma(E) = E$ para toda σ en G.

Suponga que esto último ocurre. Para cualquier σ en G, su restricción a E está bien definida, y esto define un homomorfismo de grupos de G al grupo de Galois de E sobre k. La image de este homomorfismo es un grupo de automorfismos de E cuyo campo fijo es k, por lo que la imagen debe ser todo el grupo de Galois de E sobre k. Por otro lado, el núcleo de este homomorfismo de grupos es el conjunto de automorfismos σ en G tales que σ restringido a E es la identidad, que por la correspondencia ya establecida, debe ser el grupo de Galois de F sobre E, que es el H con el que empezamos. Por el primer teorema de isomorfismo para grupos, tenemos que el grupo de Galois de E sobre k es isomorfo a G/H. Más aún, como el campo fijo del grupo de Galois de E sobre k es k, por el Teorema 8 tenemos que E es una extensión normal de k.

Finalmente, suponga que E es una extensión normal de k, y sea H su sugrupo correspondiente bajo la biyección anterior. Resta demostrar que H es normal en G, o equivalentemente, que $\sigma(E) = E$ para toda σ en G. Sea a en E arbitrario, y sea $f(x)$ el polinomio irreducible de a sobre k. Entonces $f(x)$ se factoriza totalmente sobre E (pues E es una extensión normal de k), lo que significa que para toda σ en G, $\sigma(a)$ vuelve a caer en E (pues $\sigma(a)$ debe ser raíz de $f(x)$, y $f(x)$ tiene todas sus raíces en E). Hemos establecido

que $\sigma(E) \subset E$. Note que $\sigma(E)$ y E son extensiones finitas de k del mismo grado (pues E tiene grado igual a $[G : H]$, y $\sigma(E)$ tiene grado $[G : \sigma H \sigma^{-1}]$), por lo que $\sigma(E) = E$, lo que termina nuestra demostración.

Definición 10. Sea k un campo y sea $f(x) \in k[x]$ un polinomio no constante. El grupo de Galois de $f(x)$ sobre k es el grupo de Galois de un campo de descomposición de $f(x)$ sobre k.

Ejercicio 14. Sea k un campo y sea $f(x) \in k[x]$ un polinomio de grado positivo n. Demuestre que el grupo de Galois de $f(x)$ es isomorfo a un subgrupo de S_n. *Sugerencia:* Dado un automorfismo en el grupo de Galois de $f(x)$, demuestre que induce una permutación en el conjunto de raíces de $f(x)$, que tiene a lo más n elementos.

Ejemplo 11. Calcule el grupo de Galois de $x^3 - 2$ sobre $\mathbb{Q}$. Calcule los subcampos del campo de descomposición de $x^3 - 2$ sobre $\mathbb{Q}$, y diga cuáles son extensiones normales de $\mathbb{Q}$.

Sea F el campo de descomposición de $x^3 - 2$ sobre $\mathbb{Q}$. Notemos primero que las tres raíces de $x^3 - 2$ son $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$ y $\sqrt[3]{2}\omega^2$, donde ω es una de las dos raíces cúbicas primitivas de la unidad. Se sigue entonces que el campo de descomposición de $x^3 - 2$ sobre $\mathbb{Q}$ se obtiene de $\mathbb{Q}$ agregando $\sqrt[3]{2}$ y ω. Agregando primero $\sqrt[3]{2}$ obtenemos una extensión de $\mathbb{Q}$ de grado 3, y al agregar ω obtendremos una extensión de grado no mayor a dos (pues el grado de ω sobre $\mathbb{Q}$ es dos). Tenemos entonces que $[F : \mathbb{Q}]$ es 3 o 6. Por otro lado, como $\mathbb{Q}(\omega)$ es un subcampo de F, sabemos que $[F : \mathbb{Q}] = [F : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] = [F : \mathbb{Q}(\omega)]2$, por lo que $[F : \mathbb{Q}] = 6$. Como $x^3 - 2$ tiene grado 3, el grupo de Galois de F sobre $\mathbb{Q}$ es un subgrupo de S_3. Por otro lado, como F es campo de descomposición de un polinomio separable sobre $\mathbb{Q}$, sabemos que el orden del grupo de Galois de F sobre $\mathbb{Q}$ es el grado $[F : \mathbb{Q}] = 6$, de donde dicho grupo de Galois es S_3.

Calculemos ahora los campos intermedios entre F y $\mathbb{Q}$. Claramente F y $\mathbb{Q}$ son extensiones normales, por lo que nos concentraremos en los campos intermedios propiamente contenidos en F que contienen propiamente a $\mathbb{Q}$. Al menos podemos construir $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}\omega)$, $\mathbb{Q}(\sqrt[3]{2}\omega^2)$ y $\mathbb{Q}(\omega)$, que son extensiones de grados 3, 3, 3 y 2 respectivamente. La pregunta es si hay algunos otros campos intermedios que no estemos considerando. La respuesta es que ya son todos los campos intermedios, puesto que los subgrupos de S_3 (aparte del trivial y el total) son 3 subgrupos de orden 2 y un subgrupo de

orden 3. Los tres subgrupos de orden 2 se corresponden con las tres extensiones de grado 3 (recuerde que el grado de la extensión es el índice de su subgrupo correspondiente, no su orden), y el subgrupo de orden 3 (que es el único subgrupo normal propio no trivial de S_3) se corresponde con la única extensión propia normal, que tiene grado 2, es decir, $\mathbb{Q}(\omega)$.

Ejemplo 12. Calcule el grupo de Galois de $(x^2-3)(x^2-5)$ sobre $\mathbb{Q}$. Calcule los subcampos del campo de descomposición de $(x^2-3)(x^2-5)$ sobre $\mathbb{Q}$, y diga cuáles son extensiones normales de $\mathbb{Q}$.

Sea F el campo de descomposición de $(x^2-3)(x^2-5)$ sobre $\mathbb{Q}$. Una cuenta rápida nos muestra que $[F:\mathbb{Q}]=4$. Como en el ejercicio anterior, observamos que F es campo de descomposición de un polinomio separable sobre $\mathbb{Q}$, por lo que el grupo de Galois de F sobre $\mathbb{Q}$ tiene orden 4. Sea G dicho grupo de Galois. Hay solamente dos grupos de orden 4 hasta isomorfismo, que son el cíclico de orden 4, y el grupo 4 de Klein.

Procedamos ahora a estudiar los campos intermedios entre $\mathbb{Q}$ y F. Note que al menos hay 3 subcampos intermedios de grado 2, a saber, $\mathbb{Q}(\sqrt{3}$, $\mathbb{Q}(\sqrt{5}$ y $\mathbb{Q}(\sqrt{15})$. Como hay una biyección entre subgrupos de G y campos intermedios entre $\mathbb{Q}$ y F, vemos que G tiene al menos 3 subgrupos de índice 2 (correspondientes a estos 3 campos intermedios de grado 2), por lo que podemos descartar el caso de que G sea cílico de orden 4, puesto que dicho grupo tiene solamente un subgrupo de índice 2. Tenemos entonces que G debe ser el grupo 4 de Klein. Más aún, los tres campos intermedios que encontramos son todos, pues el grupo 4 de Klein solamente tiene 3 subgrupos propios no triviales, y como todos son normales, tenemos que todos los campos intermedios son extensiones normales de $\mathbb{Q}$.

0.7. Apéndice I: Solubilidad por radicales.

Definición 13. Sea F un campo. Una **torre de campos** sobre F es una cadena de campos

$$F = F_1 < F_2 < \ldots < F_{r+1}.$$

Si además se cumple que $F_{i+1} = F_i(d_i)$ con $d_i^{n_i} \in F_i$ (n_i enteros positivos) para toda $i = 1, \ldots, r$, decimos que ésta es una **torre de raíces** sobre F. Sea $f(x) \in F[x]$ un polinomio mónico de grado positivo. Decimos que la ecuación $f(x) = 0$ es **soluble por radicales** sobre F si existe una torre de

raíces como la de arriba en la que F_{r+1} contiene un campo de descomposición de $f(x)$ sobre F.

Definición 14. Sea F un campo cualquiera, y sea n un entero positivo. El campo de descomposición del polinomio $x^n - 1$ sobre F se llama un **campo ciclotómico** de orden n sobre F.

Ejercicio 15. Sea F un campo de característica cero. Entonces el grupo de Galois del campo ciclotómico de orden n sobre F es abeliano. *Sugerencia:* Use el criterio de la derivada para ver que $x^n - 1$ tiene n raíces distintas. Dichas raíces forman un subgrupo cíclico U de las unidades del campo ciclotómico. Defina un homomorfismo inyectivo de grupos del grupo de Galois al grupo de automorfismos de U. Finalmente, los automorfismos de U son isomorfos al grupo de unidades del anillo de los enteros módulo n, que es abeliano.

Ejercicio 16. Sea F un campo que contiene n raíces n-ésimas distintas de la unidad, y sea a un elemento cualquiera de F. Entonces el grupo de Galois de $x^n - a$ sobre F es cíclico, y su orden divide a n. *Sugerencia:* Sea U el grupo de raíces n-ésimas del uno. Sabemos que U debe ser cíclico. Dada una raíz cualquiera r de $x^n - a$, demuestre que zr variando z en U son todas las raíces de $x^n - a$, y $E = F(r)$. Defina un homomorfismo inyectivo de grupos del grupo de Galois en U.

Ejercicio 17. Sea p un primo y suponga que F contiene p raíces distintas de la unidad. Sea E una extensión de F de dimensión p, con grupo de Galois cíclico. Entonces $E = F(d)$ donde $d^p \in F$. *Sugerencia:* Para cualquier c en E que no esté en F, se tiene $E = F(c)$. Sean $z_1, \ldots, z_p$ las raíces p-ésimas del uno. Sea η un generador del grupo de Galois de E sobre F. Defina $c_i = \eta^{i-1}(c)$, para $i = 1, \ldots, p$. Defina el resolvente de Lagrange $(z_i, c) = c_1 + c_2 z_i + c_3 z_i^2 + \cdots + c_p z_i^{p-1}$. Muestre que $\eta(z_i, c) = z_i^{-1}(z_i, c)$, $\eta(z_i, c)^p = (z_i, c)^p$ es elemento de F. Escriba $c_1, \ldots, c_p$ como combinaciones lineales de $(z_1, c), (z_2, c), \ldots, (z_p, c)$. Use el determinante de Vandermonde para este sistema. Concluya que $E = F(c) = F(d_1, d_2, \ldots, d_p)$ con $d_i = (z_i, c)$, y que por tanto alguna d_i no está en F. Tome $d = d_i$.

Ejercicio 18. Sea F una extensión del campo k, y sea $f(x) \in k[x]$. Entonces el grupo de Galois de $f(x)$ sobre F es isomorfo a un subgrupo del grupo de Galois de $f(x)$ sobre k. *Sugerencia:* Primero note que los campos de descomposición de $f(x)$ sobre k y sobre F se obtienen agregando las raíces de $f(x)$ a k y F respectivamente. Use el hecho de que un automorfismo está determinado por su acción en las raíces de $f(x)$.

Ejercicio 19. Sea $E = F(a_1, \ldots, a_n)$ una extensión finita de F. Sea $f_i(x)$ el polinomio mínimo de a_i sobre F y sea $f(x)$ el producto de los $f_i(x)$. Sea K un campo de descomposición de $f(x)$ sobre E. Demuestre que K también es campo de descomposición de $f(x)$ sobre F. Suponga que $f(x)$ es separable sobre F. Demuestre que cualquier extensión normal de E contiene un subcampo isomorfo a K. El campo K se llama la **cerradura normal** de E sobre F. Sea $\eta \in Gal(K, F)$. Un subcampo de K se la forma $\eta(E)$ se llama un **conjugado** del campo E sobre F. Sea K' el subcampo de K generado por todos los conjugados de E. Demuestre que $Gal(K, F)$ manda a K' en sí mismo, y por lo tanto determina un grupo finito de automorfismos G' de K' cuyo campo fijo es F. Concluya que K' es normal sobre F, y que $K' = K$. *Sugerencia:* Note que el campo de descomposición de $f_i(x)$ contiene a a_i. Use que en una extensión normal, todo polinomio irreducible que tenga al menos una raíz se debe factorizar totalmente. Compare con la demostración del Teorema Fundamental de la Teoría de Galois.

Ejercicio 20. Sea E una extensión de F, y suponga que existe una torre de raíces $F = F_1 < \ldots < F_{r+1} = E$ con $F_{i+1} = F_i(d_i)$, $d_i^{n_i} \in F_i$, y suponga además que E está generado sobre F por un conjunto finito de elementos cuyos polinomios mínimos son separables. Entonces la cerradura normal K de E sobre F tiene una torre de raíces sobre F cuyos enteros coinciden con los n_i. *Sugerencia:* Recuerde cuáles campos generan a la cerradura normal de $f(x)$. Dado un automorfismo η en el grupo de Galois de K sobre F, aplíquelo a la torre original para obtener una torre sobre F para $\eta(E)$. Demuestre que K se obtiene de F agregando todos los $\eta(d_i)$, corriendo sobre todas las η en el grupo de Galois, y todos los d_i. Use esto para construir la torre deseada.

Teorema 15. *(Criterio de Galois para solubilidad de una ecuación por radicales en característica cero) Sea F un campo de característica 0, y sea $f(x) \in F[x]$ un polinomio no constante. Se tiene que la ecuación polinomial $f(x) = 0$ es soluble por radicales sobre F si y sólo si el grupo de Galois de $f(x)$ sobre F es soluble.*

Demostración: Supongamos primero que $f(x) = 0$ es soluble por radicales sobre el campo F de característica cero, es decir, tenemos una extensión K de un campo de descomposición de $f(x)$ tal que K tiene una torre de raíces sobre F, digamos

$$F = F_1 < F_2 < \ldots < F_{r+1} = K$$

Por el Ejercicio 20, podemos suponer que K es normal sobre F. Como estamos en característica cero, tenemos separabilidad garantizada, y estamos en las hipótesis del Teorema Fundamental de la Teoría de Galois. Sea n el mínimo común múltiplo de los enteros n_i asociados con esta cadena. Podemos extender la cadena de K a $K(z)$ donde z es una raíz primitiva n-ésima de la unidad. Si K es campo de descomposición de $g(x)$, entonces $K(z)$ es campo de descomposición de $g(x)(x^n - 1)$, y también podemos aplicar el Teorema Fundamental a $K(z)$. Más aún, podemos reordenar la torre de campos para $K(z)$ para que su segundo término sea $F(z)$, es decir,

$$F = F_1 < F_2 = F(z) < F_3 = F_2(d_1) \ldots < K(z).$$

Note que cada F_{i+1} es una extensión normal, separable y de grado finito de F_i. Sea H el grupo de Galois de $K(z)$ sobre F. Demostraremos que H es un grupo soluble (H no es el grupo que nos interesa, pero es un paso hacia dicho grupo). Por el Ejercicio 15, tenemos que el grupo de Galois de F_2 sobre F_1 es abeliano. Para $i > 1$, cada F_i contiene las necesarias raíces n-ésimas de la unidad, y por el Ejercicio 16, el grupo de Galois de F_{i+1} sobre F_i es abeliano. Sea ahora H_i el grupo de Galois de de $K(z)$ sobre F_i, y note que H_i es un subgrupo de H. Más aún, como cada F_{i+1} es una extensión normal de F_i, tenemos que H_{i+1} es un subgrupo normal de H_i (recuerde que las contenciones se invierten). Por el Teorema Fundamental de la Teoría de Galois, el grupo cociente H_i/H_{i+1} es isomorfo al grupo de Galois de F_{i+1} sobre F_i, que acabamos de observar que es un grupo abeliano. Tenemos entonces que los H_i nos dan una serie normal para H con factores abelianos, por lo que H es un grupo soluble.

Sea E el campo de descomposición de $f(x)$ sobre F metido en $K(z)$. Por ser E una extensión normal de F, el grupo de Galois de E sobre F (que es el grupo que nos interesa) es isomorfo a un grupo cociente de H, y como cociente de grupo soluble es otra vez soluble, ya terminamos esta parte de la demostración.

Supongamos ahora que el grupo de Galois G de $f(x)$ sobre F es soluble. Sea $n = |G| = [E : F]$, donde E es el campo de descomposición de $f(x)$ sobre F. Sea $F_1 = F$, $F_2 = F(z)$ donde z es una raíz n-ésima primitiva de la unidad, y sea $K = E(z)$. Por el Ejercicio 18, el grupo de Galois de K sobre F_2 es isomorfo a un subgrupo H de G, por lo que H es soluble y tiene una serie de composición $1 = H_{r+1} \lhd ... \lhd H_2 \lhd H_1 = H$ cuyos factores de composición H_i/H_{i+1} son cíclicos de orden primo, digamos p_i, para

$1 \leq i \leq r$. Aplicando la correspondencia de Galois a esta cadena descendente de subgrupos, obtenemos una cadena ascendente de subcampos $F_2 < F_3 < F_{r+2} = K$ donde H_i es el grupo de Galois de K sobre F_{i+1}. Se sigue que F_{i+1} es normal sobre F_i con grupo de Galois cíclico de orden p_i. Puesto que p_i divide a n, n es el orden de G, y F_i contiene una raíz n-ésima primitiva de la unidad, F_i contiene p_i raíces p_i-ésimas de 1, y por el Ejercicio 17, tenemos que $F_{i+1} = F_i(d_i)$ donde $d_i^{p_i}$ está en F_i. Así vemos que K contiene una torre de raíces sobre F, y como K contiene el campo de descomposición de $f(x)$, hemos demostrado que la ecuación polinomial $f(x) = 0$ es soluble por radicales sobre F.

Ejercicio 21. Sea $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$. Demuestre que $f(x)$ es irreducible en $\mathbb{Q}[x]$, y que $f(x)$ tiene tres raíces reales y dos raíces complejas. Sea G el grupo de Galois de $f(x)$. Demuestre que G es (isomorfo a) un subgrupo de S_5. Demuestre que G contiene un ciclo de longitud 5 y una transposición. Concluya que G es isomorfo a S_5.

Ejercicio 22. (Teorema de Abel-Ruffini) Existe un polinomio de grado 5 en $\mathbb{Q}[x]$ que no es soluble por radicales. *Sugerencia:* El grupo S_5 no es soluble.

0.8. Apéndice II: Construcciones con regla y compás.

Para la mayor parte de esta sección utilizaremos solamente teoría básica de campos; para los últimos resultados (sobre polígonos construíbles) necesitaremos Teoría de Galois.

Comencemos esta sección con una pequeña introducción geométrica.

Dado un número finito de puntos $S = \{P_1, ..., P_n\}$ en el plano, defina un subconjunto S_m, con $m = 1, 2, ...$, del plano inductivamente haciendo $S_1 = S$, y S_{r+1} es la unión de S_r con los puntos de: (1) intersecciones de pares de rectas que conectan puntos distintos de S_r, (2) intersecciones de las líneas de (1) con todos los círculos centrados en puntos de S_r y radios dados por distancias entre puntos de S_r, (3) intersecciones de pares de círculos dados en (2). Sea $C(P_1, ..., P_n) = \cup_1^\infty S_i$. Diremos que un punto P del plano es construíble con regla y compás a partir de $P_1, ..., P_n$ si P es elemento de $C(P_1, ..., P_n)$. De lo contrario, P no puede construirse a partir de $P_1, ..., P_n$. Note que (1), (2) y (3) son precisamente el tipo de construcciones que uno puede realizar con regla y compás.

Procederemos a formular esta definición algebraicamente. Supongamos que al menos tenemos dos puntos, pues de lo contrario, $C(P_1) = \{P_1\}$. Escogemos en el plano un sistema cartesiano donde el primer punto es $P_1 = (0, 0)$, y $P_2 = (1, 0)$. Asociamos al punto $P = (x, y)$ el número complejo $x + iy$, con lo que el plano queda identificado con el campo de números complejos $\mathbb{C}$. La pregunta es entonces cuáles números complejos son construíbles con regla y compás a partir de un número finito de números complejos $z_1, ..., z_n$. La respuesta es que dicho conjunto, que denotaremos $C(z_1, ..., z_n)$, es el menor subcampo de $\mathbb{C}$ que contiene a los $z_1, ..., z_n$ y es cerrado bajo raíces cuadradas y conjugación.

Para convencernos de lo anterior, veamos la correspondencia entre operaciones algebraicas y geométricas en el conjunto $C(z_1, ..., z_n)$. La suma de z y z' se puede obtener según el método del paralelogramo, que encuentra el vector $z + z'$, y cuyo punto final es uno de los dos puntos de intersección del círculo con centro en z y radio $|z'|$ con el círculo con centro en z' y radio $|z|$. El inverso aditivo $-z$ es una reflección por el origen. Con esto vemos que $C(z_1, ..., z_n)$ es al menos un subgrupo del grupo aditivo de $\mathbb{C}$. Para ver que $C(z_1, ..., z_n)$ es cerrado bajo productos, inversos multiplicativos y raíces cuadradas, usamos la forma polar de $z = re^{i\theta}$ (y una similar para z'). El producto zz' tiene la forma $rr'e^{i(\theta+\theta')}$. Usando triángulos semejantes es posible construir rr', y un ángulo de amplitud $\theta + \theta'$ se obtiene fácilmente yuxtaponiendo los ángulos θ y θ'. Una ligera modificación a estas construcciones nos lleva a construir r/r' y $\theta - \theta'$, por lo que z/z' también es construíble (si $z' \neq 0$).

La construcción de $\sqrt{r}$ es un poco más elaborada, pues involucra un círculo de diámetro $r + 1$ y una recta perpendicular a un diámetro sobre un punto alejado una unidad de un extremo del diámetro, pero con ella uno concluye que $z^{1/2}$ está en $C(z_1, ..., z_n)$. El conjugado de z es simplemente su reflexión por el eje horizontal. Con esto vemos que $C(z_1, ..., z_n)$ es un subcampo de $\mathbb{C}$ cerrado bajo raíces cuadradas y conjugación.

Queremos demostrar que $C(z_1, ..., z_n)$ es el menor subcampo de $\mathbb{C}$ que contiene a los $z_1, ..., z_n$ y es cerrado bajo conjugación y raíces cuadradas. Sea entonces C' un subcampo de $\mathbb{C}$ que contiene a los z_i, $1 \leq i \leq n$, y cerrado bajo raíces cuadradas y conjugación. Para demostrar que $C(z_1, ..., z_n)$ está contenido en C', debemos demostrar que cada S_i está contenida en C' (pues $C(z_1, ..., z_n)$ es la unión de todas las S_i). Por la construcción de los S_i, basta con demostrar que los siguientes puntos están en C': (1) la intersección de dos rectas determinadas por puntos de C', (2) la intersección de una tal recta con un círculo cuyo centro está en C' y cuyo radio es la longitud de un

segmento entre dos puntos de C', y (3) la intersección de dos tales círculos.

Observemos primero que si un número complejo $x + iy$ está en C', tanto su parte real como imaginaria (es decir, x y y) están en C'. En efecto, como C' es cerrado bajo conjugación, tenemos que $x - iy$ está en C', por lo que $x + iy + x - iy = 2x$, está en C', y como C es campo, debe tener a los racionales, por lo que x está en C'. Por otro lado, como C' es cerrado bajo raíces cuadradas, tiene tanto a i como a $-i$ (pues ambas son raíces cuadradas del -1), por lo que $-i(x + iy) = y - ix$ está en C', y por lo observado anteriormente para las partes reales, y está en C'.

Tomemos ahora dos puntos cualesquiera en C', digamos $A+Bi$ y $C+Di$, y tomemos la recta que pasa por ellos. Si dicha recta es vertical, es de la forma $x = a$ con a en C'; si no es vertical, entonces su pendiente es $m = \frac{A-D}{B-C}$, que está en C'. La ecuación de la recta se puede ver en la forma $m = \frac{y-B}{x-A}$, o bien $y = mx - b$ donde $b = B - mA$ está en C'. Si se prefiere, se puede escribir la ecuación de esta recta en la forma $ax + by + c = 0$, con a, b, c (esta b diferente a la anterior) números reales en C'.

Tomemos ahora un punto $A + Bi$ en C' y la longitud r de un segmento que une dos puntos en C'. Tenemos que r está en C', pues se puede obtener con la fórmula de distancia como la raíz cuadrada de sumas de cuadrados de diferencias de partes reales e imaginarias de elementos de C'. La ecuación del círculo se ve $r^2 = (x - A)^2 + (y - B)^2$, que se puede llevar a la forma $0 = x^2 + y^2 + dx + ey + f$ con d, e, f números reales en C'.

Resolvamos primero (1). Dadas dos rectas (distintas) no paralelas $ax + by + c = 0$ y $a'x + b'y + c' = 0$, su intersección es un punto cuyas coordenadas (x, y) satisfacen el sistema de dos ecuaciones lineales dado anteriormente. Por la Regla de Cramer, estas soluciones únicas se pueden expresar como cocientes de determinantes que involucran a los coeficientes, y por lo tanto el punto de intersección de estas rectas está en C'.

Hagamos ahora el caso (2). Tomemos primero una recta no vertical con ecuación $y = mx + b$, donde m, b están en C'. Considere un círculo con ecuación $x^2 + y^2 + dx + ey + f = 0$ donde d, e, f son números reales que están en C'. Si la recta intersecta al círculo, sus puntos de intersección son las soluciones comunes de ambas ecuaciones. Un punto (x, y) que esté en la intersección debe cumplir entonces que $y = mx + b$, y sustituyendo esto en la ecuación del círculo tenemos que $x^2 + (mx + b)^2 + dx + e(mx + b) + f = 0$, que es una ecuación de segundo grado cuyos coeficientes están todos en C'. Usando la fórmula general para dichas ecuaciones, vemos que x está en C', y

como $y = mx + b$, también y está en C'. Si la recta fuera vertical, tendríamos que cumple la ecuación $x = a$ para alguna a en C', y sustituyendo en la ecuación del círculo, veríamos que la y debe estar en C'.

Finalmente, consideremos el caso (3). Tomemos dos círculos, con ecuaciones $x^2 + y^2 + dx + ey + f = 0$ y $x^2 + y^2 + d'x + e'y + f' = 0$, y supongamos que tienen intersección no vacía. Los puntos de intersección de estos círculos son los mismos que los puntos de intersección del primer círculo con la recta dada por la ecuación $(d' - d)x + (e' - e)y + f' - f = 0$, pues la ecuación de dicha recta se obtiene restando las ecuaciones de los círculos. Como esta recta tiene una ecuación con coeficientes en C', el caso (3) se reduce al caso (2).

Con esto hemos demostrado el siguiente hecho.

Teorema 16. *El conjunto $C(z_1, ...z_n)$ de puntos de $\mathbb{C}$ que son construíbles con recta y compás a partir de $z_1, ..., z_2$ son precisamente los elementos del menor subcampo de $\mathbb{C}$ que contiene a los $z_1, ..., z_n$ y es cerrado bajo conjugación y raíces cuadradas.*

Daremos ahora un criterio sencillo para determinar si un punto z es construíble con recta y compás a partir de $z_1, ..., z_n$.

Teorema 17. *Sean $z_1, \ldots, z_n \in \mathbb{C}$ y sea $k = \mathbb{Q}(z_1, \ldots, z_n, \bar{z}_1, \ldots, \bar{z}_n)$. Sea $z \in \mathbb{C}$. Entonces z es construíble con regla y compás a partir de $z_1, \ldots, z_n$ si y solamente si z está contenido en un subcampo de $\mathbb{C}$ de la forma $k(u_1, \ldots, u_r)$ donde $u_1^2 \in k$ y para toda $i = 2, \ldots, r$ se tiene que $u_i^2 \in k(u_1, \ldots, u_{i-1})$ (a este subcampo $k(u_1, \ldots, u_r)$ se le llama una **torre de raíces cuadradas** sobre k). En este caso, si $k = \mathbb{Q}$, decimos simplemente que z es construíble con regla y compás.*

Demostración: Sea C' el conjunto de todos los números complejos z tales que z está contenido en alguna torre de raíces cuadradas sobre k. Queremos demostrar que $C' = C(z_1, ..., z_n)$.

Puesto que $C(z_1, ..., z_n)$ es cerrado bajo conjugación y contiene a $z_1, ..., z_n$, también debe contener a $\bar{z}_1, ..., \bar{z}_n$, por lo que $C(z_1, ..., z_n)$ contiene a k. Dado un subcampo $k(u_1, \ldots, u_r)$ que sea torre de raíces cuadradas sobre k, notamos que u_1 es raíz cuadrada de un elemento de k, e inductivamente u_{i+1} es raíz cuadrada de un elemento de $k(u_1, \ldots, u_{i-1})$, por lo que todas estas $u_1, ..., u_r$ son elementos de $C(z_1, ..., z_n)$ (ya que este campo es cerrado bajo raíces cuadradas), es decir, $k(u_1, \ldots, u_r)$ (y por lo tanto C') está contenido en $C(z_1, ..., z_n)$.

Para la otra contención, demostraremos que C' es un subcampo de $\mathbb{C}$ que contiene a $z_1, ..., z_n$ y es cerrado bajo conjugación y raíces cuadradas. Sean z y z' elementos en C', contenidos en sendas torres de raíces cuadradas $k(u_1, \ldots, u_r)$ y $k(w_1, \ldots, w_s)$. Entonces $k(u_1, \ldots, u_r, w_1, \ldots, w_s)$ es una torre de raíces cuadradas sobre k que contiene a $z + z'$, zz', $-z$ y z^{-1} si $z \neq 0$, por lo que C' es un subcampo de $\mathbb{C}$. Por su construcción, C' es cerrado bajo raíces cuadradas, pues si w es un número complejo tal que w^2 está en C', entonces existe una torre de raíces cuadradas sobre k, $k(u_1, \ldots, u_r)$ a la que pertenece w^2, de donde $k(u_1, \ldots, u_r, w)$ es una torre de raíces cuadradas sobre k a la que pertenece w. Finalmente, verificaremos que C' es cerrado bajo conjugación. Sea z en C' elemento de una torre de raíces cuadradas sobre k, $k(u_1, \ldots, u_r)$. Note que $\bar{k} = k$, y $\bar{z} \in \overline{k(u_1, \ldots, u_r)} = k(\bar{u}_1, \ldots, \bar{u}_r)$, donde este último campo es una torre de raíces cuadradas sobre k, por lo que $\bar{z} \in C'$ y con esto terminamos la demostración.

Proposición 18. *Sea $F = \mathbb{Q}(z_1, \ldots, z_n, \bar{z}_1, \ldots, \bar{z}_n)$. Si z es construible con regla y compás a partir de $z_1, \ldots . z_n$, entonces z es algebraico sobre F y de grado 2^m para algún entero positivo m. Se sigue que todo número complejo construible con regla y compás es algebraico sobre $\mathbb{Q}$ de orden una potencia de 2.*

Demostración: Tenemos una torre de campos

$$F = F_1 < F_2 < \ldots < F_{r+1}.$$

donde z es elemento de F_{r+1}, por lo que $[F(z) : F]$ divide a $[F_{r+1} : F]$. Como cada grado $[F_{i+1} : F_i]$ es una potencia de dos, su producto (que es $[F_{r+1} : F]$) es una potencia de dos, y cualquier divisor suyo (en particular, $[F(z) : F]$) es una potencia de dos.

Ejercicio 23. (Duplicación del cubo.) Demuestre que no se puede construir el lado de un cubo de volumen 2. *Sugerencia:* Demuestre que el polinomio irreducible de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ es de grado 3

Ejercicio 24. Usando la identidad $\cos(3t) = 4\cos^3(t) - 3\cos(t)$, demuestre que $\cos(20°)$ es raíz del polinomio $4x^3 - 3x - 1/2$. Demuestre que dicho polinomio es irreducible en $\mathbb{Q}[x]$ demostrando primero que $x^3 - 3x - 1$ es irreducible sobre $\mathbb{Q}$.

Ejercicio 25. (Trisección del ángulo.)Demuestre que el ángulo de 60° no se puede trisectar.

Ejercicio 26. (Cuadratura del círculo.) Usando que π es trascendente sobre $\mathbb{Q}$, demuestre que no es posible construir un cuadrado cuya área sea igual al área de un círculo de radio 1 (es decir, área π).

Terminamos esta sección con una discusión de polígonos regulares construíbles. Necesitaremos algunos conceptos sencillos de teoría de números, y aplicar Teoría de Galois.

Ejercicio 27. Sea p un número primo de la forma $2^s + 1$. Demuestre que s es una potencia de 2 (se permite $2^0 = 1$). *Sugerencia:* Suponga que un número impar k divide a s, digamos $s = km$. Note que el polinomio $x^k + 1$ se factoriza sobre $\mathbb{Z}$. Haga $x = 2^m$ y obtenga un factor del primo p.

Definición 19. Los **números de Fermat** son los números enteros de la forma $F_n = 2^{2^n} + 1$, con n un entero no negativo. Los **primos de Fermat** son los números de Fermat que además son números primos.

Ejemplo 20. Los primeros cinco primos de Fermat son: 3, 5, 17, 257, 65537.

Observación 21. No se conocen (hasta el momento) más primos de Fermat, ni se sabe si hay un número infinito de ellos, o si hay una infinidad de números de Fermat que no sean primos. Hasta el año 2010, se sabe que F_n es compuesto (es decir, no primo) para $5 \leq n \leq 32$. El mayor número compuesto de Fermat conocido es $F_{2478782}$, con factor primo $(3 * 2^{2478785}) + 1$.

Teorema 22. *(Gauss) Sea p un primo impar. Entonces es posible construir un polígono regular de p lados si y solamente si p es un primo de Fermat.*

Demostración: Debemos decidir si el número $z = e^{2\pi i/p}$ es construíble con regla y compás. El polinomio irreducible de z sobre $\mathbb{Q}$ es el polinomio ciclotómico $\Phi_p(x)$ de grado $p - 1$ (pues p es primo).

Supongamos que z es contruíble. Entonces $p - 1$ debe ser una potencia de 2, digamos $p - 1 = 2^s$ para alguna s. Como se vió antes, s debe ser a su vez una potencia de 2, es decir, p es un primo de Fermat.

Supongamos ahora que $p = 2^{2^t} + 1$ es primo. Como z es una raíz primitiva p-ésima del uno, $\mathbb{Q}(z)$ es el campo de descomposición de $\Phi_p(x)$ sobre $\mathbb{Q}$. Por lo tanto el orden del grupo de Galois de $\mathbb{Q}(z)$ sobre $\mathbb{Q}$ es 2^{2^t}, es decir, el grupo de Galois de $\mathbb{Q}(z)$ sobre $\mathbb{Q}$ es un 2-grupo. Por lo tanto, dicho grupo de Galois tiene una serie normal donde cada factor tiene orden 2. Por el Teorema Fundamental de la Teoría de Galois, existe una torre de campos

$\mathbb{Q} < K_1 < ... < K_m = \mathbb{Q}(z)$ con $[K_{i+1} : K_i] = 2$ para toda i, es decir, z es construíble.

Nota: Gauss dió una construcción explícita de un polígono regular de 17 lados.

Ejercicio 28. Demuestre que es imposible construir un polígono regular de 7, 11 o 13 lados.

Ejercicio 29. Describa cómo construir un polígono regular de 34 lados.

Observación 23. Se sabe que un polígono regular de n lados es construíble con regla y compás si y solamente si n es un producto de una potencia de 2 y primos de Fermat distintos, véase ???CITEJacobson, Teorema 4.18, Basic Algebra I, Segunda Edición.

0.9. EJERCICIOS DEL CAPITULO

Ejercicio 30. Calcule el grado del campo de descomposición del polinomio $x^5 - 8$ sobre los racionales. Justifique su respuesta. *Sugerencia:* Considere a las raíces quintas de la unidad.

Ejercicio 31. Describa el campo de descomposición de $x^{11} - 12$ sobre Q, es decir, diga cómo se obtiene a partir de Q, y calcule su grado.

Ejercicio 32. Sea $f(x)$ el polinomio $x^3 - 15$ en $Q[x]$. Describa el campo de descomposición de $f(x)$ sobre Q. Encuentre el grupo de Galois del polinomio $f(x)$ sobre Q. Describa la retícula de subcampos del campo de descomposición de $f(x)$.

Ejercicio 33. Sean p un primo, K un campo de característica p, $f(x) = x^p - a$ con a en K. Demuestre que si $f(x)$ no es irreducible sobre K, entonces $f(x)$ tiene todas sus raíces en K.

Ejercicio 34. Sean p un primo, K un campo que contiene todas las raíces p-ésimas de la unidad, $f(x) = x^p - a$ con a en K. Demuestre que si $f(x)$ no es irreducible sobre K, entonces $f(x)$ tiene todas sus raíces en K. Note que la característica del campo es arbitraria.

Ejercicio 35. Sea L una extensión finita, normal y separable del campo K, y sea G su grupo de Galois. Sea $E = \{a \in L | \tau\sigma(a) = \sigma\tau(a), \text{ para cada } \sigma, \tau \in G\}$. Demuestre que E es un subcampo de L, que E es una extensión normal y separable de K, y que el grupo de Galois de E sobre K es abeliano. *Sugerencia:* Puede utilizar el subgrupo derivado y sus propiedades.

Ejercicio 36. Sea L una extensión finita del campo K, y sea $f(x) \in K[x]$ irreducible de grado primo p, y tal que p no divide a $[L : K]$. Demuestre que $f(x)$ es irreducible en $L[x]$. *Sugerencia:* Examine $K(a)$ y $L(a)$, donde a es una raíz de $f(x)$.

Ejercicio 37. Sea F un campo finito. Demuestre que F posee un automorfismo de orden dos si y solamente si el orden de F es un cuadrado. Nota: con la teoría desarrollada, hay dos formas distintas de resolver este problema.

Ejercicio 38. Sea K un campo y $K[x]$ el anillo de polinomios en la variable x con coeficientes en K. Sea A el subanillo de $K[x]$ dado por $A = \{f(x) \in K[x] | f'(0) = 0\}$. Demuestre que A no es un dominio euclidiano. *Sugerencia:* Demuestre que x^2 y x^3 son irreducibles en A.

Ejercicio 39. Calcule el número de polinomios mónicos irreducibles sobre F_7 de grado 6. *Sugerencia:* Los elementos de $\mathbb{F}_7$ se pueden separar por el grado de su polinomio irreducible. ¿Cuántos elementos hay con polinomio irreducible de grado seis?

Ejercicio 40. Sean E una extensión del campo K, $f(x) \in K[x]$ un polinomio no constante con todas sus raíces en E. Suponga que el grupo de Galois de E sobre K actúa transitivamente en el conjunto de raíces de $f(x)$. Demuestre que $f(x)$ es potencia de un irreducible de $K[x]$.

Ejercicio 41. Sea F una extensión normal, separable y de grado finito de K. Sea a un elemento arbitrario de F . Sea R el conjunto $\{\sigma(a) | \sigma \in Gal(F, K)\}$. Demuestre que el polinomio irreducible de a sobre K es precisamente

$$\prod_{b \in R} (x - b)$$

Sugerencia: Estudie la demostración del Teorema 8

Ejercicio 42. Sean K un campo, $f(x) \in K[x]$ un polinomio irreducible separable, F el campo de descomposición de f sobre K. Demuestre que para

cualesquera dos raíces a y b de f en F, existe un automorfismo $\sigma \in Gal(F, K)$ tal que $\sigma(a) = b$. Muestre con un ejemplo que no cualquier permutación de las raíces de f se obtiene por algún σ en $Gal(F, K)$. *Sugerencia:* Para el ejemplo, revise el material de campos finitos.

Ejercicio 43. Sea F una extensión normal, separable y de grado finito de K. Sea $a \in F$. Demuestre que $F = K(a)$ si y solamente si $\sigma(a) \neq \tau(a)$ para cualesquiera $\sigma, \tau \in Gal(F, K)$ distintos. *Sugerencia:* El grado de F sobre K es igual al orden del grupo de Galois de F sobre K, y el grado de $K(a)$ sobre K es igual al grado del polinomio irreducible de a sobre K. Véase el Ejercicio 41.

Ejercicio 44. Calcule el grado del campo de descomposición del polinomio $x^{12} - 1$ sobre los racionales. *Sugerencia:* Factorice tanto como sea posible.

Ejercicio 45. Sea F una extensión finita normal y separable del campo k. Demuestre que la correspondencia de Galois manda a la intersección de dos subgrupos en el campo generado por sus correspondientes campos fijos, y manda al subgrupo generado por dos subgrupos en la intersección de sus campos fijos. *Sugerencia:* Aplique el Teorema Fundamental de la Teoría de Galois.

Ejercicio 46. Sea $F = k(a)$ donde a es algebraico sobre k, y el grado del polinomio irreducible de a sobre k es impar. Demuestre que $F = k(a^2)$.

Ejercicio 47. Sea E una extensión algebraica de F, y sea R un subanillo de E que contiene a F. Demuestre que R es un subcampo de E. Muestre con un ejemplo que esto es falso si no se pide que R contenga a F.

Ejercicio 48. Sea $E = F(u)$, con u trascendente sobre F, y sea K un subcampo de E que contiene propiamente a F. Demuestre que u es algebraico sobre K.

Ejercicio 49. Sea E una extensión finita de F. Suponga que para cualesquiera K, L subcampos de E que contienen a F, se tiene que $K \leq L$ o $L \leq K$. Demuestre que E tiene un elemento primitivo sobre F, es decir, existe a en E tal que $E = F(a)$.

Ejercicio 50. Sea $E = F(u)$ una extensión finita. Sea K un campo intermedio entre F y E, y $g(x)$ el polinomio irreducible de u sobre K. Demuestre

que el subcampo de E que contiene a F y a los coeficientes de $g(x)$ es precisamente K. *Sugerencia:* Sea K' tal subcampo. Observe primero que K' es subcampo de K, y que $E = K(u) = K'(u)$. ¿Cuál es el polinomio irreducible de u sobre K'? Use este polinomio para concluir que $[E : K] = [E : K']$.

Ejercicio 51. Sea $E = F(u, v)$ una extensión finita, con F un campo infinito. Suponga que existe solamente un número finito de campos intermedios entre F y E. Demuestre que E tiene un elemento primitivo (es decir, existe z en E tal que $E = F(z)$). *Sugerencia:* Considere los subcampos $F(u + av)$ con a en F. Demuestre que existen $a \neq b$ en F tales que $F(u + av) = F(u + bv)$. Muestre que combinaciones apropiadas de $u + av$ y $u + bv$ generan primero a v y luego a u.

Ejercicio 52. (Teorema de Steinitz) Sea E una extensión finita de F. Entonces E tiene un elemento primitivo si y solamente si existen solamente un número finito de campos intermedios entre F y E. *Sugerencia:* Suponga que $E = F(u)$, y sea $f(x)$ el polinomio irreducible de u sobre F. Demuestre que los campos intermedios entre E y F son precisamente los subcampos sobre F generados por los coeficientes de los factores mónicos de $f(x)$ en $E(x)$.

Ejercicio 53. Use el Teorema de Steinitz para dar otra demostración del Teorema del Elemento Primitivo, es decir, que toda extensión finita separable contiene un elemento primitivo.