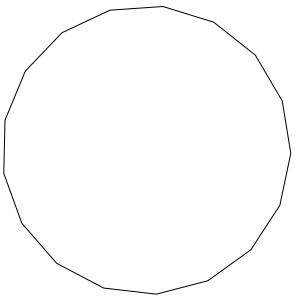
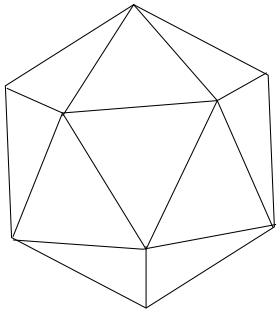
¡Qué bonita es la teoría de Galois!

Álgebra II. Tercero de Matemáticas.



Gauss



Abel

Galois

Lorente Fernando
Cozimah

2004/2005

Álgebra II reloaded

Esto será en el futuro un prefacio. Por ahora, hasta que no finalice el curso, no puedo decir más que generalidades. Entre ellas, la más relevante es que estas notas están basadas en otras que escribí de la asignatura homónima los cursos 1995/96 y 1996/97, disponibles en la página `http://www.uam.es/fernando.chamizo` (en mi "segunda vivienda").

Evidentemente, el cambio de título indica que ha habido modificaciones sustanciales desde entonces. La más notable se debe a que la parte de teoría de anillos que ha perdido Álgebra I, ahora pertenece a la asignatura que nos ocupará, por ello hay un primer capítulo totalmente nuevo. También se han añadido gran cantidad de ejercicios, algunos ejemplos, observaciones, apéndices y tonterías. En fin, nada que me haya servido para nada más que fabricarme un trocito de pasado.

Acabo estas breves líneas agradeciendo a Carlos Vinuesa (estudiante y cinéfilo) la revisión profunda que hizo de muchas secciones de la antigua versión de las notas. En reconocimiento he puesto a este prefacio provisional el título de uno de sus mensajes. Dicho sea de paso, el capítulo de agradecimientos está abierto, y ruego a los que tengan ánimo y ganas de investigar erratas, fallitos y errores vergonzantes, que me los comuniquen para incorporar los cambios pertinentes a estos apuntes.

Madrid, febrero de 2004

Prefacio

Estos apuntes reflejan los contenidos de un curso típico de teoría de Galois con un capítulo inicial de teoría de anillos. Hay muchos y buenos libros sobre el tema, especialmente el de I. Stewart *Galois Theory*. La única débil publicidad que puedo hacer a mis apuntes es su precio (igual en pesetas que en euros) y que se ajustan bien al temario real de la asignatura. Respecto a su estructura, hay cuatro capítulos, cada uno complementado con una colección de ejercicios y con un apéndice de curiosidades, consejos y tonterías. Los pocos ejercicios señalados por la leyenda correspondiente como "muy difíciles", realmente lo son, posiblemente incluso para los alumnos más aventajados. Los identificados como "opcionales" no son necesariamente complicados pero no están relacionados con el centro del curso. A veces lo están con material complementario escrito en letra pequeña.

Avanzo que no habrá grandes cambios con respecto a la versión de estos apuntes escrita el curso pasado. Si alguien dispone de una copia de ellos, puede aprovecharla por el bien de nuestros bosques. En ese caso, consúltese en la página de la asignatura `http://www.uam.es/fernando.chamizo` la lista de erratas detectadas. Allí también se pueden obtener los presentes apuntes corregidos, capítulo a capítulo.

Tras la experiencia del curso pasado, lo más posible es que la materia tal como se presenta en clase, sufra algunas reducciones con respecto a lo aquí escrito. La última sección se puede suprimir totalmente, y las otras dos secciones del cuarto capítulo presentarse con reducciones en los detalles técnicos. Especialmente la primera, ya que la teoría de grupos es un medio pero no un fin por sí mismo en este curso.

Madrid, febrero de 2005

Contenidos

Capítulo 1. Teoría de anillos

- 1.1. Definición de anillo.
- 1.2. Ideales y cocientes.
- 1.3. Factorización.

Capítulo 2. Cuerpos y sus extensiones

- 2.1. Definición de cuerpo.
- 2.2. Extensiones de cuerpos.
- 2.3. Tres problemas clásicos.

Capítulo 3. Teoría de Galois

- 3.1 Extensiones normales y separables.
- 3.2 El grupo de Galois.
- 3.3 El teorema fundamental de la teoría de Galois.

Capítulo 4. Resolubilidad por radicales

- 4.1 Grupos solubles.
- 4.2 El teorema de Galois.
- 4.3 Algunas aplicaciones.

La teoría de Galois en menos de cincuenta minutos

La idea genial bajo la teoría de Galois es que se pueden representar ciertos conjuntos asociados a la solución de ecuaciones algebraicas mediante grupos de simetrías. Esta frase es tan lapidaria como incomprensible. Afortunadamente todavía podemos utilizar los 49 minutos 50 segundos restantes para tratar de clarificarla un poco.

Comencemos resolviendo la ecuación general de segundo grado $x^2 + bx + c = 0$. Considerando sus raíces r_1 y r_2 como variables arbitrarias, los coeficientes b y c vienen dados por funciones polinómicas simétricas de ellas:

$$x^2 + bx + c = (x - r_1)(x - r_2) \;\Rightarrow\; b = b(r_1, r_2) = -r_1 - r_2, \quad c = c(r_1, r_2) = r_1 r_2.$$

La fórmula para resolver la ecuación (hallar r_1 y r_2 a partir de b y c) es $(-b+\sqrt{b^2-4c})/2$ donde el radical no es una verdadera función univaluada, sino que hay que asignarle dos valores, uno con más y otro con menos. Este radical obra el milagro de pasar de una función simétrica en r_1 y r_2, concretamente $b^2 - 4c = (r_1 + r_2)^2 - 4r_1 r_2$, a dos funciones no simétricas, $\sqrt{b^2 - 4c} = \pm(r_1 - r_2)$.

En la ecuación de tercer grado $x^3 + bx^2 + cx + d = 0$, de nuevo b, c y d se pueden considerar como funciones simétricas en las variables r_1, r_2 y r_3 que representan las raíces:

$$b = -r_1 - r_2 - r_3, \qquad c = r_1 r_2 + r_1 r_3 + r_2 r_3 \quad \text{y} \quad d = -r_1 r_2 r_3.$$

La fórmula para resolver la ecuación es en este caso bastante más complicada y se puede escribir como:

$$-\frac{b}{3} + \frac{t}{3} + \frac{b^2 - 3c}{3t} \qquad \text{con} \quad t = \sqrt[3]{E}$$

donde

$$E = \frac{9bc - 2b^3 - 27d + \sqrt{D}}{2} \qquad \text{y} \qquad D = (9bc - 2b^3 - 27d)^2 + 4(3c - b^2)^3.$$

En resumidas cuentas, la resolución de la ecuación pasa por hallar primero una raíz cuadrada de D y después otra cúbica (trivaluada) de E. Si tuviéramos tiempo y paciencia para sustituir b, c y d en términos de las raíces veríamos que

$$D = -27(r_1 - r_2)^2 (r_1 - r_3)^2 (r_2 - r_3)^2 \qquad \text{y} \qquad E = (r_1 + \zeta r_2 + \zeta^2 r_3)^3,$$

donde ζ es una raíz cúbica no trivial de la unidad, esto es, $\zeta = (-1 \pm i\sqrt{3})/2$.

De nuevo observamos la pérdida de simetrías por medio de los radicales: D es una función simétrica en r_1, r_2 y r_3, mientras que $\sqrt{D}$ no lo es, aunque perduran algunas simetrías, por ejemplo, $\sqrt{D}$ es invariante al cambiar $(r_1, r_2, r_3) \mapsto (r_2, r_3, r_1)$. También E goza de estas simetrías de $\sqrt{D}$ pero al extraer la raíz cúbica se pierden todas ellas.

Para resolver la ecuación de cuarto grado la fórmula es muchísimo más compleja. En una de las maneras de escribirla, primero hay que hacer una raíz cuadrada $\sqrt{F}$, después una raíz cúbica $\sqrt[3]{G}$, y luego dos raíces cuadradas más $\sqrt{H}$ y $\sqrt{I}$. Al expresar todo en

términos de las variables r_1, r_2, r_3 y r_4 que representan las raíces, el fenómeno de pérdida de simetrías se repite, desde F que las tiene todas, hasta $\sqrt{I}$ que no tiene ninguna.

Volvamos al caso de segundo grado. Consideremos el conjunto K_0 de todas las expresiones (fórmulas) que se pueden obtener a partir de b y c haciendo sumas, restas, multiplicaciones y divisiones, por ejemplo $b/(c^2-b)+b^2 \in K_0$, y $K_0\big(\sqrt{b^2-4c}\big)$ definido de igual manera pero permitiendo también operar con $\sqrt{b^2-4c}$. Se tiene $b, c \in K_0$ y $r_1, r_2 \in K_1 = K_0\big(\sqrt{b^2-4c}\big)$, de forma que el paso de K_0 a K_1 representa resolver la ecuación. Como las funciones de K_0 son invariantes al permutar sus dos variables (r_1 y r_2), diremos que su grupo de simetrías es S_2, mientras que las funciones de K_1 no son en general simétricas de ningún modo y por tanto le asignaremos el grupo trivial de simetrías $\{\mathrm{Id}\}$. En un esquema:

$$\begin{array}{lcl} K_0 & \text{———————} & K_1 = K_0\big(\sqrt{b^2-4c}\big) \\ G_0 = S_2 & \text{———————} & G_1 = \{\mathrm{Id}\} \end{array}$$

Con la misma notación, en el caso de tercer grado el esquema sería:

$$\begin{array}{lcccl} K_0 & \text{———} & K_1 = K_0\big(\sqrt{D}\big) & \text{———} & K_2 = K_1\big(\sqrt[3]{E}\big) \\ G_0 = S_2 & \text{———} & G_1 = A_3 & \text{———} & G_2 = \{\mathrm{Id}\} \end{array}$$

donde A_3 son las permutaciones pares, las generadas por $(r_1, r_2, r_3) \mapsto (r_2, r_3, r_1)$.

Sin entrar en detalles, en el caso de grado cuatro se tiene:

$$\begin{array}{lcccccccl} K_0 & \text{———} & K_1 & \text{———} & K_2 & \text{———} & K_3 & \text{———} & K_4 \\ G_0 = S_4 & \text{———} & G_1 = A_4 & \text{———} & G_2 & \text{———} & G_3 & \text{———} & G_4 = \{\mathrm{Id}\} \end{array}$$

con $K_1 = K_0\big(\sqrt{F}\big)$, $K_2 = K_1\big(\sqrt[3]{G}\big)$, $K_3 = K_2\big(\sqrt{H}\big)$ y $K_4 = K_3\big(\sqrt{I}\big)$, y G_2 y G_3 ciertos subgrupos de S_4 de órdenes 4 y 2 respectivamente.

De esta forma reflejamos el método para resolver las ecuaciones de grado $n = 2, 3, 4$ en una "tira" de subgrupos que empieza en S_n y acaba en $\{\mathrm{Id}\}$. Además, y aquí está la clave del teorema de Galois, siempre que empleemos radicales para romper simetrías cada subgrupo debe ser normal en el anterior, $G_i \triangleright G_{i+1}$. Para probar esto debemos tener a mano nuestros apuntes de Álgebra I y, si $K_{i+1} = K_i(R)$ con $R^p \in K_i$ (digamos con p primo y $R \notin K_i$), considerar el homomorfismo:

$$\begin{array}{rcl} \phi : G_i & \longrightarrow & \big(\mathbb{C} - \{0\}, \cdot\big) \\ \sigma & \longmapsto & \dfrac{R(r_{\sigma(1)}, r_{\sigma(2)}, \ldots, r_{\sigma(n)})}{R(r_1, r_2, \ldots, r_n)} \end{array}$$

Ahora leamos muy despacito, siempre con el Álgebra I presente: La imagen de este homomorfismo son las raíces p-ésimas de la unidad porque R^p es invariante por G_i y por consiguiente $R^p(r_{\sigma(1)}, r_{\sigma(2)}, \ldots, r_{\sigma(n)}) = R^p(r_1, r_2, \ldots, r_n)$; de donde $\mathrm{Im}\ \phi \cong \mathbb{Z}_p$. Además $\mathrm{Ker}\ \phi = G_{i+1}$ y el primer teorema de isomorfía implica $\mathrm{Ker}\ \phi = G_{i+1} \triangleleft G_i$ y $G_i/G_{i+1} \cong \mathrm{Im}\ \phi \cong \mathbb{Z}_p$.

En definitiva, la única forma de romper simetrías usando radicales es con subgrupos normales cuyo cociente sea isomorfo a un $\mathbb{Z}_p$.

Ahora podemos recoger los frutos de esta representación por medio de simetrías: Un teorema de teoría de grupos asegura que no existe ninguna cadena de grupos desde S_5 a $\{\mathrm{Id}\}$ siendo cada uno subgrupo normal del anterior y con cociente cíclico, por tanto *no existe una fórmula para resolver la ecuación de quinto grado usando sólo sumas, restas, multiplicaciones, divisiones y radicales* (Teorema de Abel). Lo mismo se aplica a la ecuación general de grado $n > 5$.

Evidentemente, hay casos particulares, como por ejemplo $x^6 - 7 = 0$, que sí pueden resolverse con radicales. El *Teorema de Galois* afirma que una ecuación se puede resolver con radicales si y sólo si existe una tira de subgrupos desde el llamado *grupo de Galois* a $\{\mathrm{Id}\}$ con las propiedades antes indicadas. El grupo de Galois es esencialmente el formado por las permutaciones de las raíces que son compatibles con las operaciones elementales (suma, resta, multiplicación y división) y que por tanto respeten las igualdades creadas con ellas. Por ejemplo, $x^4 - 2 = 0$ tiene como raíces $r_1 = \sqrt[4]{2}$, $r_2 = -\sqrt[4]{2}$, $r_3 = i\sqrt[4]{2}$, $r_4 = -i\sqrt[4]{2}$, y la permutación que intercambia r_2 y r_3 (dejando fijas las otras raíces) debe ser excluida del grupo de Galois porque, por ejemplo, $r_1^2 - r_2^2 = r_4^2 - r_3^2$ pero $r_1^2 - r_3^2 \neq r_4^2 - r_2^2$. A lo largo del curso veremos cómo hallar el grupo de Galois en casos suficientemente sencillos sin tener que pensar en todas las posibles igualdades. Si las raíces se consideran variables arbitrarias, como hemos hecho antes, no hay relaciones entre ellas, y el grupo de Galois es S_n.

El interés de este grupo no se limita a su relación con la resolubilidad por radicales, aunque sea su origen histórico. El *teorema fundamental de la Teoría de Galois* implica que para cualquier ecuación algebraica particular, la estructura interna de K_0 está fielmente reflejada en la estructura del grupo de Galois, lo cual es realmente destacable porque permite pasar de estudiar un conjunto infinito y de alguna forma continuo, a otro finito discreto.

Bibliografía

[Ak] A.G. Akritas. *Elements of computer algebra, with applications*. Wiley, 1989.

[Ca] R. Calinger (Ed.). *Classics of Mathematics*. Prentice-Hall, 1995.

[Cam] O.A. Cámpoli. A Principal Ideal Domain That Is Not a Euclidean Domain. Amer. Math. Monthly 95 (1988), 868–871.

[Cl] A. Clark. *Elementos de álgebra abstracta*. Alhambra, 1987.

[De-Fu-Xa] F. Delgado, C. Fuertes, S. Xambó. *Introducción al álgebra (Anillos, factorización y teoría de cuerpos)*. Universidad de Valladolid, 1998.

[Do-He] J.R. Dorronsoro, E. Hernández. *Números, grupos y anillos*. Addison-Wesley Iberoamericana–UAM, 1996.

[Ed] H.M. Edwards. *Galois Theory*. Springer, 1998.

[Es] *J.-P. Escofier. *Galois Theory*. Graduate Texts in Mathematics 204, Springer-Verlag, 2001.

[Ga] J.A. Gallian. *Contemporary Abstract Algebra*. Houghton Mifflin Company, 2002.

[Gal] E. Galois. *Oeuvres Mathèmatiques publièes en 1846 dans le Journal de Liouville*. Jacques Gabay, 1989.

[Gar] D.J.H Garling. *A course in Galois Theory*. Cambridge University Press, 1986.

[Gau] C.F. Gauss. *Disquisitiones Arithmeticae*. Springer-Verlag, 1986.

[Ha] C.R. Hadlock. *Field Theory and its Classical Problems*. The Mathematical Association of America, 1978.

[Ja] N. Jacobson. *Lectures in Abstract Algebra*. Vol.3. Theory of fields and Galois theory. Van Nostrand, 1964.

[Ka] I. Kaplansky. *Fields and Rings*. University of Chicago Press, 1974.

[Kl] M. Kline. *Mathematical thought from ancient to modern times*. Oxford University Press, 1972.

[Mo] *P. Morandi. *Field and Galois Theory*. Graduate Texts in Mathematics 167. Springer-Verlag, 1995.

[Ri] P. Ribenboim. *13 Lectures on Fermat's Last Theorem*. Springer-Verlag, 1979.

[Ro] *S. Roman. *Field Theory*. Graduate Texts in Mathematics 158. Springer-Verlag, 1998.

[Rot] T. Rothman. *Genius and biographers: the fictionalization of Evariste Galois*. Amer. Math. Monthly 89 (1982), 84–106.

[Rotm] J.J. Rotman. *Galois Theory*. Springer-Verlag, 1990.

[Sm] D.E. Smith. *A Source Book in Mathematics*. Dover Publications Inc., 1959.

[St] I. Stewart. *Galois Theory*. Chapman and Hall, 1973.

[Ve] F. Vera. *Científicos griegos* Vol I,II. Aguilar, 1970.

(Un asterisco indica una referencia de mayor nivel de dificultad).