En los artículos 337–341 de [Gau86], Gauss se ocupa del polinomio ciclotómico

$$x^{n-1} + x^{n-2} + \cdots + x + 1 \qquad \text{con } n > 2 \text{ primo.} \tag{1}$$

Hoy en día lo habitual sería escribir p en lugar de n pero creo que es mejor transigir con el n de Gauss porque si no, acabaríamos haciéndonos un lío.

El objetivo (que se alcanza en el art. 341) es probar que este polinomio es irreducible en $\mathbb{Q}[x]$. Hoy en día esto se hace en un par de líneas apelando al criterio de Eisenstein tras un cambio de variable simple pero muy ingenioso.

1) Busca en cualquier libro del tema (por ejemplo [Ste89]) o en la red cómo es esta prueba "moderna" de la irreducibilidad de (1).

Cuando Gauss escribió [Gau86], Eisenstein ni siquiera había nacido y su prueba de la irreducibilidad es más complicada que la actual pero bastante bonita. En cierto modo involucra algunas ideas de teoría de Galois. Lo único criticable es que Gauss alarga su demostración distinguiendo varios casos cuando en realidad sólo se puede dar uno de ellos.

En el art. 337 se dan (sin demostración) polinomios que tienen como raíces $\sin(2\pi/n)$, $\cos(2\pi/n)$ y $\tan(2\pi/n)$. He de confesar que, excepto el de la tangente que es fácil, los otros me ha llevado un rato probarlos. Esto no se necesita para nada de lo que viene después, por tanto lo único que te pido es:

2) Da un vistazo por encima al art. 337.

Hay dos resultados auxiliares que utiliza Gauss. El primero de ellos está en el art. 42, no lo tienes en tus fotocopias, y es conocido hoy en día como el lema de Gauss (para polinomios). Lo que dice es que si un polinomio no constante de coeficientes enteros es irreducible en $\mathbb{Z}[x]$ entonces también lo es en $\mathbb{Q}[x]$. Es decir, que al factorizar polinomios con coeficientes enteros no pueden aparecer denominadores de la nada. Este resultado es elemental pero no obvio.

3) Busca la demostración del lema de Gauss (viene por ejemplo en [Ste89]) y sigue los pasos.

El otro resultado, está en el art. 338 pero sólo esbozado. Casi lo da por sabido. Lo que dice es que si un polinomio tiene coeficientes racionales o enteros, entonces al elevar sus raíces a una potencia entera positiva, esa propiedad no cambia. En fórmulas, para $A = \mathbb{Q}$ ó $A = \mathbb{Z}$, dado $k \in \mathbb{Z}^+$ se tiene

$$(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \in A[x] \quad \Rightarrow \quad (x-\alpha_1^k)(x-\alpha_2^k)\cdots(x-\alpha_n^k) \in A[x].$$

Aunque admite una prueba elemental (no muy breve) hoy en día no es tan fácil encontrar esto en los libros sin usar teoría de Galois. Para no cargarte de trabajo, simplemente da por

sabido este resultado. Si tienes curiosidad, lo tengo escrito en las p.3–4 de [Cha12], es lo que está en letra pequeña. El teorema que allí discuto de los polinomios simétricos elementales era fundamental en temas de álgebra de los siglos XVIII y XIX, y tiene su origen en unas identidades de Newton a las que se refiere Gauss, pero hoy en día ha perdido su importancia. Ni siquiera las identidades de Newton [Cla84, 131β] [Wik16] se suelen ver en los cursos de álgebra.

El art. 339 dice cosas muy elementales. Nota aquí y en lo sucesivo que Gauss llama "complex" o "complex of roots" simplemente al conjunto de raíces.

4) Lee el art. 339. Posiblemente no aprendas nada nuevo pero te ayudará a ir familiarizándote con la terminología.

La prueba en sí comienza en el art. 340. Podríamos decir que es un lema de más entidad que los resultados auxiliares anteriores y, aunque no lo parezca, encierra algunos indicios de la teoría de Galois y la idea de simetría. En el lenguaje moderno uno podría decir que está usando los automorfismos de $\mathrm{Gal}\big(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}\big)$ pero no te asustes, no es algo difícil. Al leerlo seguramente te resultará tediosa la notación en parte debido a que en aquellos tiempos no había los medios de impresión actuales ni por supuesto LaTeX. Como ayuda al siguiente ejercicio te sugiero lo siguiente: la función ϕ hoy diríamos que es $\phi \in \mathbb{Q}[x_1, x_2, \ldots, x_k]$ y por tanto escribiríamos $x_1, x_2, x_3, \ldots$ en vez de $t, u, v, \ldots$, de la misma forma nadie escribiría hoy a, b y c sino 1, r y r^2 con $r = e^{2\pi i/n}$.

Hay una cosa en la que tengo una duda. Cuando Gauss dice "rational integral algebraic function", no sé si admite también que sea cociente de polinomios, es decir, $\phi \in \mathbb{Q}(x_1, x_2, \ldots, x_k)$. En ese caso el resultado también es cierto (pero más complicado) siempre que el denominador no se anule. Parece que sólo va a considerar polinomios, entonces supón que éste es el caso.

5) Lee el art. 340 y escríbelo con tus palabras y notación más moderna, completando los detalles que te parezcan oscuros y prescindiendo de lo que consideres evidente.

El enunciado de la irreducibilidad de (1) y el grueso de la prueba están en el art. 341.

Antes de que mires nada, vamos con la cosa con la que parece que Gauss se despista. Si factorizamos el polinomio de (1) como PQ en $\mathbb{Q}[x]$ (que es lo mismo que hacerlo en $\mathbb{Z}[x]$ por el lema de Gauss), cada raíz de P será de la forma $\xi = e^{2\pi k i/n}$ y $P(\xi) = 0$ implica conjugando $P(\bar{\xi}) = 0$ o equivalentemente, $P(1/\xi) = 0$. Siempre se puede suponer entonces que estamos en el caso que Gauss llama I en el art. 341, en el que los inversos de las raíces de P son también raíces de P. Con ello la distinción de $\mathfrak{P}$, $\mathfrak{Q}$, $\mathfrak{R}$, $\mathfrak{S}$ que hace al principio te la puedes saltar y empezar en I notando que $\mathfrak{P}$ significa el conjunto de raíces de P.

La notación es, de nuevo, un poco insufrible desde el punto de vista actual. Sugiero que

al escribirlo utilices[1] $P_0, P_1, P_2, \dots P_{n-2}$ o las letras que prefieras en vez de $P, P', P'', \dots P^{\nu}$. Fíjate que como dice Gauss, hay $n-1$ funciones que vienen de hasta la potencia $n-1$, por eso $\nu = n-2$ (no sé por qué lo abrevia). Lo mismo se aplica a las p minúsculas.

Dentro de la parte matemática, recuerda que cuando menciona el art. 42, se refiere al lema de Gauss. El punto más importante de la prueba y el que quizá te cueste un poquillo es la igualdad entre el producto de las P y X^{λ}. Piensa en las multiplicidades de las raíces en ese producto. Si después de pensarlo mucho no se te ocurre, pregúntame y te doy una pista pero de verdad que es asequible.

6) Lee el punto I del art. 341 y escríbelo con tus propias palabras y notación. Da algún detalle acerca de la igualdad entre el producto de las P y X^{λ}.

Lo que me tienes que entregar está dentro del ejercicio siguiente:

7) Escribe lo que has aprendido acerca de la irreducibilidad de (1) según [Gau86] para que sirva como versión preliminar del punto 3 de la propuesta de temario. Intenta ajustarte a tres páginas o así. A no ser que tengas una idea muy clara en otro sentido, te recomiendo que sigas las directrices que te indico:

1. Comienza con unas líneas de introducción explicando que en los artículos 337–341 se aborda la irreducibilidad de (1) pero que hoy en día este resultado es muy fácil y escribe la demostración breve actual.

2. Menciona los dos resultados auxiliares (lema de Gauss y potencias de raíces) poniendo la referencia de los artículos donde están. Dependiendo del espacio que tengas disponible, lo mismo puedes poner algo breve acerca de su prueba o de su importancia. Sería conveniente que dieses también referencias modernas de ellos por si un lector de tu trabajo quiere consultarlas.

3. Redacta lo que has pensado para el problema **5)**.

4. Redacta lo que has pensado para el problema **6)**.

Un comentario final: si hay cosas que te resultan chocantes, no dejes de señalarlas o explicarlas en tu redacción. El objetivo a tener en mente es que leyendo tu trabajo alguien del siglo XXI pueda ahorrase el esfuerzo de meterse en la notación y costumbres matemáticas de los primeros años del siglo XIX pero con la sensación en todo momento de que sigue el esquema original.

[1] Si te digo la verdad, yo prefiero $P_1, P_2, P_3, \dots P_{n-1}$ para que el subíndice sea la potencia pero no sé si te va a hacer un lío.

Referencias

[Cha12] F. Chamizo. ¡Qué bonita es la teoría de Galois! `http://www.uam.es/fernando.chamizo/libreria/libreria.html`, 2012.

[Cla84] A. Clark. *Elements of Abstract Algebra*. Dover Books on Mathematics Series. Dover Publications, 1984.

[Gau86] C. F. Gauss. *Disquisitiones arithmeticae*. Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[Ste89] I. Stewart. *Galois theory*. Chapman and Hall, Ltd., London, second edition, 1989.

[Wik16] Wikipedia. Newton's identities — wikipedia, the free encyclopedia, 2016. [Online; accessed 9-August-2016].