Los artículos 342–358 de [Gau86] son los que tienen los argumentos más profundos y fundamentales. Para que sean más llevaderos, los dividiré entre dos hojas. Lo que hace en ellos es introducir los *periodos* y estudiar sus propiedades. Ya aparecieron en la hoja 1 pero sólo en el caso en que $n-1$ era potencia de dos. Para tu curiosidad, en el lenguaje moderno estos periodos sirven para construir automáticamente los cuerpos intermedios de la extensión $\mathbb{Q}\big(e^{2\pi i/n}\big)/\mathbb{Q}$. Más adelante te comentaré alguna cosa acerca de esto pero, tranquilo, no será parte del trabajo a no ser que tengas mucho interés (y tiempo de sobra) al final y quieras volver sobre ello.

En los artículos 342–343, Gauss explica con palabras el objetivo y empieza a introducir la notación (confirmando mis sospechas de que en gran medida deriva de la tipografía de la época). Gauss escribe $[k]$ en lugar de ζ^k con $\zeta = e^{2\pi i/n}$. Hoy en día ζ^k es fácil de escribir, entonces te recomiendo que lo emplees en lugar de seguir a Gauss. Recuerda que n era un número primo. Por otra parte, e será un divisor de $n-1$, que al igual que n puedes suponer fijado a lo largo de esta hoja, y $f = (n-1)/e$, es decir $n-1 = ef$. Se considera g un generador de $\mathcal{U}(\mathbb{Z}_n)$, el grupo (multiplicativo) de unidades de $\mathbb{Z}_n$. Es decir, como ya vimos, g es un entero que, módulo n, al elevar a $0, 1, \ldots, n-2$ da las clases $1, 2, \ldots, n-1$ (en otro orden). Con todo ello, se define el periodo (f, λ) como

$$(f,\lambda) = \sum_{k=0}^{f-1} \zeta^{\lambda g^{ek}} \qquad \text{para} \quad \lambda \in \mathbb{Z} \quad \text{ dado y } \zeta = e^{2\pi i/n}.$$

La suma es un poco aparatosa para escribirla cada vez y por eso se sigue empleando la notación (f, λ) de Gauss. Aparentemente la definición depende del generador g elegido, pero no es así, cualquier elección da lo mismo.

1) Lee los artículos 342–343 comparando con lo que he escrito arriba y comprueba lo que dice de que para $n-1 = 19-1 = 3\cdot 6$ se tiene $(6,2) = (6,3) = \zeta^2 + \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{16} + \zeta^{17}$.

Para un n dado, a los periodos con el mismo f (y por tanto e) Gauss los llama *similares*. Todos los resultados serán para periodos similares, por eso te he dicho que podemos considerar e y f fijados. De alguna forma los periodos similares son "disjuntos", es decir, o son idénticos o no coinciden ninguno de sus sumandos. Éstas y otras dos propiedades muy sencillas son el contenido del artículo 344. En el siguiente se enuncia un teorema. Es muy sencillo pero es importante tener en cuenta sus consecuencias, que numera I–IV. Lo más destacable para lo que se va a hacer después está resumido en IV:

El conjunto

$$\mathcal{B} = \big\{1, (f,1), (f,g), (f,g^2), \ldots, (f,g^{e-1})\big\}$$

es una especie de "base entera" al hacer sumas, restas y multiplicaciones de periodos similares. Es decir, los resultados son siempre una combinación lineal entera de los elementos de $\mathcal{B}$. Por tanto lo mismo se puede decir de cualquier polinomio en $\mathbb{Z}[x_1, \ldots, x_m]$ al ser evaluado en

periodos similares. En una identidad de este tipo, se pueden multiplicar todos los segundos argumentos por una misma constante no divisible por n y la identidad se sigue cumpliendo. Por ejemplo, para $n = 7$, $e = 3$, $f = 2$, se tiene $(2,2)^2 = 2 + (2,g)$ con $g = 3$, entonces $(2,10)^2 = 2 + (2,5g)$. En teoría de Galois se diría que se está aplicando el automorfismo dado por $\zeta \mapsto \zeta^5$.

2) Lee atentamente los artículos 344 y 345 y comprueba que es cierto lo que digo en el párrafo anterior respecto al ejemplo para $n = 7$.

Lo que vamos a ver a continuación es que, excluyendo los casos triviales $(f,0) = (f,nm)$, cada periodo se puede expresar en término de cualquier otro a través de un polinomio de $\mathbb{Q}[x]$. Te cuento la analogía moderna por si te sirve para entender mejor la situación pero te la puedes saltar y no la necesitas para leer a Gauss.

[Párrafo voluntario] Los periodos generan los cuerpos fijos intermedios de la extensión $\mathbb{Q}(\zeta)/\mathbb{Q}$. Concretamente (f,λ) genera una extensión de grado e, siempre excluyendo los casos triviales $\lambda = nm$. El grupo de Galois de $\mathbb{Q}(\zeta)/\mathbb{Q}$ es $\mathcal{U}(\mathbb{Z}_n)$ [Ste89] que es cíclico. Usando el teorema de Galois, sólo puede haber un cuerpo intermedio para cada grado e que divide a $[\mathbb{Q}(\zeta) : \mathbb{Q}] = n - 1$. Sin embargo tenemos muchos periodos. La explicación es que todos los periodos no triviales con la misma f, los que Gauss llama similares, generan el mismo cuerpo sobre $\mathbb{Q}$, ése es el contenido del teorema del artículo 346. Entonces, como te avanzaba antes, en realidad los ejemplos que se hacen en la asignatura de Teoría de Galois de hallar los cuerpos intermedios de $\mathbb{Q}(\zeta)/\mathbb{Q}$ admiten una solución inmediata: son $F = \mathbb{Q}\big((f,1)\big)$ con $f \mid n-1$ y se tiene $[F : \mathbb{Q}] = e = (n-1)/f$. Es raro que tu profesor te contase esta solución sencilla.

Para facilitarte la tarea de leer el artículo 346, te voy a contar antes un ejemplo. Lo que está marcado con interrogaciones es para que lo completes tú. Supongamos que $n = 13$ y $f = 3$, con ello $e = 4$. Podemos tomar $g = 2$ (aunque otros generadores dan el mismo resultado). La lista de los periodos, destacando a la izquierda los que aparecen en $\mathcal{B}$ con esta elección de g, es:

$$\begin{array}{rcccl} X := (3,1) & = & \zeta + \zeta^3 + \zeta^9 & = & (3,3) = (3,9) \\ Y := (3,2) & = & \zeta^2 + \zeta^6 + \zeta^5 & = & (3,6) = (3,5) \\ Z := (3,4) & = & ?????????? & = & ?????????? \\ T := (3,8) & = & \zeta^8 + \zeta^1 1 + \zeta^7 & = & (3,11) = (3,7) \end{array}$$

Supongamos que queremos expresar T en términos de X. Gauss nos dice que tomemos las potencias de 1 a $e-1$ de $X = (3,1)$ y las expresemos como combinación lineal entera de los elementos de $\mathcal{B}$, que en nuestro caso es $\{1, X, Y, Z, T\}$. Esto es posible (y algorítmico) por el art. 345.IV. En la primera ecuación no usa X evitando la tautología $X = X$. Simplemente emplea que las suma de todas las raíces de la unidad, incluyendo el uno, es cero y por tanto

$X = -1 - Y - Z - T$. Haciendo las cuentas lo que sale es

$$\begin{array}{lcccccc} (3,1)^1 & = & -1 & & -Y & -Z & -T \\ (3,1)^2 & = & ? & ? & ? & ? & ? \\ (3,1)^3 & = & 6 & +X & +3Y & & +3T \end{array}$$

Tenemos 3 ecuaciones, entonces podemos eliminar $3-1$ variables, por "métodos conocidos", según Gauss (¡hoy diríamos por eliminación de Gauss!). Al eliminar la Y y la Z nos quedamos con algo que involucra la X y la T y potencias de X en el primer miembro. De ello se deduce

$$T = -\frac{5}{3}X + \alpha X^2 - \frac{1}{3}X^3 \qquad \text{con} \quad \alpha = ?$$

3) Completa en el ejemplo anterior todo lo marcado con interrogaciones.

Esencialmente lo que hace Gauss es el ejemplo en general, sin especificar los valores. Hay un problema sutil, ¿qué hubiera ocurrido si al eliminar la Y y la Z, por casualidad también desaparece la T? El resultado habría sido $0 = -\frac{5}{3}X + \alpha X^2 - \frac{1}{3}X^3$ que no nos sirve para nada. Lo que Gauss prueba es que ese caso lleva a una contradicción con que el polinomio ciclotómico sea irreducible.

4) Lee el artículo 346 comparando con lo anterior. El ejemplo final que da Gauss es un poco más simple porque e es menor. Te lo puedes saltar.

Ahora viene lo que me tienes que entregar. Una vez más, si tienes alguna idea muy clara en otro sentido, puedes violar alguna de las directrices pero entonces me tienes que convencer de que tu idea es mejor.

5) El objetivo es que escribas la demostración del Teorema del artículo 346 con tus propias palabras y con todos los resultados y definiciones anteriores que necesites. El esquema que propongo es el siguiente:

1. Introduce los periodos y e, f y g. Ilústralo con un ejemplo sencillo. Todo eso en media página o así debería caber.

2. El siguiente paso es que demuestres la parte IV del artículo 345. Como ejemplo pon el cálculo $(3,1)^2$, para $n = 19$, el que has hecho tú para el problema 3. Todo esto no creo que te ocupe en total una página.

3. Enuncia el teorema y antes de la demostración, di que vas a explicar cómo va a través de un ejemplo. Corta y pega el de esta hoja, completando las interrogaciones y sin pararte en explicar los cálculos.

4. Escribe la demostración del teorema con tus palabras y modernizando la notación para que sea más legible. Haz lo que prefieras pero se me ocurre por ejemplo denotar $p_j = (f, \lambda g^j)$ y escribir las ecuaciones como $p_0^i = b_i + \sum_{j=0}^{e-1} a_{ij} p_j$ con $1 \leq i \leq e-1$, donde el caso $i = 1$ (primera ecuación), tiene $a_{11} = 0$ y $b_0 = a_{1j} = -1$. No escatimes espacio en dar las explicaciones que consideres necesarias que no da Gauss pero entre esto y lo del punto anterior no debería llegar a página y media, seguramente te ocupará menos.

Referencias

[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.