Pontificia Universidad Católica de Chile
Facultad de Matemáticas

Profesor: Ricardo Menares
Ayudante: José Cuevas Barrientos
Curso: Teoría de Números
Sigla: MAT2814
Fecha: 7 de noviembre de 2025

Torsión y estructura de grupo

1. Reticulados

1. Sean $\omega_1, \omega_2 \in \mathbb{C}^\times$ dos complejos $\mathbb{R}$-linealmente independientes y sea $\Lambda := \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ su reticulado.
   a) Pruebe que el área A del paralelogramo de vértices $\{0, \omega_1, \omega_1 + \omega_2, \omega_2\}$ no depende de la elección de $\mathbb{Z}$-base de Λ.
   b) Pruebe que
   $$|\{\omega \in \Lambda : |\omega| \leq R\}| = \frac{\pi}{A}R^2 + O(R).$$
   c) Concluya que existe $c > 0$ tal que
   $$|\{\omega \in \Lambda : R \leq |\omega| < R + 1\}| \leq cR.$$

2. Sean $\omega_1, \omega_2 \in \mathbb{C}^\times$ dos complejos $\mathbb{R}$-linealmente independientes y sea $\Lambda := \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ su reticulado.
   a) Verifique que, para todo $s \in \mathbb{C}$ con $\operatorname{Re} s > 2$, la serie
   $$\sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{|\omega|^s} < \infty.$$

◉◉ *b*) Pruebe que la serie
   $$\wp(z) := \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \left(\frac{1}{(\omega - z)^2} - \frac{1}{\omega^2}\right),$$
   converge absoluta y uniformemente en compactos del abierto $\mathbb{C} \setminus \Lambda$. Por ende, concluya que es holomorfa allí.
   c) Pruebe que $\wp$ es una función par (i.e., $\wp(z) = \wp(-z)$) y que es periódica respecto a Λ, a decir, $\wp(z + \omega) = \wp(z)$ para todo $\omega \in \Lambda$.

3. Recuerde que en clases vió que toda curva elíptica compleja es de la forma $\mathbb{C}/\Lambda$, donde Λ es un *reticulado* (i.e., un subgrupo abeliano libre generado por dos vectores $\mathbb{R}$-linealmente independientes). Definiremos el conjunto de endomorfismos como
   $$\operatorname{End}(\mathbb{C}/\Lambda) := \{\alpha \in \mathbb{C} \colon \alpha\Lambda \subseteq \Lambda\}.$$
   a) Pruebe que $\operatorname{End}(\mathbb{C}/\Lambda)$ es un subanillo de $\mathbb{C}$.
   b) Pruebe que, o bien $\operatorname{End}(\mathbb{C}/\Lambda) = \mathbb{Z}$, o bien $\operatorname{End}(\mathbb{C}/\Lambda)$ es un anillo de enteros de una extensión cuadrática imaginaria.
   c) Defina $\operatorname{Aut}(\mathbb{C}/\Lambda) = \operatorname{End}(\mathbb{C}/\Lambda)^\times$ como el grupo de unidades. Concluya que $|\operatorname{Aut}(\mathbb{C}/\Lambda)| \in \{2, 4, 6\}$.
   Pista: Para esto puede ser útil saber que el anillo de enteros algebraicos de la extensión cuadrática $\mathbb{Q}(\sqrt{-d})$ está generado como $\mathbb{Z}$-álgebra por el elemento $\sqrt{-d}$ si $d \not\equiv 3 \pmod 4$ o por $\frac{1}{2}(1 + \sqrt{-d})$ si $d \equiv 3 \pmod 4$. □

2. Torsión

4. Sea $E\colon y^2 = f(x) = x^3 + b_2x^2 + b_4x + b_6$ una curva elíptica.
   a) Verifique que un punto $P \in E(k)$ tiene orden 3 syss es un punto de inflexión de C (i.e., su tangente solo corta a C solamente en P).
   b) Pruebe que
   $$\frac{\mathrm{d}^2y}{\mathrm{d}x^2} = \frac{2f''(x)f(x) - f'(x)^2}{4yf(x)}.$$
   c) Concluya que $E(\mathbb{R})[3] = \mathbb{Z}/3\mathbb{Z}$.
5. Pruebe que las siguientes curvas elípticas tienen infinitos puntos racionales:
   a) $y^2 = x^3 - 2$.
   b) $y^2 = x^3 + 8$.

A. Comentarios adicionales

El «conjunto de endomorfismos» del ejercicio 3 es el honesto anillo de endomorfismos de la curva elíptica $\mathbb{C}/\Lambda$ como superficie de Riemann. La correspondencia viene probada en Silverman **[1]**, §VI.4.

Si una curva elíptica compleja $E = \mathbb{C}/\Lambda$ satisface que $\mathrm{End}(E) \ncong \mathbb{Z}$ como en el ejercicio 3*b*, entonces diremos que tiene *multiplicación compleja*. Mirando las condiciones para Λ es visible de dónde viene el nombre.

6. Sea $\mathfrak{H} := \{\tau \in \mathbb{C} : \operatorname{Im}\tau > 0\}$ el semiplano superior. Pruebe que hay numerables $\tau \in \mathfrak{H}$ tales que $E_\tau := \mathbb{C}/\Lambda_\tau$, con $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$, tiene multiplicación compleja.
7. Vamos a probar la pista del ejercicio 3*c*. Defina $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} \subseteq \mathbb{Q}(\sqrt{-d})$ como el subanillo de los elementos cuyo polinomio minimal tiene coeficientes en $\mathbb{Z}$.
   a) Pruebe que $\gamma = a + b\sqrt{-d} \in \mathbb{Q}(\sqrt{-d})$ yace en $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ syss $\gamma + \overline{\gamma} = 2a$, $\gamma \cdot \overline{\gamma} = a^2 + db^2 \in \mathbb{Z}$.
   b) Concluya que $\sqrt{-d}$ genera a $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ cuando $d \not\equiv 3 \pmod 4$ y $\frac{1}{2}(1 + \sqrt{-d})$ genera cuando $d \equiv 3 \pmod 4$.

Referencias

1. Silverman, J. H. *The arithmetic of elliptic curves* 2.ª ed. (Springer-Verlag, 2009).
2. Silverman, J. H. y Tate, J. *Rational points on elliptic curves* doi:10.1007/978-1-4757-4252-7 (Springer-Verlag, New York, 1992).

Correo electrónico: josecuevasbtos@uc.cl