# MA0609 — Tópicos en Teoría de Números

## Basado en las clases impartidas por Adrián Barquero y Darío Mena

Notas tomadas por Ignacio Rojas

Verano 2021

Estas notas no están respaldadas por los profesores y han sido modificadas (a menudo de manera significativa) después de las clases. No están lejos de ser representaciones precisas de lo que realmente se dio en clase y en particular todos los errores son casi seguramente míos.

La teoría de curvas elípticas tiene al día de hoy más de 50 años de ser desarrollada continuamente. Fermat estudió ecuaciones que tenían relación con curvas elípticas y es hasta el día de hoy que se pueden ver las relaciones con estos temas. Este tema se puede ver desde las distintas areas de la matemática: análisis, álgebra, geometría... Hay métodos para el uso de firmas digitales y seguridad en tarjetas de crédito que están relacionados con curvas elípticas.

En fín, este tema es de mucho interés en la actualidad. Nosotros nos centraremos en los números racionales siguiendo la línea del libro de Silverman & Tate [2]. En concreto los temas a tratar son los siguientes:

(a) Introducción a geometría proyectiva.

(b) Curvas cúbicas y ecuaciones en forma normal de Weierstrass.

(c) Suma de puntos y la ley de grupo en curvas elípticas.

(d) Puntos de orden finito y el teorema Nagell-Lutz.

(e) La estructura del grupo de puntos racionales en una curva elíptica y el teorema Mordell-Weil.

### Requisitos

Se asume un conocimiento básico de teoría de números. Se utilizarán conceptos de teoría de grupos y variable compleja a un nivel básico.

# Índice general

# Capítulo 1

# Curvas elípticas

## 1.1. Día 1 | 20210105

### Introducción a la geometría proyectiva

### La vista algebraica

En general hay más de una manera en la que uno puede construir el plano proyectivo y más generalmente el espacio proyectivo en varias dimensiones. A manera de motivación, a la hora de estudiar ciertos problemas en matemática, se llega a observar que es suficiente trabajar con objetos en términos de clases de equivalencia.

Por ejemplo un problema que se discute en el Silverman y Tate [2], al estudiar las soluciones racionales de la ecuación

$$x^N + y^N = 1,$$

se puede ver que si $x = \frac{a}{c}$ y $y = \frac{b}{d}$ son soluciones racionales en su forma más reducida ($\mathrm{mcd}(a, c) = \mathrm{mcd}(b, d) = 1$, y $c, d > 0$) entonces debe ocurrir que $c = d$. Esto se logra después de un breve análisis de divisibilidad. Concluimos que la solución debe tener la forma $x = \frac{a}{c}$ y $y = \frac{b}{c}$.

Esta solución satisface que $a^N + b^N = c^N$ por lo que la solución $\left(\frac{a}{c}, \frac{b}{c}\right)$ del problema en términos racionales genera una solución $(a, b, c)$ de la ecuación homogénea $x^N + y^N = z^N$. La clave aquí es que como la ecuación es homogénea, cualquier múltiplo de $(a, b, c)$, $(ta, tb, tc)$ con $t \in \mathbb{R}$, va a ser una solución al mismo problema. Pero como estas soluciones se obtienen de manera relativamente trivial, podríamos querer considerarlas como equivalentes. Este tipo de razonamiento lleva a la definición algebraica del plano proyectivo.

**Definición 1.1.1.** El plano proyectivo sobre un cuerpo $K$ es el cociente del conjunto $\{(a,b,c) \in K^3 \backslash \{(0,0,0)\}\}$ por la relación

$$(a,b,c) \sim (a',b',c') \iff \exists t \in K^\times (a = ta',\ b = tb', c = tc').$$

Denotamos entonces

$$\mathbb{P}^2_K = \{x \in K^3 \backslash \{0\}\} \Big/ \sim,$$

y la clase de equivalencia de $(a,b,c)$ la denotamos $[a,b,c]$ y se llamarán sus coordenadas homogéneas.

*¿Qué pasa si incluimos el cero en nuestra definición del plano proyectivo?*

Bueno, volviendo al ejemplo que presentamos, nos gustaría que nuestras soluciones estén en correspondencia. Claramente $(0,0,0)$ resuelve la ecuación homogénea, pero no la que tiene forma racional. Quizás de manera más interesante, $(1,-1,0)$ resuelve la ecuación homogénea con exponente impar. Pero esta no da una solución de la ecuación racional, entonces podríamos pensar por ejemplo que tenemos $((a_j,b_j,c_j)) \subseteq \mathbb{R}^3$ una sucesión de soluciones reales que converge a $(1,-1,0)$ y $c_j > 0$. Esta sucesión si genera soluciones $\left(\frac{a_j}{c_j}, \frac{b_j}{c_j}\right)$ de la ecuación racional y cuando $j \to \infty$ entonces este par ordenado tiende a $(\infty, -\infty)$. Podemos entonces pensar que las tripletas con tercera coordenada nula corresponden con soluciones que se encuentran en el infinito. Esta clase de puntos en el infinito es fundamental y lo estudiaremos más adelante.

**Definición 1.1.2.** El espacio proyectivo en $n$ dimensiones sobre un cuerpo $K$ es el conjunto

$$\mathbb{P}^n_K = \{x \in K^{n+1} \backslash \{0\}\} \Big/ \sim$$

donde la equivalencia es $x \sim x' \iff \exists t \in K^\times (x = tx')$. De igual manera denotamos la clase de $x$ como $[x]$. Las coordenadas de $[x]$ igualmente se llamarán coordenadas homogéneas.

Más adelante vamos a definir curvas en el espacio proyectivo. En este momento vamos a definir lo que entenderemos como una recta en el plano proyectivo. En principio verificar que un punto proyectivo $[a,b,c]$ está en una recta proyectiva consiste en ver que cualquier elemento de la clase de equivalencia satisface la ecuación mencionada.

**Definición 1.1.3** (Recta en el plano proyectivo)**.** Una recta en el plano proyectivo $\mathbb{P}^2_K$ es el conjunto de puntos $[a,b,c]$ cuyas coordenadas satisfacen una ecuación de la forma

$$\alpha X + \beta Y + \gamma Z = 0,$$

donde $\alpha, \beta, \gamma \in K$ no son todos nulos.

En en el plano usual, una recta es el conjunto de puntos que satisface una ecuación $\alpha x + \beta y + \gamma = 0$. En el caso proyectivo, la definición de recta que obtuvimos es básicamente lo que obtendríamos de esta ecuación al hacerla homogénea.

**Una visión geométrica**

Sabemos que en $\mathbb{R}^2$ vale que dos puntos determinan una única recta y similarmente dos rectas se intersecan en un único punto salvo cuando son paralelas. Entonces buscamos extender el concepto de obtener una noción más completa, ¡quisiéramos poder decir que cualesquiera dos rectas se intersecan en un punto!

La idea va a ser asociar a cada recta en el plano una *dirección*. Al hacer esto, estaríamos agregándole un poco más de *información* a una recta. Entonces una recta va a ser el conjunto de puntos *y una dirección*. Para nosotros, dos rectas paralelas tendrán la misma dirección y como decimos ahora que la dirección es parte de la recta, las paralelas *coinciden en la intersección*.

Extendemos el concepto de recta agregando "la dirección" como un punto. Si trabajamos sobre $\mathbb{R}$, habrá que agregar un número infinito de puntos. Porque si agregamos sólo un punto en el infinito como dirección entonces dos pares de rectas paralelas se intersecan en el mismo punto. En particular dos rectas distintas se intersecarían en dos puntos y eso contradice el hecho de que dos rectas distintas se intersecan en un único punto. Esto nos lleva a una idea geométrica para definir el plano proyectivo.

**Definición 1.1.4** (Plano afín sobre $K$)**.** Sea $K$ un cuerpo, el plano afín sobre $K$ es el conjunto $\mathbb{A}^2_K = \{\, (x, y) \in K^2 \,\}$.

**Definición 1.1.5** (Espacio afín n-dimensional)**.** El espacio afín sobre un cuerpo $K$ es el conjunto $\mathbb{A}^n_K = \{\, (x_1, x_2, \ldots, x_n) \in K^n \,\}$.

Observe ahora la diferencia aquí con el plano proyectivo, se necesitaban tres coordenadas. Aquí en el plano afín necesitamos sólo dos. Análogamente en el espacio proyectivo de $n$ dimensiones, necesitamos $n + 1$ coordenadas, mientras que en el $n$-espacio afín usamos $n$ coordenadas.

**Definición 1.1.6** (Plano proyectivo sobre K (geometricamente))**.** El plano proyectivo se define como el conjunto

$$\mathbb{P}^2_K = \mathbb{A}^2_K \cup \{\, \text{direcciones en } \mathbb{A}^2_K \,\}.$$

Consideramos que dos rectas en $\mathbb{A}^2_K$ tienen la misma dirección cuando son paralelas.

Por tanto una dirección se puede considerar como una clase de equivalencia de rectas. Definimos una equivalencia en el conjunto de las rectas en $\mathbb{A}^2_K$ al considerar dos rectas como equivalentes cuando son paralelas. Así las direcciones en $\mathbb{A}^2_K$ son las clases de equivalencia de rectas paralelas.

Entonces los puntos de $\mathbb{P}^2_K$ correspondientes a las direcciones, los llamamos "puntos en el infinito". Al conjunto de puntos en el infinito de hecho lo consideramos una recta en $\mathbb{P}^2_K$, se le llama recta en el infinito.

**Ejemplo 1.1.7.** La noción de punto en el infinito se puede asociar con la idea de ver un par de lineas de tren. Desde un punto de vista, cuando se ve en la dirección de las lineas en una situación adecuada, pareciera que en el horizonte las lineas se tocan.

TO DO: Agregar imagen vectorizada de lineas de tren tocándose.

Bajo esta versión geométrica, una recta en $\mathbb{P}^2_K$ se define de una manera distinta.

**Definición 1.1.8** (Recta proyectiva (geometricamente))**.** Una recta en $\mathbb{P}^2_K$ es la unión de puntos de una recta en $\mathbb{A}^2_K$ con su correspondiente dirección.

De acuerdo con esta definición, dos rectas en el plano proyectivo sí se intersecan en un *único punto*. Si dos rectas no son paralelas se intersecan en únicamente un punto del plano afín y sus direcciones son distintas. Entonces el punto en el infinito que agregamos a ambas rectas no coincide. En el caso que las rectas sean paralelas, no se intersecan en ningún punto del plano afín. Pero pertenecen a la misma clase de equivalencia y por tanto tienen el mismo punto en el infinito asociado. El último caso es el de la recta en el infinito que interseca a todas las rectas pues todas llevan una dirección asociada.

Para reconciliar las definiciones establecemos la equivalencia entre ellas. Redefinimos el conjunto de direcciones que originalmente lo consideramos como un conjunto de clases de equivalencia. Basta considerar sólo aquellas rectas que pasan por el origen, de la cual sólo hay una por cada clase de equivalencia. Vamos a usar estas rectas para describir el conjunto de direcciones a manera de "representantes canónicos".

Las rectas que pasan por el origen tienen la forma $Ay = Bx$ donde $A, B$ no son ambos cero. Ciertamente $(A, B)$ y $(A', B')$ definen la misma recta cuando existe $t \in K^\times$ tal que $A = tA'$ y $B = tB'$. Aquellos con mente sagaz habrán reconocido esta idea como una que hicimos recién. El conjunto de direcciones en $\mathbb{A}^2_K$ se puede describir como el conjunto de puntos $[A, B] \in \mathbb{P}^1_K$ donde

$$[A, B] = \{\, (tA, tB) \in K^2 \backslash \{\, (0, 0) \,\},\ t \in K^\times \,\}.$$

Concluimos que $\mathbb{P}^2_K = \mathbb{A}^2_K \cup \mathbb{P}^1_K$ donde $[A, B]$ corresponde con la dirección de la recta $Ay = Bx$. De manera totalmente análoga se puede ver que $\mathbb{P}^n_K = \mathbb{A}^n_K \cup \mathbb{P}^{n-1}_K$.

## 1.2. Día n+1 | 20210113

Hemos concluido la lección anterior observando ejemplos de intersecciones entre curvas. Para lograr que dos curvas de grados $d_1$ y $d_2$ se intersecaran en $d_1 \cdot d_2$ puntos, necesitábamos trabajar tanto en el plano proyectivo como en $\mathbb{C}$. Continuamos con otro ejemplo:

**Ejemplo 1.2.1.** Consideramos las curvas

$$C_1 : \ x + y = 2,$$
$$C_2 : \ x^2 + y^2 = 2.$$

La recta $C_1$ interseca al círculo de forma tangencial en el punto $(1, 1)$. De hecho si

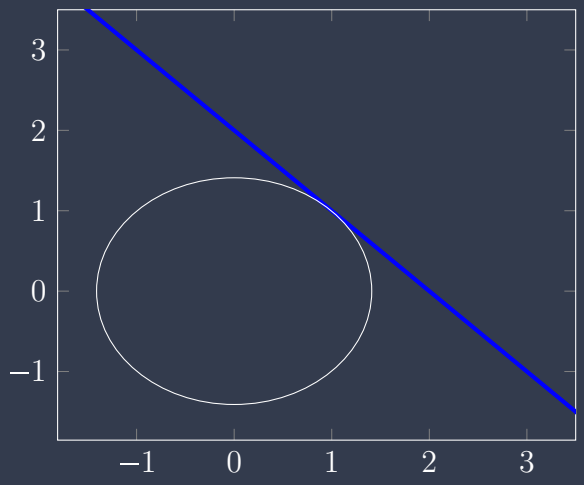


Figura 1.1: aaa

homogenizamos y buscamos las intersecciones de las curvas proyectivas

$$\tilde{C}_1 : \ x + y = 2z,$$
$$\tilde{C}_2 : \ x^2 + y^2 = 2z^2,$$

entonces despejamos $z = \frac{x+y}{2}$. Lo que nos lleva a $x^2 + y^2 = 2\left(\frac{x+y}{2}\right)^2$. Despejando vale que $(X - Y)^2 = 0$ y no podría ocurrir que $X, Y$ son ambos cero y $X = Y$. Esto nos lleva al punto $[X, X, X] = [1, 1, 1] \in \tilde{C}_1 \cap \tilde{C}_2$ y este punto corresponde al punto afín que ya habíamos encontrado.

Nosotros esperábamos dos puntos de intersección, pero no hay manera ni siquiera pasando por los complejos. Sólo obtenemos un punto de intersección y esto ocurre

porque la recta interseca de manera tangencial. Este problema es el análogo al de una variable, recuerde que el teorema fundamental del álgebra garantiza la existencia cierto número de raíces para los polinomios. Lo que no hemos mencionado es la *multiplicidad* de la raíz. En este caso vemos que la misma ecuación $(X-Y)^2=0$ nos dice que la raíz tiene multiplicidad dos.

En conclusión sólo encontramos un punto de intersección, incluso después de haber buscado posibles puntos en el infinito. Esto es porque $[1,1,1]$ se debe contar con multiplicidad dos y corresponde con el hecho de que ambas curvas se intersecan de manera tangencial en este punto. De hecho, se ve reflejado en que al resolver el sistema de ecuaciones obtuvimos la ecuación $(X-Y)^2=0$.

Este no es el único caso en que esto puede ocurrir y el siguiente ejemplo lo ilustra.

**Ejemplo 1.2.2.** Considere ahora la curvas

$$\begin{aligned} C_1 &: \ y = x, \\ C_2 &: \ y^2 = x^3. \end{aligned}$$

aregar figura Estas curvas se intersecan en dos puntos del plano afín. Al homogenizar obtenemos

$$\begin{aligned} \tilde{C}_1 &: \ X - Y = 0, \\ \tilde{C}_2 &: \ X^3 - Y^2 Z = 0, \end{aligned}$$

y resolviendo llegamos a $X^3 - X^2Z = 0$ y de aquí que $X = 0$ ó $X = Y = Z$. Si $X = 0$, entonces $Y = 0$ y así $Z$ queda libre lo que nos lleva a los puntos $[1,1,1]$ y $[0,0,1]$. A diferencia del caso anterior, no hay multiplicidades mayores a uno. Aquí lo que ocurre es que uno de los puntos de intersección es un punto que no es suave. Las rectas cuyas direcciones aproximan la identidad tienen dos puntos de intersección con la curva cuspidal, entonces en el límite, el punto singular $[0,0,1]$ tiene multiplicidad dos. agregar figura

**Ejemplo 1.2.3.** Esta vez consideramos las curvas

$$\begin{aligned} C_1 &: \ x + y + 1 = 0, \\ C_2 &: \ 2x^2 + xy - y^2 + 4x + y + 2 = 0. \end{aligned}$$

Aquel que esté atento podrá notar que

$$2x^2 + xy - y^2 + 4x + y + 2 = (x + y + 1)(2x - y + 2)$$

y así $C_1 \subseteq C_2$ lo que nos dice que la cantidad de puntos de intersección es infinita. Pero entonces las situaciones así no deben entrar en la consideración de los puntos de intersección de manera tan vaga. En el caso de $\mathbb{A}^2_{\mathbb{R}}$ hay infinitos puntos por lo que debemos especificar lo que buscamos.

**Definición 1.2.4.** Sea $C:\ f(x,y) = 0$ una curva con $f \in K[x,y]$. Si factorizamos $f$ como un producto de polinomios irreducibles $f = \prod_{j=1}^{n} p_j$, entonces los componentes de la curva $C$ son las curvas $C_j:\ p_j(x,y) = 0$. Diremos que $C$ es irreducible cuando tenga un único componente. Es decir, sólo si el polinomio $f$ es irreducible.

**Ejemplo 1.2.5.** De las curvas estudiadas en el ejemplo anterior, la curva $C_1$ es irreducible al ser un polinomio lineal y la segunda curva se puede factorizar en dos componentes. Ambas rectas son las componentes irreducibles de esta curva.

**Definición 1.2.6.** Diremos que dos curvas afines $C_1, C_2$ no tienen componentes en común si sus componentes irreducibles son distintos.

Un resultado básico en teoría de curvas que no vamos a demostrar es el siguiente:

**Proposición 1.2.7.** *Si $C_1, C_2$ son dos curvas afines sin componentes en común, entonces $C_1 \cap C_2$ es un conjunto finito.*

*Observación* 1.2.8. De manera análoga al caso afín, se definen componentes de curvas proyectivas y la noción de dos curvas proyectivas sin componentes comunes.

El teorema de Bezout es más general que este resultado. Con lo que hemos visto hasta ahora, lo podemos enunciar.bajé a agarrar agua

Por ahora mencionamos las siguientes propiedades:

(a) Si $P \notin C_1 \cap C_2$, entonces $I(C_1 \cap C_2, P) = 0$.

(b) Si $P \in C_1 \cap C_2$ y $P$ es un punto no singular de $C_1$ y $C_2$, y si adicionalmente $C_1$ y $C_2$ tienen direcciones tangenciales diferentes en $P$, entonces $I(C_1 \cap C_2, P) = 1$. En este caso, se dice que $C_1$ y $C_2$ se intersecan en $P$ de manera transversal.

(c) Si $P \in C_1 \cap C_2$ y $C_1$ y $C_2$ no se intersecan transversalmente, entonces $I(C_1 \cap C_2, P) \geqslant 2$.

**Teorema 1.2.9** (Bezout). *Sean $C_1, C_2 \subseteq \mathbb{P}^2_{\mathbb{C}}$ sin componentes en común. Entonces vale que*

$$\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = \deg(C_1)\deg(C_2).$$

*En particular si $C_1, C_2$ son suaves y únicamente tienen intersecciones transversales, entonces*

$$|C_1 \cap C_2| = \deg(C_1)\deg(C_2)$$

*y en todo momento se tiene la desigualdad $|C_1 \cap C_2| \leqslant \deg(C_1)\deg(C_2)$.*

## 1.3. Día n+2 | 20210114

**Multiplicidad de la intersección de dos curvas**

Vamos a estudiar algunas propiedades y ejemplos de cálculo de la multiplicidad o índice de intersecciones $I(C_1 \cap C_2, P)$. Vamos a comenzar con un teorema que establece la existencia de la multiplicidad de la intersección y nos permite hacer cálculos.

Rápidamente para poder simplificar la notación introducimos los conceptos de variedad.

**Definición 1.3.1.** La variedad afín de $f$ es el conjunto de ceros de $f$ dentro del espacio afín $\mathbb{A}^2$. Denotamos

$$V(f) = \{\, x \in \mathbb{A}^2 :\ f(x) = 0 \,\}$$

y análogamente la variedad proyectiva de $F$ es su conjunto de ceros dentro del espacio proyectivo. Este conjunto es

$$V(F) = \{\, X \in \mathbb{P}^2 :\ F(X) = 0 \,\}.$$

**Teorema 1.3.2.** *Considere $V(f), V(g)$ dos curvas afines en $\mathbb{A}^2_{\mathbb{C}}$ y $P \in \mathbb{A}^2_{\mathbb{C}}$ dado. Entonces existe un número $I(V(f) \cap V(g), P)$ definido de manera única tal que las siguientes propiedades se satisfacen*:

(a) *$I(V(f) \cap V(g), P) \in \mathbb{Z}_{\geqslant 0}$, a menos que $P$ esté en un componente común de $V(f), V(g)$ y en ese caso $I(V(f) \cap V(g), P) = \infty$.*

(b) *$I(V(f) \cap V(g), P) = 0$ si y sólo si $P \notin V(f) \cap V(g)$.*

(c) *Dos rectas distintas se intersecan con multiplicidad uno en su punto de intersección.*

(d) *$I(V(f) \cap V(g), P) = I(V(g) \cap V(f), P)$.*

(e) *Si $f = \prod p_i^{\alpha_i}$ y $g = \prod q_i^{\beta_i}$, entonces*

$$I(V(f) \cap V(g), P) = \sum_{i,j} \alpha_i \beta_j I(V(p_i) \cap V(q_j), P).$$

(f) $I(V(f) \cap V(g), P) = I(V(f) \cap V(g + hf), P)$ *para* $h \in \mathbb{C}[x, y]$.

**Definición 1.3.3.** El número $I(V(f) \cap V(g), P)$ se llama multiplicidad de la intersección de $V(f)$ y $V(g)$ en $P$.

**Ejemplo 1.3.4.** (a) $x^2$ con $y$

(b) círculo con recta

(c) cuspidal con identidad

**Definición 1.3.5.** Sea $f$ un polinomio con coeficientes en $\mathbb{C}$ y $P \in V(f)$. La multiplicidad de $f$ en $P$

# Capítulo 2

# Análisis de Fourier

## 2.1. Día k | 20210203

### La tranformada de Fourier

Trabajaremos en $\mathbb{R}^d$ con $m$ la medida de Lebesgue, las funciones a considerar son $f : \mathbb{R}^d \to \mathbb{C}$ y suponemos que son Borel medibles. De aquí tenemos el espacio

$$L^p(\mathbb{R}^d) = \left\{ f : \mathbb{R}^d \to \mathbb{C} \text{ medible}, \int_{\mathbb{R}^d} |f(x)|^p \boldsymbol{d}x < \infty \right\}$$

para $p \in [1, \infty[$. En el caso cuando $p = \infty$ tenemos que $\|f\|_\infty = \operatorname{ess\,sup}(f)$ como el $\inf_{C>0}\{ m(|f| \geqslant C) = 0 \}$ y definimos $L^\infty$ de manera análoga a $L^p$ como $\{ \|f\|_\infty > \infty \}$. Trabajamos también con el espacio $C_0$... estaba cambiando el word wrap

Así, $f$ es integrable cuando $f_r$ y $f_i$ lo sean.

Si $z \in \mathbb{C},\ z = x + iy$ definimos el módulo complejo como $|z| = \sqrt{x^2 + y^2}$. El módulo complejo cumple algunas propiedades tales como la desigualdad triangular para integrales $\left|\int f \boldsymbol{d}x\right| \leqslant \int |f| \boldsymbol{d}x$. Recordemos la identidad de Euler, si $x \in \mathbb{R}$ entonces $e^{ix} = \cos(x) + i \sin(x)$ y este número tiene módulo 1.

**Definición 2.1.1.** Sea $f \in L^1(\mathbb{R}^d)$, definimos su transformada de Fourier como

$$\mathcal{F}(f)(\xi) = \hat{f}(\xi) = \int_{\mathbb{R}^d} f(x) e^{-2\pi i \langle x|\xi \rangle} \boldsymbol{d}x,\ \xi \in \mathbb{R}^d.$$

Note que $|\hat{f}(\xi)| \leqslant \|f\|_1$.

**Teorema 2.1.2.** *El mapeo $f \mapsto \hat{f}$ es una aplicación continua entre $L^1$ y $L^\infty$. Vale que $\left\|\hat{f}\right\|_\infty \leqslant \|f\|_1$. Además si $f \in L^1$ entonces $\hat{f}$ es una función uniformemente continua.*

**Prueba**

Note que inmediatamente de la definición tenemos $|\hat{f}(\xi)| \leqslant \|f\|_1$ para $\xi \in \mathbb{R}^d$ lo que implica $\left\|\hat{f}\right\|_\infty \leqslant \|f\|_1$.
Por otro lado considere la cantidad

$$\begin{aligned}|\hat{f}(\xi+h) - \hat{f}(\xi)| &= \left|\int f(x)e^{-2\pi i\langle x|\xi+h\rangle}\boldsymbol{d}x - \int f(x)e^{-2\pi i\langle x|\xi\rangle}\boldsymbol{d}x\right| \\ &\leqslant \int |f(x)||e^{-2\pi i\langle x|\xi\rangle}||e^{-2\pi i\langle x|\xi\rangle} - 1|\boldsymbol{d}x \\ &= \int |f(x)||e^{-2\pi i\langle x|\xi\rangle} - 1|\boldsymbol{d}x.\end{aligned}$$

La cantidad $|e^{-2\pi i\langle x|\xi\rangle} - 1|$ tiende a cero conforme $h \to 0$ por lo que aplicando el teorema de convergencia dominada tenemos que $|\hat{f}(\xi+h) - \hat{f}(\xi)| \to 0$ cuando $h \to 0$ independiente de $\xi$.

**Lema 2.1.3** (Riemann-Lebesgue). *Si $f \in L^1$, entonces $\hat{f}(\xi) \to 0$ cuando $\|\xi\| \to \infty$. Es decir, $\hat{f} \in C_0$.*

**Prueba**

Sea $R = \times_{i\in[d]}[a_i, b_i] \subseteq \mathbb{R}^d$ un rectángulo en $\mathbb{R}^d$. Si $f = \mathbf{1}_R$ entonces tenemos que $f = \prod_{i\in[d]} \mathbf{1}_{[a_i,b_i]}$.aaaa me perdí
Vale entonces

$$\hat{\mathbf{1}}_{[a,b]}(\xi) = \int_a^b e^{-2\pi i x\xi}\boldsymbol{d}x = \int_a^b (\cos(-2\pi x\xi) + i\sin(-2\pi x\xi))\boldsymbol{d}x.$$

Esta cantidad resulta ser $\frac{-1}{2\pi i\xi}(e^{-2\pi ib\xi} - e^{-2\pi ia\xi})$ que tiende a cero cuando $|\xi| \to 0$.
Así $\hat{\mathbf{1}}_R(\xi) \to 0$ cuando $\|\xi\| \to \infty$.
Para $f \in L^1$ en general, aproximamos con funciones simples cuyas indicadoras son sobre rectángulos.

Recuerde que la convolución de funciones en $L^1$ es

$$f * g(x) = \int f(x-y)g(y)\boldsymbol{d}y.$$

La convolución es cerrada en $L^1$, es asociativa y conmutativa.

**Teorema 2.1.4.** *Tome $f \in L^p, g \in L^1$ para $p \in [1, \infty]$. Entonces $f * g \in L^p$ y $\|f * g\|_p \leqslant \|f\|_p \|g\|_1$.*

De este resultado extraemos que la convolución hereda las propiedades más bonitas de sus operandos.

Prueba

Por Minkowski tenemos

()

finish

**Proposición 2.1.5.** *Para $f, g \in L^1$ vale que*:

(a) $\mathcal{F}(f * g) = \mathcal{F}(f)\mathcal{F}(g)$.

(b) $\mathcal{F}(\tau_h f)(\xi) = e^{2\pi i \langle h|\xi\rangle}\mathcal{F}(f)(\xi)$. *Es decir, traslación se convierte en modulación.*

(c) *Si $A \in O(d)$, el grupo ortogonal en $d$ dimensiones, entonces*

$$\mathcal{F}(f(A\cdot))(\xi) = \mathcal{F}(f(A\xi)).$$

(d) *Si $f_\lambda(x) = \frac{1}{\lambda^d}\left(\frac{x}{\lambda}\right)$ entonces $\mathcal{F}(f_\lambda)(\xi) = \mathcal{F}(f)(\lambda\xi)$.*

(e) $\mathcal{F}\left(\frac{\partial f}{\partial x_j}\right)(\xi) = 2\pi i \xi_j \mathcal{F}(f)(\xi)$, *cuando $f_j \in L^1$. Y para el otro lado,* $\mathcal{F}(-2\pi i x_j f)(\xi) = \mathcal{F}\left(\frac{\partial f}{\partial \xi_j}\right)(\xi)$ *cuando $x_j f \in L^1$.*

Note que a partir del último punto, podemos iterar con derivadas de orden superior cuando todo esté bien definido. Vale por ejemplo que

$$\mathcal{F}\left(\frac{\partial^2 f}{\partial x_j \partial x_k}\right)(\xi) = (2\pi i \xi_j)(2\pi i \xi_k)\mathcal{F}(f)(\xi).$$

Naturalmente nos preguntamos,

*¿Se puede recuperar $f$ por medio de $\mathcal{F}(f)$?*

Cuando se trabaja con series de Fourier, se puede recuperar $f$ por medio de sus coeficientes de Fourier. Lo esperado es que $f(x) = \int \hat{f}(\xi) e^{2\pi i \langle x|\xi\rangle} \boldsymbol{d}\xi$. Pero $\hat{f}$ no necesariamente es integrable.

### La clase de Schwartz

Indistintamente hablaremos de la derivada parcial de $f$ respecto a $x_j$ como $\partial_j f$ o $D_j f$. La $m$-ésima derivada será en su lugar $\partial_j^m f$ o $D_j^m f$. Introducimos brevemente la notación multi-índice, si $\alpha \in \mathbb{N}^d$ entonces

$$D^\alpha f = D_1^{\alpha_1} \cdot \ldots \cdot D_d^{\alpha_d} f.$$

Por ejemplo $D^{(3,1,4)} f = \frac{\partial^8 f}{\partial x_1^3 \partial x_2 \partial x_3^4}$. También tenemos $\alpha! = \prod \alpha_j!$ y $x^\alpha = \prod x_j^{\alpha_j}$.

**Definición 2.1.6.** Una función $f$ está en la clase de Schwartz $\mathcal{S}(\mathbb{R}^d)$ si es infinitamente diferenciable y todas sus derivadas decrecen rápidamente a infinito. Es decir para $\alpha, \beta$ multi-índices vale

$$\sup_{\mathbb{R}^d} |x^\alpha D^\beta f(x)| = \rho_{\alpha,\beta}(f) < \infty.$$

Inmediatamente de la definición $\mathcal{C}_c^\infty \subseteq \mathcal{S}$, también $\rho_{\alpha,\beta}$ es una seminorma lo que nos puede llevar a una topología. El conjunto $\{ \rho_{\alpha,\beta} \}$ es una familia contable. Entonces $(f_n) \to 0$ en $\mathcal{S}$ cuando $\rho_{\alpha,\beta}(f_n) \to 0$ para $\alpha, \beta$ son cualquier multi-índice. Podemos ver que $\mathcal{S}$ es un espacio de Fréchet, la métrica que se puede definir es

$$d(f,g) = \sum_{j \in \mathbb{N}} \frac{\rho_j(f-g)}{2^j(1+\rho_j(f-g))},$$

donde $(\rho_j)$ es una enumeración de las seminormas.

**Teorema 2.1.7.** *Ocurre que $\mathcal{S}$ es denso en $L^p$ para $p \in [1, \infty[$.*

Note que si valiese que $\mathcal{S} \subseteq L^p$ entonces, como $\mathcal{C}_c^\infty \subseteq \mathcal{S}$ y $\mathcal{C}_c^\infty$ es denso ya entonces estaríamos listos. Basta probar que el espacio de Schwartz está en $L^p$.

Prueba

Tome $f \in \mathcal{S}$, entonces

$$\begin{aligned}
\int |f|^p \boldsymbol{d}x &= \int (1+|x|^{d+1}) \frac{|f|}{1+|x|^{d+1}} \\
&\leqslant \int \frac{c(|f| + \sum_{j\in[d]} |x_j|^{2d+2}|f|)^p}{(1+|x|^{d+1})^p} \boldsymbol{d}x \\
&\leqslant \int \frac{c(\rho_{0,0} f + \sum_{j\in[d]} \rho_{(2d+2)e_j,0} f)^p}{(1+|x|^{d+1})^p} \boldsymbol{d}x \\
&\leqslant c_2 \int \frac{\boldsymbol{d}x}{(1+|x|^{d+1})^p} < \infty
\end{aligned}$$

no terminé

En particular, el espacio de Schwartz está contenido en $L^1$ y por tanto podemos definir la transformada de Fourier en $\mathcal{S}$.

**Teorema 2.1.8.** *El mapeo $f \mapsto \hat{f}$ es continuo sobre $\mathcal{S}$ y cumple*:

(a) $\int f\hat{g} = \int \hat{f}g$.

(b) *Vale la fórmula de inversión*

$$f(x) = \int \hat{f}(\xi) e^{2\pi i \langle x|\xi\rangle} d\xi.$$

Precisamos un par de lemas antes de probar este resultado. Note que la fórmula de inversión tiene *casi* las misma forma que la fórmula que la transformada ordinaria. En cierto sentido $f(x) = \hat{\hat{f}}(-x)$.

**Lema 2.1.9.** *Si $f(x) = e^{-\pi\|x\|^2}$, entonces $\hat{f} = f$.*

Prueba

me salté la prueba, DO

Ahora podemos probar el teorema de la fórmula de inversión.

Prueba

Tenemos que para $f \in \mathcal{S}$ y $\alpha, \beta$ multi-índices vale que

$$\begin{aligned}\xi^\alpha D^\beta \hat{f}(\xi) &= (\prod \xi_j^{\alpha_j})(D_{\xi_1}^{\beta_1} \dots D_{\xi_d}^{\beta_d})\hat{f}(\xi) \\ &= C(\mathcal{F}((D_{\xi_1}^{\beta_1} \dots D_{\xi_d}^{\beta_d})(\prod_{j\in[d]} x_j^{\beta_j}))) \dots\end{aligned}$$

$D^\alpha(x^\beta f)$ es una suma de monomios por derivadas de $f$.

## 2.2. Día k+1 | 20210204

**La transformada de Fourier en $L^2$**

anotación sobre el conjugado y extensión a L2.

En $L^2$ por tanto existe una extensión de la transformada de Fourier. Los límites en el enunciado del teorema son consecuencia de la continuidad de la transformada pues lo que tenemos es que $f\mathbf{1}(B(0,R)) \to f$ y $\hat{f}\mathbf{1}(B(0,R)) \to \hat{f}$ donde ambas convergen en $L^2$. Esto se conoce como extender el operador por densidad y más adelante veremos cómo extender esto a $L^p$ para $p > 2$.

Vimos que en $L^1$ no necesariamente hay inversa de la transformada porque esta no necesariamente es integrable. Tomemos $f \in L^1(\mathbb{R}^d)$, esperamos que $f(x) = \int_{\mathbb{R}^d} \hat{f}(\xi) e^{2\pi i \langle x|\xi\rangle} \boldsymbol{d}\xi$ en algún sentido de convergencia. Sin embargo no estamos asumiendo que $\hat{f}$ es integrable, puede que dicha integral ni siquiera tenga sentido. Aún siendo $f$ la indicadora de un intervalo, la integral en cuestión no existe.

**Ejemplo 2.2.1.** Si $f = \mathbf{1}([-a,a])$, entonces $\hat{f}(\xi) = \frac{\sin(\pi a \xi)}{\pi a \xi}$ y esta función no es integrable en el sentido de Lebesgue.

Dado esto, necesitamos aplicar métodos de sumabilidad.

**Definición 2.2.2.** Sea $\varepsilon > 0$, definimos la media de Abel de $f$ como

$$A_\varepsilon f = \int_{\mathbb{R}^d}$$

**Definición 2.2.3.** Si definimos $G_\varepsilon f = \int f(x) e^{-\varepsilon \|x\|^2} \boldsymbol{d}x$ para $\varepsilon > 0$, entonces decimos que $\int f$ es Gauss sumable a $\ell$ si $\lim_{\varepsilon \to 0} G_\varepsilon f = \ell$.

Ambos promedios se pueden escribir de la forma

$$M_{\varepsilon,\Phi} f = M_\varepsilon f = \int_{\mathbb{R}^d} \Phi(\varepsilon x) f(x) \boldsymbol{d}x$$

con $\Phi \in \mathcal{C}_0$ y $\Phi(0) = 1$.

Entonces la idea es modificar un poco las cosas para obtener cierta convergencia. Para lo que queremos hacer, necesitamos las transformadas de Fourier de $e^{-\varepsilon\|x\|^2}$ y $e^{-\varepsilon\|x\|}$. Sabemos que $\mathcal{F}(e^{-\pi\|x\|^2})(\xi) = e^{-\pi\|\xi\|^2}$ por lo que para tener la de $\varepsilon$ basta con hacer una dilatación. Si llamamos $g(x) = e^{-\pi\|x\|^2}$, entonces $e^{-\varepsilon\|x\|^2} = g\left(\sqrt{\frac{\varepsilon}{\pi}} x\right)$ y como $\mathcal{F}(\lambda^{-d} h(\lambda^{-1} x)) = \hat{h}(\lambda\xi)$, entonces tendremos que

$$\mathcal{F}(e^{-\varepsilon\|x\|^2})(\xi) = \mathit{calc}.$$

**Teorema 2.2.4.** *En general, si $a > 0$, tenemos que*

$$\int_{\mathbb{R}^d} e^{-\pi a\|x\|^2} e^{-2\pi i\langle x|\xi\rangle} \boldsymbol{d}x = a^{-\frac{d}{2}} e^{-\frac{\pi}{a}\|\xi\|^2}.$$

*También vale que*

$$\int_{\mathbb{R}^d} e^{-2\pi a\|x\|} e^{-2\pi i\langle x|\xi\rangle} \boldsymbol{d}x = c(d)\frac{a}{(a^2+\|\xi\|^2)^{\frac{d+1}{2}}}$$

*con* $c(d) = \frac{\Gamma\left(\frac{d+1}{2}\right)}{\pi^{\frac{d+1}{2}}}$.

Prueba

Ejercicio

Para simplificarnos los cálculos, llamemos $W = W(\xi, a) = \mathcal{F}(e^{-4\pi^2 a\|\cdot\|^2})$ y $P = P(\xi, a) = \mathcal{F}(e^{-2\pi a\|\cdot\|})$. A $W$ lo conocemos como el núcleo de Gauss-Weierstrass y $P$ como el núcleo de Poisson.

Así, queremos probar que las medias de Abel y Gauss de $\int \hat{f}\exp(2\pi i\langle x|\xi\rangle)\boldsymbol{d}\xi$ convergen a $f$ en norma y casi por doquier. Esto nos diría que

$$f(x) = \int_{\mathbb{R}^d} \hat{f}(\xi) e^{2\pi i\langle x|\xi\rangle} w(\xi)\boldsymbol{d}\xi$$

lo que nos permite recuperar $f$ por medio de su transformada.

Tomemos $\Phi \in \mathcal{C}_0 \cap L^1$, con $\Phi(0) = 1$. Llame $\varphi = \hat{\Phi}$ y $\varphi_\lambda = \lambda^{-d}\varphi(\lambda^{-1}x)$ para $\lambda$ positivo. Con esta notación vale que

$$\Phi(x) = \exp\left(-4\pi^2\|x\|^2\right) \Rightarrow \varphi_\varepsilon = W(algo),$$
$$\Phi(x) = \exp(-2\pi\|x\|) \Rightarrow \varphi_\varepsilon = P(\xi, \varepsilon).$$

**Teorema 2.2.5.** *Si $f, \Phi \in L^1(\mathbb{R}^d)$ y $\varphi = \hat{\Phi}$, entonces*

$$\int \hat{f}(\xi) e^{2\pi i\langle x|\xi\rangle}\Phi(\varepsilon\xi)\boldsymbol{d}\xi = \int f(x)\varphi_\varepsilon(x-\xi)\boldsymbol{d}x, \varepsilon > 0.$$

*En particular,* $\int \hat{f}(\xi) e^{2\pi i\langle x|\xi\rangle} e^{-2\pi\varepsilon\|\xi\|}\boldsymbol{d}\xi = \int f(x)P(x-\xi,\varepsilon)\boldsymbol{d}x$.

La prueba del teorema se basa en la fórmula $\int f\hat{g} = \int \hat{f}g$ a $f$ y a $\Phi(\varepsilon x)e^{2\pi i\langle x|\xi\rangle}$. Resta por notar que los núcleos con los que estamos trabajando, ambos integran a uno. La prueba de estos hechos es un ejercicio.

**Teorema 2.2.6.** *Si $\varphi \in L^1$ con $\int \varphi = 1$ y para $\varepsilon > 0$ definimos $\varphi_\varepsilon(x) = \frac{1}{\varepsilon^d}\varphi\left(\frac{x}{\varepsilon}\right)$, entonces si $f \in L^p \cup \mathcal{C}_0$ para $1 \leqslant p < \infty$, vale que*

$$\|f * \varphi_\varepsilon - f\|_p \to 0, \quad \varepsilon \to 0.$$

*En particular $\int f(\xi)P(x-\xi,\varepsilon)\boldsymbol{d}\xi$ y $\int f(\xi)W(x-\xi,\varepsilon)\boldsymbol{d}\xi$ convergen a $f$ en $L^p$ cuando $\varepsilon \to 0$.*

# Índice Analítico

# Bibliografía

[1] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009.

[2] Joseph H. Silverman, John T. Tate, and Springer-Verlag (Nowy Jork). *Rational Points on Elliptic Curves*. Structure and Bonding. Springer-Verlag, 1992.