Exposición

(Agradecementos).

A clasificación de formas cuadráticas sobre corpos (é dicir de polinomios homoxéneos de grao dous) é un problema fundamental en matemáticas. Cando o corpo base é $\mathbb{R}$, $\mathbb{C}$ ou un corpo finito, a clasificación é completamente elemental. Na memoria tratamos a clasificación sobre o corpo $\mathbb{Q}$ dos números racionais (*Teorema de Hasse-Minkowski*), que é un problema moito máis difícil.

(Índice). Veremos a intuición do problema. Necesaria a construción dos corpos p–ádicos, pois será esencial clasificar previamente sobre $\mathbb{Q}_p$, aparte de sobre $\mathbb{R}$, as formas cuadráticas para finalmente abordar o *Teorema de Hasse-Minkowski*, que nos dá a clasificación sobre $\mathbb{Q}$.

Para analizar o problema que nos propoñemos, veremos como exemplo o comportamento de certas *ecuacións diofánticas*: ecuacións con coeficientes enteiros nas que nos interesamos polas solucións enteiras. As ecuacións diofánticas xogan un papel relevante nas matemáticas xa dende a época de Pitágoras e Diofanto ata hoxe en día con Wiles e Faltings[Th. de Mordel]. No século VI os matemáticos indios xa sabían resolver as ecuacións diofánticas lineais de forma xeral (e de forma parcial xa algo antes na mesma India e na China). O seguinte paso sería, pois, estudar as ecuacións diofánticas cuadráticas.

Consideremos por exemplo a ecuación diofántica

$$x^2 + y^2 = z^2$$

Dita ecuación aparece xa resolta nos *Elementos* de Euclides. Ca nosa linguaxe moderna, podemos resolvela da seguinte forma. Unha solución non trivial $a^2 + b^2 = c^2$ con a, b, c números enteiros proporciona un punto racional $\frac{a}{b}$, $\frac{b}{c}$ da circunferencia $x^2 + y^2 = 1$. Reciprocamente, un punto racional da circunferencia $x^2 + y^2 = 1$ dános (multiplicando por un enteiro para eliminar denominadores) unha solución enteira (e os seus múltiplos) de $x^2 + y^2 = z^2$. Así pois, o problema redúcese a calcular os puntos racionais da circunferencia $x^2 + y^2 = 1$.

Dado a recta r que pasa por $(-1, 0)$ con pendente racional t (é dicir $y = t(x+1)$), o punto P onde a recta corta a circunferencia é racional ($P = (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$).

Reciprocamente, se P é un punto racional da circunferencia distinto de $(-1,0)$, a recta que pasa por $(-1,0)$ e P ten claramente pendente racional. Así pois a aplicación $\mathbb{Q} \ni t \to (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ dános todos os puntos racionais da circunferencia (aparte de $(-1,0)$).

En vez do punto $(-1,0)$ poderiamos elixir calquera outro punto racional (cambiando a recta vertical pola tanxente no punto). Así por exemplo tomando o punto $(1,1)$ da circunferencia $x^2+y^2=2$, por este método calculamos todos os puntos racionais da mesma e así todas as solucións da ecuación diofántica $x^2+y^2=2z^2$. En xeral, se P é un punto racional dunha cónica, e r unha recta que pasa por P (non tanxente) con pendente racional, o outro punto de corte da recta coa cónica é racional, pois os dous puntos de corte dáos unha ecuación cuadrática con coeficientes racionais, e así se un é racional o outro tamén. Por este proceso pódense obter todos os puntos racionais dunha cónica a partir dun dado.

Non obstante, consideremos a circunferencia $x^2+y^2=3$. Atopámonos nunha situación completamente distinta debido a que non ten ningún punto racional (se tivese un, tería infinitos e calcularíanse como antes). Pode verse que non ten ningún eliminando denominadores e observado que a ecuación diofántica $x^2+y^2=3z^2$ non ten solucións non triviais. Isto é fácil de ver pasando a módulo 3.

diapositiva

A terceira circunferencia é entón completamente distinta (a nivel de puntos racionais) ás outras dúas, aínda que en $\mathbb{R}$ parecen todas moi similares como se observa no debuxo. O que ocorre é que $\mathbb{R}$ é só unha das completacións de $\mathbb{Q}$, e para a circunferencia $x^2+y^2=3$ non é a completación axeitada. En $\mathbb{Q}$ hai infinitas métricas (compatibles en certo sentido coa estrutura de corpo), unha para cada número de primo p e outra para o "primo ∞", e en cada un deles podemos completar $\mathbb{Q}$ obtendo o corpo dos números p–ádicos $\mathbb{Q}_p$ e o corpo dos números reais $\mathbb{Q}_\infty = \mathbb{R}$. A circunferencia $x^2+y^2=3$ en $\mathbb{Q}_3$ non ten ningún punto.

As formas cuadráticas racionais en xeral (é dicir, os polinomios homoxéneos

de grao 2 con coeficientes racionais) quedan completamente determinadas se coñecemos o seu comportamento en todas as completacións de $\mathbb{Q}$, é dicir, en cada corpo de números p–ádicos e en $\mathbb{R} = \mathbb{Q}_\infty$. Isto débese ao *Teorema de Hasse-Minkowski*, que é o principal resultado destas notas. E en cada completación, xa sexa $\mathbb{Q}_p$ ou $\mathbb{R}$, temos criterios moi cómodos para clasificar as formas cuadráticas, que tamén estudaremos nestas notas (son criterios en termos de igualdades de dous ou tres invariantes numéricos, para os cales temos fórmulas explícitas e sinxelas para calculalos). O *Teorema de Hasse-Minkowski* é de feito o principal resultado na teoría de formas cuadráticas racionais.

Comezamos as formas cuadráticas cun primeiro capítulo estudando as formas cuadráticas en xeral, sobre un corpo arbitrario. Isto é típico dos primeiros cursos de álxebra lineal cunha motivación xeométrica, poñendo énfase nos corpos $\mathbb{R}$ ou $\mathbb{C}$, con obxecto de estudar métricas nos espazos vectoriais $\mathbb{R}^n$ ou $\mathbb{C}^n$. O noso punto de vista é diferente, pois tamén nos interesa o corpo $\mathbb{Q}$, e por isto teremos que estudar tamén os corpos $\mathbb{Q}_p$ e $\mathbb{Q}_\infty = \mathbb{R}$. Así pois, o primeiro capítulo é un estudo das formas cuadráticas sobre un corpo arbitrario (só evitaremos o caso de corpos de característica 2, que é distinto, xa que todos os corpos que nos imos atopar teñen característica 0).

No segundo capítulo estudaranse os corpos de números p–ádicos. Para definimolos facémolo mediante os enteiros p–ádicos: unha vez profundizado en $\mathbb{Z}_p$, resultará moi cómodo definir os números p–ádicos como o seu corpo de fracción. Así a partir de certas propiedades (as da diapositiva), podemos definir una valoración p–adica que dá lugar a unha métrica en $\mathbb{Z}_p$ a cal se pode estender facilmente a $\mathbb{Q}_p$. Ademais, $\mathbb{Z}_p$ é un anel topolóxico que como anel é un dominio e como espazo topolóxico é de feito un espazo métrico compacto e así completo. A partir de $\mathbb{Z}_p$ é entón máis fácil estudar a estrutura alxébrica e topolóxica de $\mathbb{Q}_p$, que resulta ser a completación de $\mathbb{Q}$ por esta métrica p–ádica, como queriamos probar.

O terceiro capítulo dedícase a introducir diversas ferramentas que necesitamos para estudar as formas cuadráticas sobre os corpos p–ádicos, por exemplo o *símbolo de Legendre* e o *símbolo de Hilbert*

$$diapositiva$$

estudando tamén algunhas das súas principais propiedades. Por exemplo a *Fórmula produto* para o *símbolo de Hilbert*

$$diapositiva$$

que dá un primeiro indicio da utilidade do estudo local (i.e.,para cada primo p) das formas cuadráticas para o seu coñecemento global.

O *símbolo de Hilbert* dos coeficientes dunha forma cuadrática vai xogar un papel destacado para clasificar as formas cuadráticas sobre os corpos p–ádicos, así que é necesario ter unha fórmula sinxela que o calcule, xa que a propia definición non nos dá un cálculo. Así, utilizando teoremas de estrutura obtidos no capítulo 2 sobre o grupo de unidades de $\mathbb{Z}_p$, podemos probar a seguinte fórmula para o *símbolo de Hilbert*

$$diapositiva$$

No capítulo cuarto obtense unha clasificación completa das formas cuadráticas sobre calquera completación de $\mathbb{Q}$. Para o caso de $\mathbb{R}$ o rango e a signatura determinan a forma cuadrática

$$diapositiva$$

No caso dos números p–ádicos obtense

$$diapositiva$$

O último capítulo dedícase a probar o *Teorema de Hasse-Minkowski*

$$diapositiva$$

Durante as demostracións tivemos tamén que estudar que números son representados polas formas cuadráticas:

$$diapositiva$$

O feito de que $a \in \mathbb{Q}_p^*$ estea ou non representado por unha forma cuadrática só depende da súa clase en $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$, así que este resultado determina completamente cando unha forma cuadrática sobre $\mathbb{Q}_p$ representa un número p–ádico.

Estes resultados ás veces poden "levantar" aos números enteiros. Por exemplo, non é díficil deducir do nosos resultados (aínda que non o facemos no traballo) os teoremas de *Gauss* e *Legendre* sobre que enteiros poden poñerse como suma de tres cadrados e como suma de catro cadrados respectivamente (resultados que obviamente son anteriores ao *Teorema de Hasse-Minkowski*).