Técnicas Criptográficas

José Manuel E. Valença *

8 de Junho de 2009

*Departamento de Informática, Universidade do Minho, Campus de Gualtar Braga

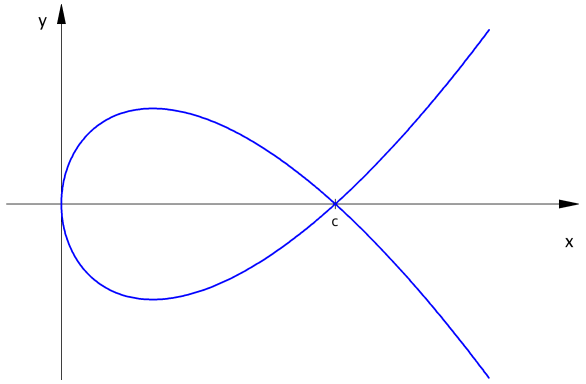
8.Curvas Elípticas

Na procura de grupos cíclicos com as melhores propriedades criptográficas, capazes de aliar garantias de segurança (na perspectiva de dificuldade computacional em resolver os problemas clássicos: DLP, CDHP, BCDHP, etc.) com eficiência de implementação (eficiência na representação e na manipulação computacional), uma área tradicional da Matemática foi "redescoberta": a Geometria Algébrica.

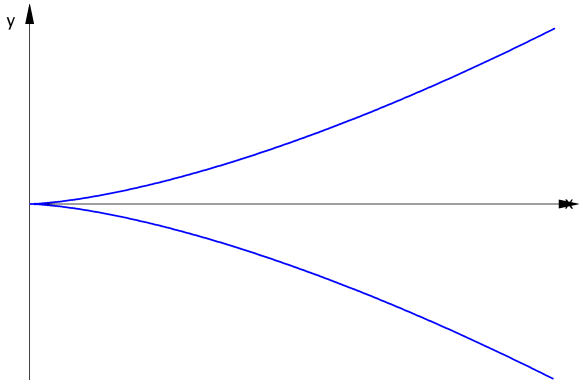
Esta área da Matemática personifica, por um lado, a visão que no século XIX se tinha da Álgebra: o estudos dos polinómios e das sua raízes. Por outro lado dá-lhe a dimensão geométrica e, por isso, estudava essencialmente as curvas definidas em espaços de dimensão real ou racional por equações polinomiais.

Como exemplo considere-se as seguintes curvas definidas no plano $\mathbb{Q}^2$ pelas raízes $\phi(x, y)$ dos polinómios indicados. Note-se que são polinómios a duas variáveis e todos são do 2^o grau em y e do 3^o grau em x.

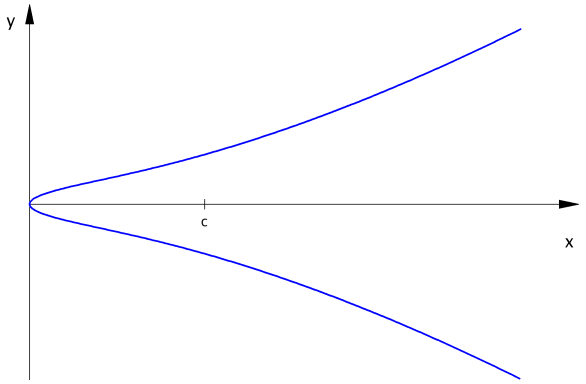
Informalmente, entende-se por *curva* plana racional o conjunto dos pontos $(x, y) \in \mathbb{Q}^2$ para os quais $\phi(x, y) = 0$, i.e, os pontos (x, y) que são *raízes* deste polinómio. Note-se que, ao contrário do que ocorre num polinómio a uma só variável em que as raízes são em número limitado pelo grau do polinómio, para polinómios com mais do que uma variáveis as raízes não estão limitadas pelo grau.



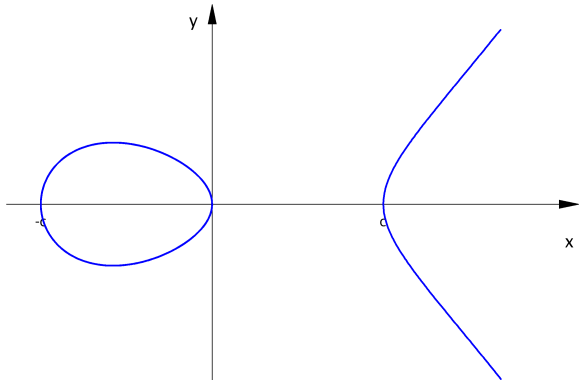
$y^2 - x\,(x-c)^2$



$y^2 - x^3$



$y^2 - x\,(x^2 + c^2)$



$y^2 - x\,(x^2 - c^2)$

Figura 4: Quatro exemplos de curvas planas cúbicas em x e quadráticas em y.

Alguns aspectos importantes que devemos ter em conta:

Estamos habituados a ver este tipo de curvas no plano real $\mathbb{R}^2$; desta forma existem pontos que pertencem à curva no plano real que não estão no plano $\mathbb{Q}^2$. Por exemplo, um ponto de coordenada $x = 1/2$ na curva $y^2 - x(x^2+1)$ tem ordenada $y = \pm\sqrt{5/8}$ que não pertence a $\mathbb{Q}$ (apesar de pertencer a uma extensão algébrica desse corpo). Portanto procurar os pontos em $\mathbb{Q}^2$ da curva $y^2 - x(x^2+1)$, não é uma tarefa trivial.

Na definição de curva, o corpo $\mathbb{Q}$ não tem nada de particular e pode ser substituído por um qualquer outro corpo $\mathbb{K}$. Agora ϕ pertence ao anel dos polinómios a duas variáveis com coeficientes numa extensão de $\mathbb{K}$.

Assim, genericamente, e como primeira definição, pode-se considerar que uma **curva plana** $C/\mathbb{K}$ é o conjunto das raízes em $\mathbb{K}^2$ de um polinómio $\phi \in \mathbb{K}[x, y]$.

Para evidenciar a relação entre a curva, o corpo de suporte e o polinómio, representamos a curva por $C/\mathbb{K}: \phi$.

Note-se que os coeficientes do polinómio estão numa extensão do corpo $\mathbb{K}$ mas não necessariamente em $\mathbb{K}$. Isto faz com que não seja suficiente escolher uma coordenada $x \in \mathbb{K}$ para existir um $y \in \mathbb{K}$ tal que $\phi(x, y) = 0$. De facto pode até acontecer que o polinómio $\phi(x, y)$ não tenha qualquer raiz em $\mathbb{K}^2$

Por exemplo, considere-se um polinómio com coeficientes em $\mathbb{C}$, $\phi(x, y) = i\,y - x - i$ (sendo i a unidade imaginária, $i^2 + 1 = 0$). A curva em $\mathbb{Q}$ definida por este polinómio é formada por um só ponto $\{(0, 1)\}$.

A procura dos pontos de uma curva é, portanto, um processo essencial e, para isso. pode-se recorrer a algumas "heurísticas". Por exemplo, quando o corpo $\mathbb{K}$ é finito, a curva é também um conjunto finito uma vez que o número de raízes de $\phi(x,y)$ em $\mathbb{K}$ está limitado pelo número de pontos disponíveis no plano $\mathbb{K}^2$. De facto, se $\mathbb{K} \equiv \mathbb{F}_q$ for o corpo finito de q elementos, o plano $\mathbb{K}^2$ tem exactamente q^2 possíveis pontos.

Assim é possível, em princípio, encontrar a curva C percorrendo sistematicamente todos $(x,y) \in \mathbb{K}$ e testando, para cada ponto, se verifica $\phi(x,y) = 0$. Obviamente, este procedimento só será computacionalmente viável se q^2 for razoavelmente pequeno.

Algumas formas particulares de polinómio facilitam a construção da curva. Por exemplo, uma classe de curvas importante é a formada pelas *rectas*. No plano $\mathbb{K}^2$ uma **recta** é definida por um polinómio de primeiro grau $l \in \overline{\mathbb{K}}[x,y]$, com $l(x,y) = a\,y + b\,x + c$ sendo $a,b,c \in \overline{\mathbb{K}}$ e $(a \neq 0) \vee (b \neq 0)$.

A curva $C\colon l(x,y)$ goza de uma propriedade muito importante: se tiver dois pontos distintos $P,Q \in \mathbb{K}^2$, com $P = (x_1,y_1)$ e $Q = (x_2,y_2)$, então qualquer $x \in \mathbb{K}$, distinto de x_1 e x_2, ou qualquer $y \in \mathbb{K}$ distinto de y_1 ou y_2, determinam um terceiro ponto $(x,y) \in \mathbb{K}^2$ na mesma curva [64].

[64] Passando a recta pelos pontos $(x,y),(x_1,y_1)$ e (x_2,y_2), tem de se verificar $a\,(y_2-y_1) + b\,(x_2-x_1) = 0$ e $a\,(y-y_1) + b\,(x-x_1) = 0$. Se for $a = 0$ tem-se $x = x_1 = x_2 \in \mathbb{K}$; todo $y \in \mathbb{K}$ determina um ponto em $\mathbb{K}^2$. Se for $a \neq 0$, verifica-se $(y-y_1) = (y_2-y_1)\,(x-x_1)/(x_2-x_1)$; todo $x \in \mathbb{K}$ determina um ponto em $\mathbb{K}^2$.

Quando as rectas se sobrepõem com outras curvas, definidas por polinómios de grau mais elevado, esta propriedade permite dizer
Considere-se, por exemplo, a curva $C\colon y^2 - x^3 - 1$ e a recta $L\colon y - x - 3/4$ representadas na figura 5. Queremos ver que curvas definem em $\mathbb{Q}$; nomeadamente queremos determinar as raízes racionais de $y^2 - x^3 - 1$.

A recta intersecta a curva C em 3 pontos; pela propriedade das rectas, se dois deles tiverem coordenadas racionais o terceiro também tem coordenadas racionais.

Isto sugere um mecanismo para construção de C. Se forem já conhecidos dois pontos de coordenadas racionais em C, traça-se a recta que eles determinam e calcula-se o terceiro ponto de intersecção com a curva. Esse ponto, porque está na recta, também tem coordenadas racionais desde que uma das coordenadas seja racional.

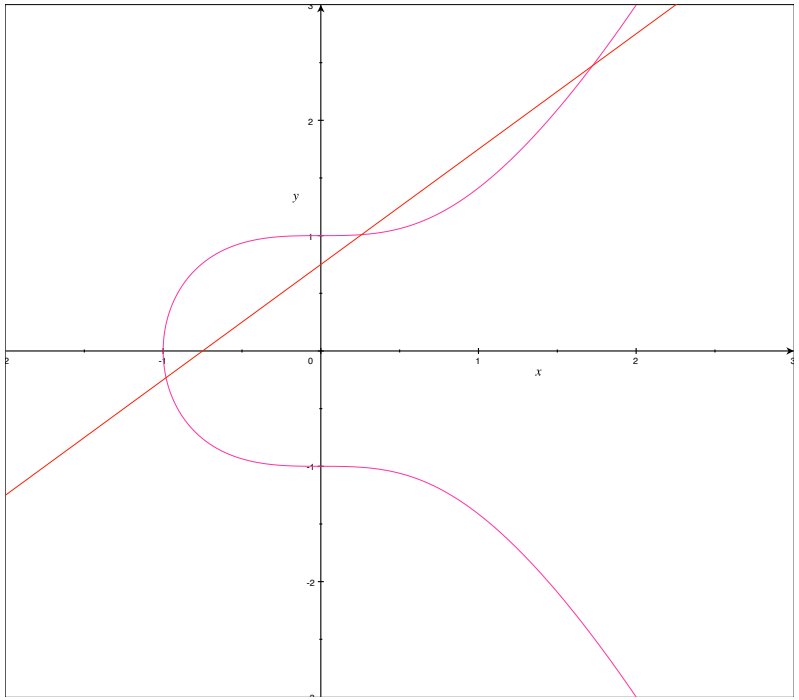


Figura 5: Curvas $y^2 - x^3 - 1$ e $y - x - 3/4$.

Na viabilidade deste mecanismo reside a razão porque se usam este tipo de curvas em Criptografia.

Intersecção de rectas com curvas cúbicas em $\mathbb{Q}$

Considere-se, por exemplo, uma curva cúbica definida pelos pontos $(x, y) \in \mathbb{C}^2$ que verificam a equação

$$y^2 + (a_1\, x + a_3)\, y \;=\; x^3 + a_2\, x^2 + a_4\, x + a_6 \qquad \text{com} \quad a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q} \tag{129}$$

e procuremos determinar os pares (x, y) que pertencem a $\mathbb{Q}^2$.

Para iniciar este procedimento é necessário ter, pelo menos, dois pontos de coordenadas racionais (que podem não ser distintos). Agora a construção de um terceiro ponto a partir de dois outros pontos, $P = (x_1, y_1)$ e $Q = (x_2, y_2)$, passa pela determinação da recta que eles definem e, depois, pelo cálculo da intersecção dessa recta com a curva. Vamos descrever o mecanismo que permite calcular as coordenadas (x_3, y_3), em função das cordenadas de P e Q, do terceiro ponto R de intersecção da recta com a curva.

Se a recta é vertical, que se traduz por ser $x_1 = x_2 \wedge y_1 = -y_2$, o terceiro ponto de intersecção é um ponto especial, designado por *ponto no infinito* e representado por P_∞, que estudaremos na próxima secção.

Quando a recta não é vertical existem parâmetros a determinar $\lambda, \mu \in \mathbb{C}$ tais que todo o ponto (x, y), sobre recta, verifica $y = \mu + \lambda\, x$. Como os três pontos P, Q, R estão sobre a recta, tem-se

$$y_i \;=\; \mu + \lambda\, x_i \qquad \text{para} \quad i = 1, 2, 3 \tag{130}$$

Efectuando a substituição $y \longrightarrow \mu + \lambda\, x$ em (129) obtém-se

$$(\mu + \lambda\, x)^2 + (a_1\, x + a_3)\,(\mu + \lambda\, x) = x^3 + a_2\, x^2 + a_4\, x + a_6$$

Expandindo e agrupando os termos obtém-se

$$x^3 - (\lambda^2 + a_1\, \lambda - a_2)\, x^2 + \ldots \textit{monómios de ordem inferior} \;=\; 0$$

As três soluções desta equação são três ordenadas x_1, x_2, x_3 dos três pontos de intersecção da recta com a curva. Portanto esta mesma equação pode-se também escrever como $(x - x_1)\,(x - x_2)\,(x - x_3) \;=\; 0$. Dado que

$$(x - x_1)\,(x - x_2)\,(x - x_3) \;=\; x^3 - (x_1 + x_2 + x_3)\, x^2 + \ldots \textit{monómios de ordem inferior}$$

conclui-se

$$\lambda^2 + a_1\, \lambda - a_2 \;=\; x_1 + x_2 + x_3 \tag{131}$$

Uma vez que x_1 e x_2 são conhecidos, se λ for conhecido a equação (131) determina x_3. Além disso, sendo λ e x_3 conhecidos, as equações (130) determinam $y_3 = y_1 + \lambda\,(x_3 - x_1)$.

Para determinar λ temos duas situações possíveis:

$P \neq Q$

Sendo $(x_1, y_1) \neq (x_2, y_2)$, e sendo a recta não vertical (o que implica $x_1 \neq x_2$), então as equações (130) conduzem a

$$\lambda = (y_2 - y_1)/(x_2 - x_1) \tag{132}$$

$P = Q$

Neste caso a recta é tangente à curva no ponto (x_1, y_1); portanto λ é o declive da tangente nesse ponto; isto é, $\lambda = [\partial y/\partial x]\,(x_1, y_1)$. Derivando em ordem a x a equação (129), tem-se

$$(2\,y + a_1\,x + a_3)\;(\partial y/\partial x) + a_1\,y = 3\,x^2 + 2\,a_2\,x + a_4$$

Calculando esta derivada no ponto P, conclui-se

$$\lambda \;=\; (3\,x_1^2 + 2\,a_2\,x_1 - a_1\,y_1 + a_4)/(2\,y_1 + a_1\,x_1 + a_3) \tag{133}$$

Através de (132) (quando $P \neq Q$) ou através de (133) (quando $P = Q$) determinamos o parâmetros λ de uma recta não vertical que seja definida pelos dois pontos. Com (131) determinamos

$$x_3 \;=\; \lambda^2 + a_1\,\lambda - a_2 - x_1 - x_2 \qquad , \qquad y_3 \;=\; y_1 + \lambda\,(x_3 - x_1) \tag{134}$$

Estas relações definem o mecanismo computacional que, dados dois pontos racionais P e Q da curva em (129) determina um terceiro ponto racional R que é *colinear* com os dois pontos anteriores.

Note-se que, apesar de um ponto genérico $X = (x, y)$ que verifique a equação (131) ter coordenadas complexas, o mecanismo que acabámos de apresentar assegura que, sendo $P = (x_1, y_1)$ e $Q = (x_2, y_2)$ pontos de coordenadas racionais, o ponto $R = (x_3, y_3)$ também tem coordenadas racionais. De facto os parâmetros λ e μ calculados por (132) ou (133) são racionais e, desta forma, x_3 e y_3, calculados por (134), são necessariamante racionais.

O mecanismo de **colinearidade** determina uma relação ternária entre o três pontos de tal forma que, dados dois deles, é sempre possível calcular o terceiro. Por motivos que serão claros em seguida, vamos escrever essa relação da forma seguinte

$$P \oplus Q \oplus R = P_\infty$$

Para já não vamos dar significado especial ao símbolo "$\oplus$" (que será visto, apenas, como um separador de argumentos) e vamos interpretar "$\cdot = P_\infty$" apenas como um símbolo de predicado ternário. A notação apenas significa que os três pontos são colineares.

Se este fosse o único mecanismo para gerar pontos estaríamos bastante limitados já que, com os três pontos iniciais, o mecanismo permitiria gerar apenas dois pontos adicionais: o ponto $(2, 3)$, que é colinear com os pontos $P = (-1, 0)$ e $S = (0, 1)$, e o ponto $(2, -3)$ colinear com os pontos $(-1, 0)$ e $(0, -1)$.

Por isso são necessários outros mecanismos com esta função. O primeiro deles é óbvio: uma curva que seja definida por um polinómio onde o único termo em y tem grau 2 (um polinómio da forma $y^2 + f(x)$) então se $X = (x, y)$ é raiz do polinómio, também o ponto $(x, -y)$ é raiz do mesmo polinómio. Representamos este ponto por $-X$.

Temos agora uma nova transformação que mapeia pontos racionais da curva noutros pontos racionais da mesma curva: a aplicação $X \mapsto -X$ mapeia o ponto racional (x, y) no ponto racional $(x, -y)$. Esta aplicação designa-se por **simetria**.

O mecanismo da colinearidade parte do princípio que uma recta $y - \mu - \lambda\, x$ contém exactamente 3 pontos da curva $y^2 - x^3 - 1$. A figura 6 ilustra um conjunto de rectas que parecem contrariar esta assumpção.

A recta $y - 2\, x + 1$, que contém R e $-Q$ só parece conter estes dois pontos. A recta horizontal $y = 0$, que contém Q, não contém qualquer outro ponto da curva.

Por outro lado, a recta horizontal $y = 0$ (que passa por P) e as rectas verticais $x = 2$ (que passa por R e $-R$), $x = 0$ (que passa por Q e $-Q$) e $x = -1$ (que passa só por P) parecem conter exclusivamente os pontos indicados.

Tudo depende, porém, da forma como entendemos a noção de "ponto da curva" e como contamos esses pontos.

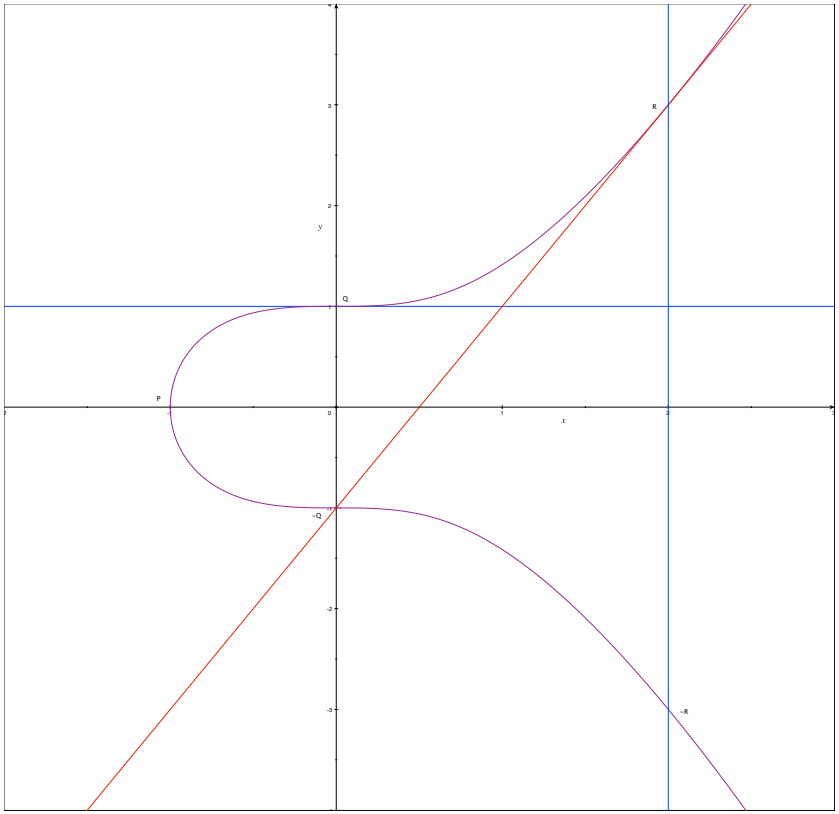


Figura 6: Ponto no infinito na curva $y^2 - x^3 - 1$.

Os pontos comuns a uma recta não-vertical $y + \lambda\, x + \mu = 0$ e à curva $y^2 - 1 - x^3 = 0$ são soluções deste sistema de equações. Substituindo a 1ª equação na segunda obtém-se

$$x^3 - \lambda^2\, x^2 - 2\,\lambda\,\mu\, x - \mu^2 + 1 \;=\; 0 \tag{135}$$

Este polinómio de 3º grau em x tem, no fecho algébrico de $\mathbb{Q}$ (i.e. os complexos $\mathbb{C}$), exactamente 3 raízes distintas. Pode ter uma raiz dupla quando a 1ª derivada também se anula nesse ponto, ou até uma raiz tripla se a 2ª derivada também se anular no mesmo ponto.

Raízes racionais múltiplas do polinómio dão origem a pontos onde a recta é tangente à curva. Quando a raiz é dupla (como no ponto $R = (2, 3)$ para a recta que também passa pelo ponto $-Q = (0, -1)$) interpretamos isso como se a recta intersecta-se duas vezes a curva nesse ponto. A relação de colinearidade deve, neste caso, escrever-se

$$(-Q) \;\oplus\; R \;\oplus\; R \;=\; P_\infty$$

A recta horizontal $y - 1 = 0$ (definida por $\lambda = 0$ e $\mu = -1$) dá origem a um polinómio muito simples; o polinómio (135) reduz-se a x^3 que tem uma raiz tripla no ponto $x = 0$. Neste caso a recta "intersecta" a curva 3 vezes no ponto $Q = (0, 1)$; a relação de colinearidade será, aqui,

$$Q \;\oplus\; Q \;\oplus\; Q \;=\; P_\infty$$

Outra situação deriva da existência de raízes complexas de (135). Por exemplo, a recta horizontal $y = 0$ (definida por $\lambda = \mu = 0$) conduz ao polinómio $x^3 + 1$ que tem uma raiz racional $x_1 = -1$ e duas raízes complexas

$x_2 = -\zeta$ e $x_3 = -\zeta^2$, em que $\zeta \neq 1$ é uma raíz cúbica da unidade[65]. A figura 6 indica apenas o ponto de intersecção $P = (-1, 0)$ definido pela raíz racional; os pontos de intersecção definidos pelas duas raízes complexas, $(-\zeta, 0)$ e $(-\zeta^2, 0)$, não são, aqui, representáveis.

Uma situação distinta ocorre com rectas verticais; tais rectas não podem ser descritas pelo polinómio $y + \lambda\, x + \mu$ [66] mas são descritas, simplesmente, por um polinómio da forma $x - \mu$. Os eventuais pontos racionais comuns à recta e à curva são determinados pelas possíveis raízes quadradas racionais de $1 + \mu^3$ com $\mu \in \mathbb{Q}$. Isto é, serão pontos da forma $(\mu, \pm\sqrt{1 + \mu^3})$ caso μ seja racional e a ráiz quadrada também seja racional.

Portanto uma recta vertical contém, quanto muito, duas raízes racionais do polinómio $y^2 - x^3 - 1$. No entanto, se acrescentar-mos ao conjunto de raízes um ponto extra por onde passam, por definição, todas as rectas verticais, resolve-mos a questão de ter sempre a propriedade da colinearidade estabelecida em triplos de pontos da curva.

Para justificar a introdução do **ponto no infinito** temos de recorrer a algum formalismo de Geometria Algébrica, o que faremos na próxima secção.

Vamos aceitar, para já, que um tal ponto existe, que é representado por P_∞ e por ele passam todas as rectas verticais. Nessa perspectiva a nossa curva vai ser constituída por duas componentes: a primeira é formada pela

[65] As raízes cúbicas complexas da unidade ζ são as raízes em $\mathbb{C}$ do polinómio $X^2 + X + 1$.

[66] Teria que ser $\lambda = \infty$.

raízes racionais do polinómio $\phi(x,y) = y^2 - x^3 - 1$, e se designa-se por "componente afim", e uma segunda componente formada exclusivamente pelo ponto P_∞.

Com esta definição de curva podemos verificar que, pelo menos para este exemplo, duas propriedades importantes:

1. Cada recta intersecta a curva em exatamente 3 pontos, desde que cada ponto conte tantas vezes quantas a respectiva multiplicidade e se entre em conta com o ponto no infinito P_∞ e pontos de coordendas complexas.
2. Cada recta (mesmo que seja vertical), se passa por dois pontos da curva de coordenadas racionais, passa sempre por um terceiro ponto de coordenadas racionais na mesma curva.

Por exemplo, a recta $x = 0$ passa pelos pontos $Q = (0,1)$ e $-Q = (0,-1)$; como é uma recta vertical passa também pelo ponto no infinito P_∞. A colinearidade exprime-se, aqui, por

$$Q \oplus (-Q) \oplus P_\infty = P_\infty$$

A recta vertical $x = -1$ é tangente à curva no ponto $P = (-1,0)$; passa, portanto, duas vezes por esse ponto. Como é vertical passa por P_∞; por isso a colinearidade é

$$P \oplus P \oplus P_\infty = P_\infty$$

8.1 Curvas Planas

A formalização do conceito de curva plana requer algumas noções elementares de Geometria Algébrica. Para não correrrmos o risco de enveredar-mos de forma excessiva por uma área da Matemática que, apesar de ser extremamente rica e interessante, tem objectivos que ultrapassam em muito o âmbito deste curso, vamos impor algumas limitações a esse estudo.

Assim, neste curso, vamos entender como "curvas planas" as curvas definidas no espaço bidimensional-dimensional pelas raízes de um polinómio a duas variáveis. Serão apenas estas o objecto do nosso estudo. Procuraremos, desta forma, evitar as complexidades de derivam do estudo das variedades algébricas. Procuraremos também, sempre que possível, usar o chamado sistema de coordenadas afins $\mathbb{A}^2$ e evitar um estudo detalhado de curvas em espaços projectivos.

Essencial ao nosso estudo é não impor limitações ao corpo $\mathbb{K}$ onde vão estar definidas as curvas. Apesar de as intuições geométricas serem mais óbvias em curvas definidas no plano real $\mathbb{R}^2$, não nos podemos esquecer que o nosso objectivo é estudar curvas com interesse criptográfico e isso implica, normalmente, usar outro tipo de corpos, nomeadamente corpos finitos. Como um polinómio de coeficientes no corpo $\mathbb{K}$ tem raízes no seu fecho algébrico $\overline{\mathbb{K}}$, é conveniente pensar, desde o início, em polinómios cujos coeficientes pertencem também a $\overline{\mathbb{K}}$.

Tomemos, então, um corpo $\mathbb{K}$ e $\overline{\mathbb{K}}[x, y]$ o anel dos polinómios a duas variáveis com coeficientes no fecho algébrico $\overline{\mathbb{K}}$ de $\mathbb{K}$. O conjunto dos polinómios $\overline{\mathbb{K}}[x, y]$ tem a estrutura algébrica de um anel. De facto estes polinómios têm

uma estrutura algébrica ainda mais rica: é também um **domínio de factorização única**; isto é, cada elemento do anel pode ser decomposto (de forma única a menos da ordem dos factores) no produto de um número finito de elementos irredutíveis.

□

Curvas planas são conjuntos de pontos que são, de alguma forma, "raízes" de um polinómio irredutível ϕ. Existem dois sistemas possíveis de representar estes pontos: em **coordenadas afins** ou em **coordenadas projectivas**.

Coordenadas Afins

Cada curva é determinada por um polinómio a duas variáveis $\phi(x, y)$ que é irredutível em $\overline{\mathbb{K}}[x, y]$.

Note-se que os coeficientes dos polinómios são elementos do fecho algébrico do corpo $\mathbb{K}$. Note-se também que um polinómio irredutível em $\mathbb{K}[x, y]$ pode não ser irredutível em $\overline{\mathbb{K}}[x, y]$.

Por exemplo, o polinómio $x^2 + 2y^2$ é irredutível em $\mathbb{Q}[x, y]$ mas não é irredutível no anel de polinómios sobre o fecho algébrico. De facto tem-se $(x^2 + 2\,y^2) = (x - i\,\sqrt{2}\,y)\,(x + i\,\sqrt{2}\,y)$ em $\mathbb{C}[x, y]$. Por isso $x^2 + 2\,y^2$ não define uma curva plana no espaço $\mathbb{Q}^2$.

Cada par $(a, b) \in \overline{\mathbb{K}}^2$ determina um ponto P em coordenadas afins. Cada polinómio ϕ mapeia pontos $P \in \overline{\mathbb{K}}^2$ em elementos de $\bar{\mathbb{K}}$ definindo $\phi(P)$ como $\phi(a, b)$. O ponto $P = (a, b) \in \overline{\mathbb{K}}^2$ é **raiz** de ϕ quando $\phi(P) = 0$.

Um polinómio da forma $(x-a)^i\,(y-b)^j$ é um **factor local** em P. O polinómio ϕ é **m-factorizável em P**, se é divisível por um factor local em P de grau m.

193 PROPOSIÇÃO
*Para toda a raíz P de ϕ, existem um inteiro $m \geq 1$ e uma decomposição $\phi = \phi_1 + \cdots + \phi_l$ em que todos os polinómios ϕ_i são m-factorizáveis em P. O maior de tais m designa-se por **multiplicidade** de ϕ em P e representa-se por $\eta_P(\phi)$.*

Este resultado é um corolário de um importante teorema da Álgebra, o Nullstellensatz, que estudaremos com um pouco mais detalhe na secção seguinte.

Note-se que não se exige que todos os polinómios ϕ_i, na decomposição de ϕ, tenham o mesmo factor de grau m. O que tem de ser comum a todas as componentes é o grau do factor e não o próprio factor.

EXEMPLO 39: Considere-se a origem $P = (0,0)$; um factor local em P de grau m é um polinómio da forma $x^i\,y^j$, com $i+j=m$.

Considere-se também o polinómio $\phi = 2\,x\,y + x^3$; obviamente que P é raiz de ϕ. O polinómio é a soma de duas componentes, $2\,x\,y$ e x^3 , ambas 2-factorizáveis em P. A primeira componente tem o factor local $x\,y$; a segunda tem o factor local x^2. Os factores locais em P são distintos, mas ambos têm grau 2.

Qualquer das componentes tem outros factores locais em P: ambas têm factores de grau 1 e a componente x^3 tem um factor de grau 3. Porém o grau 2 é o maior grau que é comum a factores locais em P de ambas as componentes.

Os polinómios x, y e $x+y$ têm todos uma raíz em P de multiplicidade 1. Isto é, $\eta_P(x) = \eta_P(y) = \eta_P(x+y) = 1$. Tem-se $\eta_P(x^2) = \eta_P(y^2) = \eta_P(x\,y) = 2$. Somando um polinómio de multiplicidade 1 com um de multiplicidade 2 (por exemplo, $x + x\,y$) obtém-se um polinómio de multiplicidade 1 em P. O polinómio $2\,x\,y + x^3$ tem, como vimos no exemplo 39, multiplicidade 2 em P.

Como resultado imediato da proposição 193 tem-se

194 TEOREMA
Para toda a raíz P de ϕ, existem polinómios p_{ij}, em que $p_{ij} \neq 0$ implica $p_{ij}(P) \neq 0$, tais que

$$\phi(x,y) \quad = \sum_{i+j=\eta_P(\phi)} (x-a)^i\,(y-b)^j\,p_{ij}(x,y) \tag{136}$$

Se $\eta_P(\phi) > 1$, os polinómios $\partial\phi/\partial x(x,y)$ e $\partial\phi/\partial y$ têm em P uma raíz de multiplicidade $\eta_P(\phi) - 1$. Consequentemente verifica-se $\eta_P(\phi) = 1$ se e só se $\partial\phi/\partial x(P) \neq 0$ e $\partial\phi/\partial y(P) \neq 0$.

A decomposição em (136) pode ser generalizada para polinómios com qualquer número finito de variáveis e, desta forma, pode-se estender a definição de multiplicidade de raíz (proposição 193) para este tipo de polinómios. Por exemplo, se for $\phi \in \mathbb{K}[x,y,z]$ e $P = (a,b,c)$ uma raíz de ϕ em $\mathbb{K}^3$, o polinómio decompõe em $\phi(x,y,z) = \sum_{i+j+k=m} (x-a)^i\,(y-b)^j\,(z-c)^k\,p_{ijk}(x,y,z)$; a multiplicidade de ϕ em P é o maior m para o qual existe esta decomposição de ϕ.

□

Nem todos os pontos das curvas são definidos por pares $(a, b) \in \overline{\mathbb{K}}^2$. Nomeadamente o comportamento assimptotico de curvas é expresso pela existência dos chamados "pontos no infinito".

Considere-se o caso simples das rectas; sabemos que uma recta no plano pode ser determinada por dois pontos distintos ou, em alternativa, por um ponto e um declive ("direcção"). Numa recta o declive pode ser infinito (se a recta for vertical) ou então, sendo finito, é um elemento de $\overline{\mathbb{K}}$.

O polinómio para uma recta que passe pelos pontos (a, b) e (a', b') é $(x - a)(b - b') - (y - b)(a - a')$. O polinómio para a recta que passa pelo ponto (a, b) tem declive μ, exige um pouco mais cuidado: se o declive for infinito (recta vertical) o polinómio é $(x - a)$; se μ for finito, o polinómio é $\mu(x - a) - (y - b)$.

Idealmente deveríamos ter apenas uma situação: uma recta é definida por dois pontos. Para isso, e para tentar unificar estas três situações, os matemáticos do século XVII introduziram a noção de **pontos no infinito**.

Nesta perspectiva cada declive μ (finito ou infinito) introduz um ponto no infinito P_μ; diz-se que uma recta passa pelo ponto P_μ se e só se tem declive μ. Uma curva C passa pelo ponto P_μ se tem uma assimptota com declive μ.

A unificação completa destas representações e um sistema de pontos que contenha os pontos no infinito só pode ser feito recorrendo às coordenadas projectivas. No entanto, mesmo nas coordenadas afins, interessa-nos ver o papel dos pontos no infinito na caractarização do comportamento assimptótico de curvas.

195 NOÇÃO

A **homogenização** *de* $\phi \in \mathbb{K}[x,y]$ *com grau total* d*, é o polinómio* $\phi_h \in \mathbb{K}[x,y,z]$ *tal que*

$$\phi_h(x,y,z)/z^d \;=\; \phi(x/z, y/z) \tag{137}$$

Diz-se que $\phi(x,y)$ *tem uma raiz de multiplicidade* m *em* P_∞ *quando* $\phi_h(z,y,z)$*, tem uma raiz de multiplicidade* m *em* $(0,1,0)$*; identicamente, para* μ *finito, diz-se que* ϕ *tem uma raiz de multiplicidade* m *em* P_μ *quando* $(1,\mu,0)$ *for uma raiz de multiplicidade* m *de* $\phi_h(z,y,z)$*.*

Tento em atenção que $\phi(x,y) = \phi_h(x,y,1)$, constata-se que as raizes (x,y) de ϕ são precisamente as raízes de ϕ_h da forma $(x,y,1)$. Portanto ϕ_h captura não só todas as raízes afins de ϕ como também as raízes no infinito. Este incremento em representatividade tem, obviamente, um custo: a variável adicional z. Para ϕ, as raízes procuram-se num espaço a duas dimensões; ao invés as raízes de ϕ_h procuram-se num espaço a três dimensões.

EXEMPLO 40:

1. Uma recta $\phi = a\,x + b\,y + c$ homogeniza em $\phi_h = z\,(a\,x/z + b\,y/z + c) = a\,x + b\,y + c\,z$. Temos $\phi_h(0,1,0) = b$ e $\phi_h(1,\mu,0) = a + b\,\mu$. Portanto P_∞ é raíz da recta se e só se $b = 0$; i.e., se a recta é vertical e passa pelo ponto $x = -c/a$. Se $b \neq 0$, P_μ é raíz da recta se for $\mu = -a/b$.
2. O polinómio $\phi = y^2 + x^3 + x\,y + 1$ tem grau total é 3 e a sua homogenização é

$$\phi_h \;=\; z^3\,((y/z)^2 + (x/z)^3 + (x/z)\,(y/z) + 1) \;=\; y^2\,z + x^3 + x\,y\,z + z^3$$

Tem-se $\phi_h(0,1,0) = 0$ e $\phi_h(1,\mu,0) = 1$; portanto ϕ tem P_∞ como raíz de ϕ mas nenhum P_μ, com μ finito, é raíz.

Não é possível construir ϕ_h como uma soma de múltiplos de monómios $x^i\,(y-1)^j\,z^k$ cujo grau total $i+j+k$ seja 2 ou superior; assim a multiplicidade da raíz P_∞ é, apenas, 1.

3. Considere-se finalmente $\phi = x^2\,y + x$ cujo grau total é 3 e tem homogenização $\phi_h = x^2\,y + x\,z^2$. Tem-se $\phi_h(0,1,0) = 0$ e $\phi_h(1,\mu,0) = \mu$. Portanto P_∞ e P_0 são ambas raízes no infinito de ϕ.

   Claramente, a multiplicidade de ϕ_h é 2 em $(0,1,0)$ (atente-se à forma $\phi_h = x^2\,p + z^2\,q$, com $p = y$ e $q = x$) e é 1 em $(1,0,0)$ (atente-se à forma $\phi_h = (x-1)\,p + y + z\,q$, com $p = (x+1)\,y$ e $q = x\,z$).

196 NOÇÃO

A **curva plana** *em* $\mathbb{A}^2$, *definida por um polinómio* $\phi \in \mathbb{K}[x,y]$ *que é irredutível em* $\overline{\mathbb{K}}\,[x,y]$, *é o conjunto formado pelas raízes afins ou no infinito de* ϕ. *Um* **ponto singular** *é uma raíz de* ϕ *com multiplicidade* > 1. *A curva diz-se* **não-singular** *se não contém pontos singulares. Se* K *é uma qualquer extensão de* $\mathbb{K}$, *os pontos* K-**racionais** *da curva são os pontos afins de coordenadas* $(x,y) \in K^2$.

Notas

1. **Curvas Triviais**

   Os polinómios 1 e 0 são ambos irredutíveis e definem duas "curvas" triviais. O polinómio 1 não tem qualquer raíz; por isso, a "curva" é o conjunto vazio de pontos $\emptyset$. O polinómio 0, ao invés, tem como raizes qualquer ponto $(x,y) \in \overline{\mathbb{K}}^2$ e qualquer ponto no infinito; é o espaço total que representamos por $\mathbb{P}^2$.

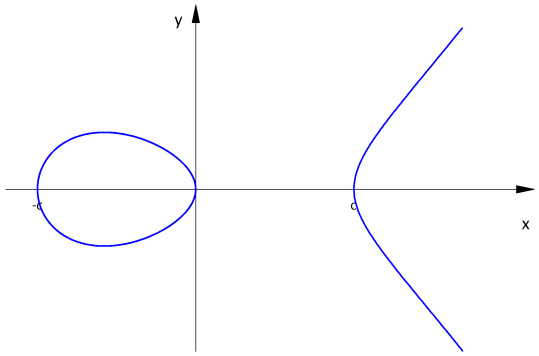
2. **Pontos Singulares**

   Para detectar pontos singulares pode-se usar o teorema 194 e o critério das derivadas parciais.

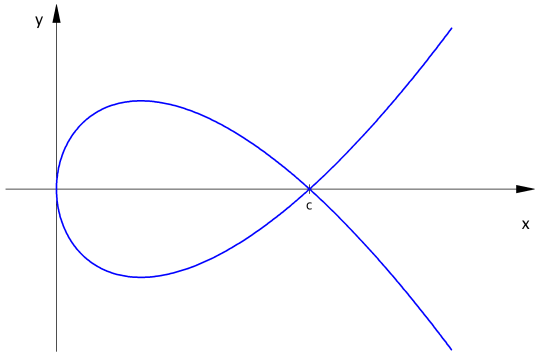
   Por exemplo, cúbica $\phi = y^2 - x\,(x^2-1)$ define uma curva plana formada por todos os pontos (x,y) que são raízes deste polinómio e ainda pelo ponto P_∞ já que, se verifica facilmente, o polinómio tem essa raiz no infinito.

Note-se que $\partial\phi/\partial x = 1 - 3\,x^2$ e $\partial\phi/\partial y = 2\,y$; os únicos pontos que são raízes de ambas as derivadas são $(\pm\sqrt{1/3}, 0)$. Porém nenhum destes pontos pertence à curva; por isso ela é não-singular.

Já o polinómio $\phi' = y^2 - x\,(x-1)^2$ tem derivadas parciais $\partial\phi'/\partial y = 2\,y$ e $\partial\phi'/\partial x = (x-1)\,(1-3\,x)$. As raízes comuns a ambas estes dois polinómios são os pontos $(1,0)$ e $(1/3,0)$. Note-se que $(1,0)$ é um ponto da curva; por isso ela é singular.



$y^2 - x\,(x^2-1)$



$y^2 - x\,(x-1)^2$

3. **Pontos Racionais**

É preciso ter em conta que as raízes afins de $\phi \in \mathbb{K}[x,y]$ podem ter coordenadas fora do corpo $\mathbb{K}$. Tome-se, por exemplo, $\mathbb{K} \equiv \mathbb{Q}$ e considere-se $\phi = y^2 - x^3 - 1$. Genericamente as raízes afins de ϕ têm coordendas complexas, uma vez que $\overline{\mathbb{Q}} \equiv \mathbb{C}$.

Fixe-se um racional qualquer b e procure-se pontos afins da curva da forma (a,b). O valor de a tem de ser raíz do polinómio $x^3 - (b^2-1)$. Se for $b^2 \neq 1$ existem três raízes distintas deste polinómio: um valor algébrico, $a = \sqrt[3]{b^2-1}$, e dois valores complexos $a\,\zeta$ e $a\,\zeta^2$, sendo ζ uma raíz cúbica complexa da unidade. Se for $b^2 = 1$ o polinómio tem uma raíz tripla em 0. A menos deste último caso, as raízes de ϕ da forma (a,b), com b racional, muito provavelmente não têm uma cordenada a que seja racional: duas são complexas e uma é algébrica, provavelmente irracional.

Existem, no entanto, raízes racionais do polinómio $x^3 - (b^2-1)$, para determinados valores de b. Por exemplo, para $b = 0$, temos

uma raíz racional $a = -1$; para $b = 3$ temos a raíz $a = 2$, etc. Estes pontos, $(-1, 0), (2, 3)$, etc, são pontos racionais da curva.

Seja C a curva plana determinada pelo polinómio ϕ; esse facto denota-se por $C : \phi$. Uma maneira de interpretar a curva C é através do conjunto formado por todos os polinómios que se anulam em todos $P \in C$.

$$\mathbf{I}(C) \;=\; \{\, f \in \overline{\mathbb{K}}\,[x, y] \;\mid\; f(P) = 0 \quad \text{para todo} \quad P \in C \,\} \tag{138}$$

É fácil verificar que o conjunto $\mathbf{I}(C)$ é um ideal; isto é, é fechado por somas e por multiplicação por um qualquer polinómio. O facto de ϕ ser irredutível em $\overline{\mathbb{K}}\,[x, y]$ assegura que o ideal é primo; isto é, se $f \cdot g$ pertence ao ideal, um dos polinómios f ou g tem de pertencer ao ideal. Veremos adiante (ver noção 215, página 493) uma exposição sucinta da noção de ideal e suas aplicações à Teoria das Curvas.

O anel quociente $\overline{\mathbb{K}}\,[x, y]/\mathbf{I}(C)$ identifica como equivalentes dois polinómios que são iguais em todos os pontos da curva; isto é, $p \sim q$ sse $p - q \in \mathbf{I}(C)$ ou, equivalentemente, sse $p(P) = q(P)$ para todo $P \in C$. Este anel representa-se por $\mathbb{A}(C)$ e designa-se por **anel afim** ou **anel de coordenadas** da curva C.

As noções de m-factorização e multiplicidade podem ser estendidas a

197 NOÇÃO
Seja ϕ um polinómio que tem uma raíz P sobre uma curva C. Representamos por $\eta_P(\phi; C)$, e designa-se por

multiplicidade *de* ϕ *em* P *sobre* C*, o maior* m *para o qual existe um polinómio* $u \in \mathbf{I}(C)$ *tal que* $\phi - u$ *tem uma raíz de multiplicidade* m *em* P*.*

Quando $\eta_P(\phi; C) = 1$*, então* ϕ ***intersecta*** *a curva* C *em* P*; se* $\eta_P(\phi; C) > 1$ *,* ϕ *é* ***tangente*** *a* C *em* P*.*

Comparando com a noção de multiplicidade simples (proposição 193) vemos que a mudança essencial está no facto de não se exigir que ϕ tenha multiplicidade m em P mas, em vez disso, exigir-se que a diferença $\phi - u$, para algum $u \in \mathbf{I}(C)$, tenha essa multiplicidade. Desta forma a multiplicidade de ϕ em P, $\eta_P(\phi)$, é equivalente à multiplicidade $\eta_P(\phi; 0)$ de ϕ em P sobre a curva trivial definida pelo polinómio 0.

EXEMPLO 41: Considere-se a recta $\phi = (y - 1)$. Seja C a curva definida pelo polinómio $\psi = y^2 - 1 - x^3$. O ponto $P = (0, 1)$ é raíz de ϕ e de ψ; por isso é um ponto de C comum com a curva definida por ϕ.

Com um pouco de manipulação pode-se constatar que

$$(y - 1) - \frac{1}{4}(3 - y)(y^2 - 1 - x^3) = \frac{1}{4}(3 - y)x^3 + \frac{1}{4}(y - 1)^3$$

O lado direito da igualdade é um polinómio com uma raíz em P de multiplicidade 3 (atente-se aos factores locais x^3 e $(y - 1)^3$). O lado esquerdo é uma diferença da forma $\phi - u$ para um polinómio $u = \frac{1}{4}(3 - y)\psi$ que, por ser múltiplo de ψ, é um elemento de $\mathbf{I}(C)$.

Consequentemente, atendendo à definição, o polinómio $y - 1$ tem uma multiplicidade 3 em P sobre a curva C. De facto $(y - 1)$ representa uma recta tangente à curva C onde o ponto de contacto P tem multiplicidade 3.

A noção de intersecção ou contacto de duas curvas é caracatrizada por um importante teorema[67].

198 TEOREMA (BEZOUT)
Sejam $C:\phi$ e $D:\psi$ duas curvas distintas. Então $C \cap D$ é um conjunto finito e verifica-se

$$\sum_{P \in C \cap D} \eta_P(\phi;\psi) \quad = \quad \sum_{P \in C \cap D} \eta_P(\psi;\phi) \quad = \quad \deg(\phi) * \deg(\psi) \tag{139}$$

É importante ter-se em atenção que nas curvas C e D estão incluídos não só os pontos afins como os pontos no infinito. Se uma das curvas (por exemplo $C:\phi$) for uma recta, tem grau 1 e, por isso, a soma (139) é igual ao grau do polinómio ψ. Isso significa que uma recta contacta uma curva ψ em tantos pontos (incluindo os pontos no infinito e contando cada ponto tantas vezes quantas a sua multiplicidade) quantos o grau de ψ.

EXEMPLO 42:
Considere-se a curva elíptica $\psi = y^2 - x^3 - 1$. Como o grau de ψ é 3, o teorema de Bézout diz-nos que qualquer recta ϕ contacta a curva em exactamente 3 pontos.

Por exemplo, recta $\phi = y$ intersecta a curva em 3 pontos distintos: o ponto racional $(-1,0)$ e dois pontos de ordenada complexa $(-\zeta,0)$ e $(-\zeta^2,0)$, sendo ζ uma raíz cúbica, complexa da unidade. Todos eles têm multiplicidade 1.

[67] Para prova ver HARTSHORNE, *Algebraic Geometry*.

A recta $\phi = y - 1$ contacta a curva ψ no ponto $P = (0, 1)$ e, como vimos no exemplo 41, a multiplicidade do contacto é 3. Portanto esta recta não contacta a curva em qualquer outro ponto.

A recta $\phi = x$ contacta a curva em dois pontos afins $(0, 1)$ e $(0, -1)$ e ainda no ponto do infinito P_∞.

Coordenadas Projectivas

Desde pelo menos o século XVII que os matemáticos se aperceberam que, adicionando certos pontos fictícios a rectas e outras curvas, a geometria Euclidiana poderia ser muito simplificada. Como exemplo, considere-se um par de asserções duais da geometria plana clássica:

(1) Duas rectas distintas determinam um único ponto: o seu ponto de intersecção.

(2) Dois pontos distintos determinam uma única recta: a recta que passa por ambos os pontos.

A asserção (1) não é válida quando as rectas são paralelas; esta excepção pode ser resolvida assumindo que rectas contêm um "ponto no infinito" e que as rectas paralelas se intersectam nesse "ponto no infinito"; a asserção, agora, é universalmente válida.

Para que a 2ª asserção continue válida com a introdução dos pontos no infinito temos de assumir que um ponto no plano e um ponto no infinito determinam também uma única recta. Isto faz supor que "ponto no infinito" seja equivalente ao conceito de "direcção" ou "inclinação" das rectas: um ponto no plano e uma directação determinam, realmente, uma única recta. Do mesmo modo, para que (2) continue a ser válida com dois pontos no infinito

distintos (duas direcções diferentes), somos levados naturalmente à conclusão que todos os pontos no infinito estão colocados sobre uma mesma recta e que tal recta só contém pontos no infinito; isto é, existe uma recta totalmente situada no infinito.

Estes conceitos têm resultados algébricos importantes; no entanto, em coordenadas afins, são difíceis de visualizar e conduzem a noções pouco naturais; por exemplo, pontos que são direcções. As coordenadas projectivas apareceram nos princípios do século XIX para ser possível lidar facilmente com este tipo de situações sem ter necessidade de introduzir interpretações "estranhas" para certos pontos, rectas ou outras curvas e todas estas entidades serem representados de uma única forma.

Esta representação unificada exige uma representação das entidades (pontos, rectas e curvas) segundo vários pontos de vista que são, de alguma forma, equivalentes. Nomeadamete, para representação de pontos, não basta apenas um tuplo de coordenadas (como nas coordenadas afins) mas vários tuplos ligados por uma relação de equivalência.

199 Noção

Representa-se por $\mathbb{P}^2$ *o conjunto das rectas em* $\mathbb{K}^3$ *que passam pela origem. Os elementos de* $\mathbb{P}^2$ *designam-se por* ***pontos projectivos*** *ou* ***pontos em coordenadas projectivas*** *de dimensão 2.*

Cada recta em $\mathbb{K}^3$ que passa pela origem é determinada por por um polinómio da forma $a\,x + b\,y + c\,z$ em que pelo menos um dos coeficientes (a, b, c) é diferente de zero. Note-se que a mesma recta pode ser representada por outro polinómio $a'\,x + b'\,y + c'\,z$ desde que se verifique $a = \lambda\,a' \wedge b = \lambda\,b' \wedge c = \lambda\,c'$ para algum $\lambda \neq 0$.

Esta observação conduz-nos a uma forma alternativa de definir $\mathbb{P}^2$ através de uma relação de equivalência sobre triplos de coordenadas. Considere-se triplos $P = (a, b, c)$ e $Q = (a', b', c')$ em $\mathbb{K}^3 \setminus \{(0, 0, 0)\}$ (i.e., pelo menos uma das componentes de cada tuplo é $\neq 0$); defina-se a a seguinte relação nesse espaço

$$P \sim Q \quad \Leftrightarrow \quad (\exists \lambda \neq 0)\, [a = \lambda a' \ \wedge \ b = \lambda b' \ \wedge \ c = \lambda c'] \tag{140}$$

A relação $\sim$ é claramente uma relação de equivalência. Os pontos em coordenadas projectivas são as classes de equivalência definidas em $\mathbb{K}^3 \setminus \{(0, 0, 0)\}$ por esta relação de equivalência.

200 NOÇÃO

No contexto de $\mathbb{P}^2$ *os* **pontos afins** *são as classes de equivalência que contêm triplos da forma* $(x, y, 1)$ *. Os* **pontos no infinito** *são classes de equivalência que contém triplos da forma* $(x, y, 0)$ *, em que* $x \neq 0$ *ou* $y \neq 0$*; nomeadamente* P_∞ *designa o ponto determinado pelo triplo* $(0, 1, 0)$ *e, para cada* $\mu \in \overline{\mathbb{K}}$*,* P_μ *designa o ponto no infinito determinado pelo triplo* $(1, \mu, 0)$ *.*

Um polinómio $\phi \in \overline{\mathbb{K}}\,[x, y, z]$ em que todos os monómios têm o mesmo grau d diz-se **homogéneo** de grau d. Um tal polinómio verifica $\phi(\lambda\, x, \lambda\, y, \lambda\, z) = \lambda^d\, \phi(x, y, z)$ para todo λ e todo triplo (x, y, z). Por isso se um triplo (x, y, z) é raiz do polinómio, qualquer outro triplo que lhe seja equivalente é também raiz do polinómio.

Um ponto P é **raiz** de um polinómio homogéneo quando existe um representante desta classe que é raiz do polinómio. Se tal acontecer, então (como vimos) qualquer outro triplo que lhe seja equivalente é também raiz do mesmo polinómio. Nestas circunstância escreve-se $\phi(P) = 0$.

Por exemplo, P_∞ é raíz do polinómio homogéneo $z\,y^2 + x^3 + x\,z^2$.

201 NOÇÃO

Um polinómio homogéneo $\phi \in \mathbb{K}[x, y, z]$ *que seja irredutível no fecho algébrico* $\overline{\mathbb{K}}\,[x, y, z]$ *determina uma* **curva plana** *em coordenadas projectivas (ou* **curva projectiva***) definida como o conjunto das raízes desse polinómio. A curva é* **singular** *quando existe um ponto da curva que é raiz, simultaneamente, das três derivadas parciais* $\partial\phi/\partial x$, $\partial\phi/\partial y$ *e* $\partial\phi/\partial z$.

Na representação de pontos, a vantagem das coordenadas projectivas está no facto de situações exceptionais (como o ponto no infinito) não exigirem nenhum tratamento especial; todos os pontos são referenciados do mesmo mod. A desvantagem está no facto de precisarmos de 3 coordenadas (em vez de 2) para definir o ponto e esse triplo de coordenadas ser apenas um representante da classe de equivalência que determina o ponto. Isto significa que qualquer propriedade que quisermos mostrar para um ponto tem de ser invariante pela multiplicação das coordenadas por um factor de escala $\lambda \neq 0$ arbitrário.

Uma consequência desta exigência é o facto de apenas se poder usar polinómios homogéneos. Enquanto que nas coordenadas afins qualquer polinómio irredutível definia uma curva, nas coordenadas afins só os polinómios homogéneos definem curvas.

□

Vamos colocar de novo a questão de curvas projectivas em $\mathbb{P}^2$ sobre um corpo algebricamente fechado K.

Como vimos na noção 201 na página 482, cada curva é determinada por um polinómio homogéneo e irredutível $\phi \in K[x,y,z]$ irredutível[68]. Dada uma curva $C:\phi$, representa-se por $\mathbf{I}(C)$ o seu ideal

$$\mathbf{I}(C) \;=\; \{\, p \in K\,[x,y,z] \;\mid\; p(P)=0 \text{ para todo } P \in C \,\} \tag{141}$$

Como consequência do Nullstellensatz, do facto de K ser algebricamente fechado e ϕ ser irredutível, tem-se

202 FACTO
Tem-se $p \in \mathbf{I}(C)$ se e só se p é divisível por ϕ.

Quando passamos à segunda parte desta definição (a noção de curva não-singular) surge a exigência de as três derivadas principais de ϕ não se anularem simultânemamente em nenhum ponto da curva. Para vermos o alcance desta restricção, é importante ver o seguinte morfismo e os resultados seguintes.

203 NOÇÃO
Seja C uma curva projectiva não-singular determinada por um polinómio homogéneo ϕ; seja d o seu grau. O morfismo $\mathcal{J}: C \longrightarrow \mathbb{P}^2$ determinado pelo triplo de polinómios homogéneos de grau $d-1$

$$\mathcal{J} \;=\; [\,\partial\phi/\partial x \;,\; \partial\phi/\partial y \;,\; \partial\phi/\partial z\,] \tag{142}$$

designa-se por ***jacobiano*** *de C.*

[68] Atente-se que, neste caso, K coincide com o seu fecho algébrico.

Porque C é não-singular, em qualquer zero do polinómio ϕ pelo menos uma das três componentes de $\mathcal{J}^C$ não se anula. Por isso $\mathcal{J}$ define realmente um morfismo.

204 TEOREMA
Seja $\mathcal{J}$ o jacobiano da curva projectivas C; então, imagem $\mathcal{J}^C(C)$ define em $\mathbb{P}^2$ uma curva projectiva que designamos por **curva dual** *de C.*

205 LEMA *Se $\phi \in K[x,y,z]$ é um qualquer polinómio homogéneo de grau d, verifica-se*

$$x\,\partial\phi/\partial x + y\,\partial\phi/\partial y + z\,\partial\phi/\partial z \quad = \quad d\cdot\phi \tag{143}$$

Prova O polinómio pode-se escrever como $\phi = \sum_{i+j+k=d} a_{ijk}\,x^i\,y^j\,z^k$. Temos

$$x\,\partial\phi/\partial x \;=\; \sum_{i+j+k=d} i\cdot a_{ijk}\,x^i\,y^j\,z^k$$

e formas análogas para $y\cdot\partial\phi/\partial y$ e $z\cdot\partial\phi/\partial z$. Donde

$$x\,\partial\phi/\partial x + y\,\partial\phi/\partial y + z\,\partial\phi/\partial z \;=\; \sum_{i+j+k=d} (i+j+k)\cdot a_{ijk}\,x^i\,y^j\,z^k \;=\; d\cdot\phi$$

Curvas definidas por polinómios do 1º grau, $a\,x + b\,y + c\,z$ designam-se por **rectas projectivas**.

Claramente, cada triplo $(a, b, c) \in \mathbb{K}^3$ determina uma recta projectiva a menos da relação de equivalência nos pontos de $\mathbb{P}^2$; isto é, os triplos (a, b, c) e $(\lambda\, a, \lambda\, b, \lambda\, c)$, com $\lambda \neq 0$, determinam exactamente a mesma recta. Consequentemente

206 FACTO
Existe um isomorfismo entre $\mathbb{P}^2$ *e o conjunto de todas as rectas projectivas em* $\mathbb{P}^2$*, isomorfismo esse que ao ponto* $P = [a, b, c]$ *faz corresponder a recta definida por* $a\, x + b\, y + c\, z$.

A recta projectiva (e o respectivo polinómio homogéneo de 1º grau) determinados por $P \in \mathbb{P}^2$ são, aqui, representados por $\mathbf{l}(P)$.

207 NOÇÃO
A recta $\mathbf{l}(\mathcal{J}^C(P))$ *designa-se por* **tangente** *à curva* C *no ponto* P.

□

No espaço afim $\mathbb{A}^3$ uma curva projectiva C determina uma superfície cónica com vértice na origem. Considere-se o ideal $\mathbf{I}(C)$ e o anel afim $\mathbb{A}^3(C)$. Recorde-se que este anel é definido como o quociente $K\,[x, y, z]\,/\mathbf{I}(C)$.

No anel afim $\mathbb{A}^3(C)$, a noção de multiplicidade de um polinómio p num ponto $P \in \mathbb{A}^3$ sobre a superfície C é definido da forma usual.

Sumariamente: um **factor local** de $P = (a, b, c)$ é um polinómio da forma $(x-a)^i\,(y-b)^j\,(z-c)^k$; p é m-**factorizável** em P se é divisível por um factor local em P de grau m; a **multiplicidade** de p em P é o maior $m \geq 0$ tal que p é decomponível numa soma de polinómios m-factorizáveis em P. O Nullstellensatz assegura que p tem uma raíz em P se e só se tem multiplicadade maior que zero nesse ponto.

Finalmente, se $P \in C$, a **multiplicidade** de $p \notin \mathbf{I}(C)$ em P **sobre** C, representada por $\eta_P(p; C)$, é a maior multiplicidade em P de polinómios u tais que $p - u \in \mathbf{I}(C)$.

Se $p(P) \neq 0$, convencionamos que $\eta_P(p; C) = 0$. Se $p \in \mathbf{I}(C)$ convencionamos que $\eta_P(p; C) = \infty$.

208 PROPOSIÇÃO
Seja $p \in K[x, y, z]$ um polinómio homogéneo e $C : \phi$ uma curva projectiva. Então, para todos $P = (a, b, c) \in K^3$ e $\lambda \neq 0$, tem-se $\eta_P(p; C) = \eta_{\lambda P}(p; C)$.

Prova Se $\eta_P(p; C) = m$ então existem polinómios u, v tais que $p = u\,\phi + v\,f$ sendo f um factor local em $P = (a, b, c)$ de grau m. Isto é, $f = (x-a)^i\,(y-b)^j\,(z-c)^k$ com $i + j + k = m$. Seja H a aplicação que mapeia qualquer polinómio $h(x, y, z)$ em $\lambda^m\,h(x/\lambda, y/\lambda, z/\lambda)$. Se h for homogéneo de grau d tem-se $H(h) = \lambda^{m-d}\,h$. Verifica-se facilmente que $f' = H(f)$ é um factor local em λP de grau m.

Consequentemente $H(p) = H(u)H(\psi) + H(v)\,H(f)$ conduz à igualdade $p = u'\,\phi + v'\,f'$ já que tanto p como ϕ são homogéneos. Consequentemente a multiplicidade de p sobre C em λP é, pelo menos, m. Dada a simetria da afirmação, terá de ser exactamente m.

Uma multiplicidade importante é a multiplicidade da tangente a uma curva no ponto de tangência e sobre a curva. Em consequência do lema 205, a tangente à curva C no ponto P, contém sempre esse ponto P. Portanto a tangente intersecta a curva. De facto, tem-se

209 LEMA *Seja $t_P = \mathbf{l}(\mathcal{J}^C(P))$ a recta tangente à curva C no ponto P. Então tem-se sempre $\eta_P(t_P; C) > 1$.*

EXEMPLO 43: Considere-se a curva C definida por $y^2\,z - x^3 - z^3$. São pontos da curva,

$$P = [0,1,1] \qquad Q = [1,0,1] \qquad P_\infty = [0,1,0]$$

Pretende-se determinar as tangentes nesses pontos assim como a multiplicidade respectiva. Nesta curva tem-se

$$\mathfrak{D} \;=\; [-3\,x^2, 2\,y\,z, y^2 - 3\,z^2] \qquad \mathcal{J}^C(P) = [0,-1,1] \qquad \mathcal{J}^C(Q) = [1,0,1] \qquad \mathcal{J}^C(P_\infty) = [0,0,1]$$

As tangentes respectivas são as rectas

$$t_P \;=\; z - y \qquad t_Q \;=\; x + z \qquad t_{P_\infty} \;=\; z$$

Como o polinómio tem grau 3 e as rectas tangente têm grau 1, o teorema de Bézout (teorema **??**) diz-nos que a multiplicidade não excede 3. O lema 209 diz-nos que a multiplicidade é > 1.

As funções racionais em coordenadas projectivas são definidas, também, através de fracções de polinómios homogéneos com o mesmo grau.

210 NOÇÃO
Seja C/K uma curva projectiva em $\mathbb{P}^2$ e K um corpo algebricamente fechado. Um par de polinómios $f, g \in K[x, , y, z]$ determina uma **fracção homogénea** *quando ambos são homogéneos e têm o mesmo grau.*

O espaço $K(C)$ *das* ***funções racionais*** *sobre* C *é o espaço quociente definido no conjunto das fracções homogéneas pela relação de equivalência*

$$f/g \sim p/q \quad \Leftrightarrow \quad f\,q - g\,p \in \mathbf{I}(C)$$

211 DEFINIÇÃO
A ***ordem*** *de* $f = p/q \in \mathbb{K}(C)^*$ *(isto é,* $f \neq 0$*) em* P*, representado por* $\mathsf{ord}_P(f)$ *, é a diferença*

$$\mathsf{ord}_P(f) \;=\; \eta_P(p;C) - \eta_P(q;C)$$

Se for $\mathsf{ord}_P(f) > 0$ *diz-se* f *tem um* ***zero*** *de ordem* $\mathsf{ord}_P(f)$ *em* P*; se for* $\mathsf{ord}_P(f) < 0$ *diz-se que* f *tem um* ***pólo*** *de ordem* $-\mathsf{ord}_P(f)$ *em* P*.*

Por convenção, a função racional nula $f = 0$ *tem um zero de ordem* ∞ *em todo o ponto de* C*.*

É fácil verificar que estas noções são independentes do representante p/q escolhido para a função racional f. Tem-se também, para todo o par de funções racionais $f, g \in \bar{\mathbb{K}}(C)^*$ e todo o ponto P da curva C

$$\mathsf{ord}_P(f\,g) \;=\; \mathsf{ord}_P(f) + \mathsf{ord}_P(g) \tag{144}$$

O seguinte resultado é essencial para o entendimento do papel das funções racionais e pode ser facilmente demonstrado. Vamos considerar uma curva projectiva $C/\mathbb{K}$ e uma qualquer função racional $f \in \bar{\mathbb{K}}(C)^*$. Então

212 FACTO

A função f tem um número finito de zeros e de pólos em C e a ordem de cada zero ou pólo é finita. Se f não for uma função constante sobre C (isto é, $f \notin \mathbb{K}^*$) então, pelo menos num ponto $P \in C$ tem-se $\mathrm{ord}_P(f) \neq 0$. *Adicionalmente verifica-se sempre*

$$\sum_{P \in C} \mathrm{ord}_P(f) \;=\; 0$$

Este resultado diz-nos que o número de pólos de f (cada um contanto tantas vezes quanto a sua ordem) tem de ser igual ao número de zeros. Diz-nos também que, a menos do caso trivial das funções constantes sobre na curva[69], existem sempre pólos e zeros e em número finito.

□

Frequentemente interessa-nos resolver o problema inverso:

> *dado um conjunto de pontos eventuais pólos $P_1, P_2, \cdots, P_n$ e de eventuais zeros $Z_1, Z_2, \cdots, Z_n$ quere-se construir uma função racional f que tenha exactamente estes pólos e estes zeros*

Essencialmente quere-se $f = p/q$ definindo dois polinómios p e q homogéneos e com o mesmo grau; o primeiro deve ter os pontos Z_i como raízes e o segundo deve ter os pontos P_i como raízes.

[69] Note-se que f pode ser constante sobre C sem ser uma função constante; por exemplo, se ϕ determinar a curva C, a fracção $(\lambda + \phi)/(\mu + \phi)$, com $\lambda, \mu \in \mathbb{K}^*$, não é constante mas determina uma função racional que é constante sobre C.

Vamos começar por considerar versões simplificadas deste problema começando por polinómios homogéneos lineares; isto é **rectas**. Para isso precisamos de algumas ferramentas que nos ajudem a construir e manipular rectas.

213 DEFINIÇÃO
Sejam $P, Q \in \mathbb{P}^2$ *determinados por representantes* (a, b, c) *e* (a', b', c') *respectivamente. Se* $P \neq Q$ *define-se*

$$P \otimes Q \doteq [bc' - cb' \ , \ ca' - ac' \ , \ ab' - ba'] \tag{145}$$

Representa-se por $\mathrm{l}(P)$ *o polinómio homogéneo do* 1^o *grau* $a\,x + b\,y + c\,z$ *ou, indistintamente, a recta definida por isso polinómio.*

Facilmente se verifica que $P \otimes Q$ e $\mathrm{l}(P)$ são independentes do representante escolhido para os pontos P e Q.

Como $P \otimes$ Q só está definido para pontos distintos, pode-se estender a definição acrescentando um ponto $\mathfrak{O}$ extra ao espaço $\mathbb{P}^2$ (identificado com o triplo de coordenadas todas nulas $(0, 0, 0)$) e fazendo $P \otimes P = P \otimes \mathfrak{O} = \mathfrak{O}$. Também $\mathrm{l}(\mathfrak{O}) \doteq \mathbb{P}^2$. Nestas circunstâncias

214 PROPOSIÇÃO
O operador $\otimes$ *definido em* $\mathbb{P}^2 \cup \{0\}$ *por* (145) *é comutativo. Para* $P, Q \in \mathbb{P}^2$ *verifica-se* $P \otimes Q = \mathfrak{O}$ *se e só se* $P = Q$. *Adicionalmente, para todo* $P, Q, R \in \mathbb{P}^2$, *verifica-se*

$$R \in \mathrm{l}(P \otimes Q) \quad \textit{sse} \quad P \in \mathrm{l}(R \otimes Q) \quad \textit{sse} \quad Q \in \mathrm{l}(P \otimes R)$$

Assim cada ponto determina, através das suas coordenadas, uma recta. A recta que passa pelos pontos P e Q é determinada pelas coordenadas do ponto $P \otimes Q$.

□

Nestas circunstâncias, voltando ao problema inicial de construir funções racionais dados os seus pólos e zeros, tem-se

1. Se pretendermos um polinómio que tenha exactamente dois zeros, P e Q, basta construir a recta $\mathrm{l}(P \otimes Q)$.
2. Se pretender-mos uma função racional que tenha um zero Z e um polo P, podemos começar por escolher um outro qualquer ponto O que seja distinto de Z e de P e construir duas rectas, ambas passando por O, e passando por Z e por P.
$$p = \mathrm{l}(Z \otimes O) \quad , \quad q = \mathrm{l}(P \otimes O)$$
A fracção $f = p/q$ determina a função racional pretendida. Note-se que ela tem um polo em O que se anula com o zero que tem em O; por isso f acaba por ter só o polo P e o zero Z.
3. A estratégia anterior pode ser usada para construir funções racionais com pólos e zeros com ordem superior a 1. Vamos supor que se quer um polo P de ordem 2 e um zero Z também de ordem 2. Então escolhem-se dois quaisquer pontos O_1 e O_2 distintos entre si e distintos de P e Z. Em seguida constroem-se rectas
$$p_1 = \mathrm{l}(Z \otimes O_1) \qquad p_2 = \mathrm{l}(Z \otimes O_2) \qquad q_1 = \mathrm{l}(P \otimes O_1) \qquad q_2 = \mathrm{l}(P \otimes O_2)$$
A fracção $f = (p_1\, p_2) \,/\, (q_1\, q_2)$ determina a função racional pretendida. Note-se que tanto O_1 como O_2 aparecem simultaneamente como zeros e pólos e, por isso, anulam-se.

4. Vamos agora considerar que se quer n zeros $Z_1, \cdots, Z_n$, todos distintos, e n pólos $P_1, \cdots, P_n$ também todos distintos e distintos dos zeros. Basta escolher um ponto auxiliar O e construir as rectas

$$p_i = \mathrm{l}(Z_i \otimes O) \qquad q_i = \mathrm{l}(P_i \otimes O) \qquad i = 1 \cdots n$$

e definir a função racional $f = \prod_{i=1}^{n} (p_i/q_i)$.
Obviamente, se um zero ou um polo aparecer repetido (ordem > 1) temos de usar mais pontos auxiliares tal como fizemos no caso anterior.

Estes casos indicam um algoritmo simples para construir uma função racional dados os seus conjuntos de zeros e pólos. Este algoritmo é particularmente importante em curvas elípticas na construção de emparelhamentos.

8.2 Introdução a ideais e variedades

Problema simportantes, como a caracterização da intersecção de duas curvas, que são fundamentais ao estudo das curvas elípticas requerem uma análise, mesmo resumida, da noção de variedade e, por isso, da noção de ideal.

Seja R um anel; no que se segue vamos sempre assumir que os anéis são formam um domínio integral: isto é, são comutativos e $r, s \neq 0 \in R$ implica sempre $r\,s \neq 0$.

Dados subconjuntos $I, J \subseteq R$ define-se $I+J = \{\, r+s \mid r \in I\ ,\ s \in J \,\}$ e $I\,J = \{\, r\,s \mid r \in I\ ,\ s \in J \,\}$. Define-se, $I^0 = R$ e $I^{n+1} = I\,I^n$. O conjunto $\{s\}J$ escreve-se como sJ.

215 NOÇÃO

Um subconjunto não vazio $I \subseteq R$ é um **ideal** *quando $I\,R = I$ e $I + I = I$.*

Um ideal $\mathfrak{p} \neq R$ é **primo** *quando $r\,s \in \mathfrak{p}$ implica $r \in \mathfrak{p}$ ou $s \in \mathfrak{p}$. O ideal $\mathfrak{m}$ é* **máximo** *quando não está contido em nenhum outro ideal primo.*

Claramente, a soma e o produto de ideais são ideais. Se I é um ideal então o conjunto $\{\, r \mid r^n \in I$ para algum $n \,\}$ é também um ideal. Tal conjunto representa-do por $\sqrt{I}$ e designa-se por **radical** de I. Um **ideal radical** é qualquer ideal I que coincida com o seu radical. Todo o ideal primo $\mathfrak{p}$ é radical.

Cada ideal primo $\mathfrak{p} \subset R$ determina uma relação de equivalência em R da forma usual: $r \sim s$ sse $r - s \in \mathfrak{p}$. Porque $\mathfrak{p}$ é primo, o espaço quociente respectivo tem a estrutura de um domínio integral; representa-se $R/\mathfrak{p}$ tal anel. Seja $I \subset R$ um ideal que contenha $\mathfrak{p}$; define-se $I/\mathfrak{p}$ como o ideal $\mathfrak{q}$ tal que $I = \mathfrak{p} + \mathfrak{q}$. Verifica-se facilmente que $I/\mathfrak{p}$ determina um ideal em $R/\mathfrak{p}$; adicionalmente, todos os ideais em $R/\mathfrak{p}$ têm esta forma.

216 NOÇÃO

Um ideal da forma $s\,R$, com $s \in R$, diz-se **principal** *e representa-se por $\langle s \rangle$. Um ideal I é* **finitamente gerado** *quando se pode escrever como $I = s_1R + s_2R + \cdots + s_nR$, para um conjunto finito $\{s_1, s_2, \ldots, s_n\}$ de elementos de R designados por* **geradores**. *Neste caso escreve-se $I = \langle s_1, s_2, \ldots, s_n \rangle$.*

Se $\mathfrak{p}$ é um ideal primo, o seu **peso** *é o maior k tal que existe uma cadeia $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_{k-1} \subset \mathfrak{p}$ em que os vários $\mathfrak{p}_i$ são ideais primos distintos entre si e distintos de $\mathfrak{p}$. O supremo dos pesos de todos os ideais primos de R designa-se por* **dimensão de Krull** *(ou, simplesmente,* **dimensão***) de R. Um anel de dimensão finita diz-se* **Noeteriano**.

217 TEOREMA (BÁSICO DE HILBERT)

Um anel R é Noeteriano se e só se for finitamente gerado. Adicionalmente, sendo R Noteriano, qualquer anel de polinómios $R[x_1, \cdots, x_n]$ é noeteriano.

□

Considere-se agora um corpo $\mathbb{K}$ e o anel $S_n = \overline{\mathbb{K}}[x_1, \ldots, x_n]$ dos polinómios nas variáveis $x_1, \ldots, x_n$ com coeficientes no fecho algébrico de $\mathbb{K}$. Interessa-nos considerar o anel S_n mas também os anéis quociente

$R = S_n/\mathfrak{p}$, sendo $\mathfrak{p}$ um ideal primo. Qualquer dos casos será designado por um **anel de polinómios**.

Uma observação importante resulta do facto de qualquer corpo $\mathbb{K}$, visto como um anel, ser noeteriano. De facto o único ideal primo de $\mathbb{K}$ é o anel trivial $\{0\}$ que tem peso 1. Então, pelo teorema básico de Hilbert, todo S_n é noeteriano; o que implica

218 COROLÁRIO *Todo o ideal $I \subset S_n$ é finitamente gerado.*

EXEMPLO 44: Tomemos $\mathbb{K}$ como $\mathbb{Q}$ (o corpo dos números racionais) e o anel de polinómios a duas variáveis S_2. Vamos ver alguns exemplos de ideais neste anel. Tenha-se em atenção que $S_2 = \overline{\mathbb{Q}}[x, y]$ e, dado que o fecho algébrico de $\mathbb{Q}$ é o corpo dos complexos $\mathbb{C}$, os elementos de S_2 são polinómios nas variáveis x, y com coeficientes complexos.

Como todo o ideal de S_2 é finitamente gerado (corolário 218) para definir um ideal basta indicar os seus geradores. É possível definir o ideal de outras formas: através de operações sobre outros ideais ou através de definição do conjunto por compreensão a partir de uma propriedade dos polinómios.

Via geradores temos, por exemplo, os ideais

$$I = \langle x, y - x \rangle \qquad J = \left\langle y^2 - x^3 - 1 \right\rangle$$

Pode-se definir ideias através das operações de soma e produto. Por exemplo

$$I + J = \left\langle x, y - x, y^2 - x^3 - 1 \right\rangle \quad , \quad I\,J = \left\langle x\,(y^2 - x^3 - 1), (y - x)\,(y^2 - x^3 - 1) \right\rangle$$

Pode-se finalmente definir ideiais por compreensão: seja $U = \{p_1, \ldots, p_n\}$ um conjunto finito de $\mathbb{K}^2$-pontos, então pode-se definir

$$I_U = \{ f \in S_2 \mid f(p) = 0 \quad \text{para todo } p \in U \}$$

Considere-se, de novo, $S_n = \overline{\mathbb{K}}[x_1, \ldots, x_n]$. Os ideais no anel S_n têm uma relação clara com determinados conjuntos $X \subset \mathbb{K}^n$ designados por **algébricos**. Para todo subconjunto $X \subseteq \mathbb{K}^n$ define-se

$$\mathbf{I}(X) = \{ f \mid f(p) = 0 \text{ para todo } p \in X \} \tag{146}$$

Pode-se verificar que $\mathbf{I}(X)$ é um ideal. Alternativamente seja $I \subset S_n$ um qualquer ideal; define-se

$$\mathbf{Z}(I) = \{ p \in \mathbb{K}^n \mid f(p) = 0 \text{ para todo } f \in I \} \tag{147}$$

Conjuntos $X \subseteq \mathbb{K}^n$ da forma $\mathbf{Z}(I)$, para algum ideal I dizem-se **algébricos**. $\mathbf{Z}$ mapeia ideais em conjuntos algébricos; a construção $\mathbf{I}(X)$ mapeis quaisquer conjuntos em ideais. A relação entre estas duas construções é expressa num dos resultados mais importantes da Álgebra.

219 TEOREMA (NULLSTELLENSATZ)
Todo o ideal $I \subset S_n$ verifica $\mathbf{I}(\mathbf{Z}(I)) = \sqrt{I}$.

Alguns corolários que são consequência imediata deste teorema e do facto do corpo $\overline{\mathbb{K}}$ ser algebricamente fechado.

220 COROLÁRIO *Sejam* $I, J \subset S_n$ *ideais e* $X, Y \subset S_n$ *conjuntos algébricos. Então verifica-se* $\mathbf{Z}(I+J) = \mathbf{Z}(I) \cap \mathbf{Z}(J)$, $\mathbf{Z}(I \cap J) = \mathbf{Z}(I) \cup \mathbf{Z}(J) = \mathbf{Z}(I\ J)$, $\mathbf{I}(X \cap Y) = \sqrt{\mathbf{I}(X) + \mathbf{I}(Y)}$ *e* $\mathbf{I}(X \cup Y) = \mathbf{I}(X) \cap \mathbf{I}(Y)$.

221 COROLÁRIO *Dado um qualquer conjunto* $X \subseteq \mathbb{K}^n$ *(algébrico ou não), seja* $\overline{X}$ *a intersecção de todos os conjuntos algébricos* Y *que contém* X*. Então* $\overline{X} = \mathbf{Z}(\mathbf{I}(X))$.

O conjunto $\overline{X}$ designa-se por **fecho** de X. Se X é algébrico e $X = \overline{X}$, então X diz-se **algébricamente fechado**.

Se existir uma partição $X = Y \cup Y'$, sendo Y e Y' subconjuntos próprios de X que são algébricamente fechados, então X diz-se **redutível**. Se não existir tal partição, X diz-se **irredutível**.

222 COROLÁRIO *Um conjunto algébrico* $X \subset \mathbb{K}^n$ *é irredutível se e só se* $\mathbf{I}(X)$ *é primo. Adicionalmente, se* X *for irredutível, o seu fecho* $\overline{X}$ *também é irredutível.*

223 COROLÁRIO *Um ideal principal* $\langle \phi \rangle$ *é primo se e só se* ϕ *for irredutível em* $\overline{\mathbb{K}}[x_1, \ldots, x_n]$.

224 COROLÁRIO *Para todo ponto* $p = (a_1, a_2, \cdots, a_n) \in \mathbb{K}^n$ *, o conjunto singular* $\{p\}$ *é algébrico.*

O ideal $\mathfrak{m}_p = \mathbf{I}(\{p\})$ *é máximo e é gerado pelos* n *polinómios* $\{(x_i - a_i)\}_{i=1}^n$ *. Isto é*

$$\mathfrak{m}_p = \langle\, x_1 - a_1\ ,\ x_2 - a_2\ ,\ \cdots\ ,\ x_n - a_n \,\rangle \tag{148}$$

Adicionalmente todo o ideal máximo em S_n *tem a forma* $\mathfrak{m}_p$ *, para algum ponto* $p \in K^n$ *. Finalmente, para todo o ideal* $I \subset R$*, tem-se* $p \in \mathbf{Z}(I)$ *se e só se* $I \subseteq \mathfrak{m}_p$.

Notas Provas para o Nullstellensatz e para estes corolários podem ser obtidas no textos standard de Geometria Algébrica; por exemplo, Commutative Algebra de David Eisenbud ou Algebraic Geometry de Robin Hartshorne, publicados no Graduate Texts in Mathematics da Springer-Verlag.

225 Definição
Uma **variedade afim** *(ou, simplesmente,* **variedade***) é um conjunto algébrico* $V \subseteq \mathbb{K}^n$ *irredutível e algebricamente fechado.*

A **dimensão** *de* V *é o maior* k *para o qual existe uma cadeia* $X_1 \subset X_2 \subset \cdots \subset X_k$, *de subconjuntos próprios* $X_i \subset V$ *que são distintos, irredutíveis e algebricamente fechados. Uma variedade designa-se por* **ponto**, **curva**, **superfície** *ou* **hipersuperfície**, *consoante a sua dimensão é, respectivamente,* 0, 1, 2 *ou* > 2.

O domínio integral $S_n/\mathbf{I}(V)$ *representa-se por* $\mathbb{A}(V)$ *e designa-se por* **anel afim** *de* V.

O conjunto $\mathbb{K}^n$, visto como uma variedade, representa-se por $\mathbb{A}^n$. O respectivo ideal $\mathbf{I}(\mathbb{A}^n)$ é o ideal trivial $\{0\}$. O conjunto vazio, visto como conjunto algébrico, é também uma variedade gerada pelo ideal $\langle 1 \rangle$.

Note-se que, sendo V uma variedade, o corolário 222 diz-nos que $\mathbf{I}(V)$ é um ideal primo e, por isso, o anel quociente $\mathbb{A}(V) = S_n/\mathbf{I}(V)$ é um domínio integral.

Claramente $\mathbb{A}(V)$ tem a estrutura de um espaço vectorial sobre $\overline{\mathbb{K}}$. Anéis que são extensões de um corpo K e são espaços vectoriais sobre esse corpo designam-se por K-**álgebras**. Assim $\mathbb{A}(V)$ é uma $\overline{\mathbb{K}}$-álgebra.

Como espaço vectorial, tem uma dimensão que coincide com o número de elementos numa sua base. No entanto $\mathbf{I}(V)$, como todo o ideal de S_n, é finitamente gerado; isto faz-nos pensar que o espaço vectorial $S_n/\mathbf{I}(V)$ tem uma dimensão finita. De facto, temos um resultado bastante mais forte.

226 TEOREMA
Seja V uma variedade. O anel afim $\mathbb{A}(V)$ é uma $\overline{\mathbb{K}}$-álgebra finitamente gerada. A dimensão de $\mathbb{A}(V)$ como espaço vectorial coincide com sua dimensão de Krull como anel e coincide também com a dimensão da variedade V.

Uma série de resultados importantes resultam deste teorema.

227 COROLÁRIO *A dimensão de $\mathbb{A}^n$ é n. Uma variedade $V \subset \mathbb{A}^n$ tem dimensão $n-1$ se e só se tem $I(V) = \langle \phi \rangle$ para algum polinómio ϕ irredutível em S_n.*

228 PROPOSIÇÃO
Seja V uma variedade de dimensão d e seja $\mathfrak{p}$ um ideal primo do anel afim $\mathbb{A}(V)$ de peso p. Então

$$\dim \mathbb{A}(V)/\mathfrak{p} \;=\; d - p$$

□

Os ideias máximos $\mathfrak{m}_p$ e as suas diversas potências $\mathfrak{m}_p^m$, definidos por pontos $p \in K^n$, são essenciais para a definição de multiplicidade (das raízes de um polinómio, da intersecção de duas curvas, etc.). Note-se que, para todo $n \geq 0$, o ideal $\mathfrak{m}_p^n$ está contido em $\mathfrak{m}_p$ e, genericamente, em todos os $\mathfrak{m}_p^k$, com $k < n$.

229 Noção

Seja $\mathfrak{p}$ *um ideal primo e* $p \in K^n$ *um ponto em* $\mathbf{Z}(\mathfrak{p})$ *(isto é, verifica-se* $\mathfrak{p} \subseteq \mathfrak{m}_p$*). Dado um qualquer ideal* $\mathfrak{a} \not\subseteq \mathfrak{p}$*, define-se a* **multiplicidade** *de* $\mathfrak{a}$ *em* p **sobre** $\mathfrak{p}$*, como a maior potência* $m \geq 0$ *tal que* $\mathfrak{a} \subseteq \mathfrak{m}_p^m/\mathfrak{p}$*. Representa-se essa multiplicidade por* $\eta_p(\mathfrak{a};\mathfrak{p})$*.*

Nomeadamente, quando $\mathfrak{p}$ *coincide com o ideal trivial* $\langle 0\rangle$*,* $\eta_p(\mathfrak{a};\langle 0\rangle)$ *representa-se simplesmente por* $\eta_p(\mathfrak{a})$ *e designa-se por* **multiplicidade** *de* $\mathfrak{a}$ *em* p*.*

A situação mais comum verifica-se quando se tem $\mathfrak{p} = \mathbf{I}(V)$, para uma determinada variedade V, e $\mathfrak{a} = \langle f\rangle$ para um polinómio f. Nestas circunstâncias, temos a noção de multiplicidade de um polinómio f num ponto p sobre a variedade V ou, simplesmente, multiplicidade do polinómio f no ponto p.

Exemplo 45: Considere-se o espaço afim $\mathbb{A}^3$ e a variedade afim E definida pelo polinómio $\phi \equiv x^2+y^2+z^2-z$. É facil verificar que E é uma esfera de raio $1/2$ centrada no ponto $(0,0,1/2)$. O plano definido pelo polinómio $p \equiv z$ é tangente à esfera na origem $(0,0,0)$. Trivialmente tem-se

$$z = (x^2+y^2+z^2) - \phi$$

Isto significa que, em $\mathbb{A}(E)$, temos $z \sim (x^2+y^2+z^2)$. O termo $(x^2+y^2+z^2)$ é um factor local na origem $(0,0,0)$ de grau 2; portanto o plano tangente z tem multiplicidade 2 na origem sobre a esfera E.

Numa variedade V, um ponto $p \in V$ diz-se **singular** quando $\eta_p(\mathbf{I}(V)) > 1$. As variedades não-singulares V são aquelas que não têm pontos singulares.

EXEMPLO 46: Tomemos de novo a esfera $E : \phi$, com $\phi \equiv x^2 + y^2 + z^2 - z$, que vimos no exemplo 45. Como determinar a multiplicidade de ϕ num ponto genérico $p = [a, b, c]$ da esfera?

Para isso a melhor solução é usar um sistema de computação algébrica, como o MAPLE, e um pacote de funções, como `PolynomialIdeal`, para computar as várias operações com ideais.

1. Começa-se por determinar o ideal máximo genérico $m_p = \langle x - a, y - b, z - c \rangle$ e as respectivas potências $m_p^2 = m_p\, m_p$, $m_p^3 = m_p^2\, m_p$, etc.
2. Tratando a, b, c como 3 novas variáveis, constrói-se o ideal $S := \langle \phi(a, b, c) \rangle$ que denota o facto de o ponto (a, b, c) pertencer à variedade E. Neste caso tem-se $S = \left\langle a^2 + b^2 + c^2 - c \right\rangle$.
3. No espaço de polinómios a 6 variáveis (x, y, z, a, b, c) constroem-se sucessivamente os ideais $s_1 = m_p + S$, $s_2 = m_p^2 + S$, $s_3 = m_p^3 + S$, etc.
4. Testa-se sucessivamente, $\phi \in s_1$, $\phi \in s_2$, $\phi \in s_3$, etc. O último k onde o teste $\phi \in s_k$ tem sucesso, é a multiplicidade pretendida.

Executando este algoritmo verifica-se que a multiplicidade é sempre 1 e, portanto, a variedade é não-singular.

A noção de ponto singular está assocoada à noção de tangente a uma variedade num ponto e, baseado neste conceito, é possível verificar facilmente se um ponto é ou não singular. Para isso precisamos de uma extensão das noções de jacobiano (noção 239, página 511) e de tangente (noção 207) a variedades.

230 NOÇÃO
Seja $V \subset \mathbb{A}^n$ *a variedade definida pelo ideal* $\langle g_1, \ldots, g_l \rangle$. *O* **jacobiano** *de* V *é a matrix de polinómios* $\mathcal{J}$ *cujo elemento genérico é* $\mathcal{J}_{ij} = \partial g_j / \partial x_i$.

O seguinte teorema[70] permite detectar os eventuais pontos singulares das variedades.

231 TEOREMA
Seja $\mathcal{J}$ *o jacobiano da variedade* V*; um ponto* $p \in V$ *é não-singular se e só*

$$\text{Rank}(\mathcal{J}(p)) \;=\; n - \dim(V)$$

EXEMPLO 47: Considere-se de novo a esfera nos exemplos 45 e 46. Nesta variedade a dimensão é 2 e o espaço tem dimensão 3. Donde, neste caso, $n - \dim(V) = 1$.

O ideal que define a esfera tem apenas um gerador (o polinómio ϕ). Portanto o jacobiano é o vector coluna das derivadas parciais $(\partial\phi/\partial x, \partial\phi/\partial y, \partial\phi/\partial z)$. Neste caso será $\mathcal{J} = (2\,x, 2\,y, 2\,z - 1)$ que, como matriz, tem *rank* 1 para todo ponto da variedade.

[70] Para prova veja-se HARTSHORNE, *Algebraic Geometry*.

Se considerar-mos a intersecção da esfera com o plano $x = 0$ temos um círculo; a dimensão da variedade é 1 donde, neste caso, $n - \dim(V) = 2$.

Os geradores do ideal que define o círculo são $\left\langle x^2 + y^2 + z^2 - z, x \right\rangle$. O jacobiano é a matriz $\begin{bmatrix} 2\,x & 1 \\ 2\,y & 0 \\ 2\,z - 1 & 0 \end{bmatrix}$.

No círculo tem-se $x = 0$. Para que esta matriz tenha *rank* < 2, a primeira coluna terá de ser múltipla da segunda; isto só acontece se for $y = 0$ e $z = 1/2$. No entanto o ponto $(0, 0, 1/2)$ não pertence à variedade. Por isso, neste círculo, o *rank* do jacobiano é sempre 2 e não existem pontos singulares.

Um terceiro exemplo é a variedade de dimensão 2 definida pelo polinómio $\psi = y^2\,z - x\,(x - z)^2$. O jacobiano é a matriz coluna $\mathcal{J} = \left[(x - z)\,(z - 3\,x)\ ,\ 2\,y\,z\ ,\ y^2 + 2\,x\,(x - z)\right]$.

Note-se que qualquer ponto onde seja $x = z$ e $y = 0$ é um ponto da variedade definida por ψ; nesses pontos o jaconiano reduz-se a $\mathcal{J} = [0, 0, 0]$; portanto tem *rank* 0. Como consequência todos os pontos da forma $(x, 0, x)$ são pontos singulares da variedade definida por ψ.

A noção de tangente a uma variedade é um conceito um pouco mais complexo do que o de tangente a uma curva. Por exemplo, em relação a uma superfície $V \subset \mathbb{A}^3$ (como a esfera dos exemplos anteriores) pode-se ver a tangente como um plano, uma recta ou mesmo só um ponto.

Por isso convém estender cuidadosamente este conceito.

Cada ponto $p = (a_1, \ldots, a_n) \in \mathbb{A}^n$ define a variedade $\mathbf{l}(p)$, designada por **hiper-plano** de p, gerada pelo polinómio do 1º grau $a_1\, x_1 + \cdots + a_n\, x_n$. A dimensão de $\mathbf{l}(p)$ é $n-1$, se for $p \neq (0, \ldots, 0)$ ou é n em caso contrário.

Um vector de pontos $L = (p_1, \ldots, p_n) \in (\mathbb{A}^n)^l$ gera a variedade $\mathbf{l}(L) = \bigcap_{j=1}^{l} \mathbf{l}(p_j)$. A dimensão desta variedade depende do número de pontos não nulos que são linearmente independentes. Vendo L como uma matriz, o número de pontos não-nuos linearmente independentes é dado pelo *rank* da matriz. Por isso,

232 FACTO
$\mathbf{l}(L)$ *é uma variedade e um* K*-espaço vactorial de dimensões* $n - \mathrm{Rank}(L)$.

233 NOÇÃO
Dada uma variedade afim $V \subset \mathbb{A}^n$ *de jacobiano* $\mathcal{J}$, *seja* $\mathcal{T}(V)$ *a variedade dada por*

$$\mathcal{T}(V) \;=\; \{\, (p, X) \in V \times \mathbb{A}^n \;\mid\; X \in \mathbf{l}(\mathcal{J}(p)) \,\} \tag{149}$$

Caso V *seja não-singular então* $\mathcal{T}(V)$ *designa-se por* **feixe tangente** *de* V.

Note-se nesta definição que, sendo V é não-singular, temos $\dim(V) = n - \mathrm{Rank}(\mathcal{J}(p)) = \dim(\mathbf{l}(\mathcal{J}(p)))$, independentemente de $p \in V$. Portanto a variedade $\mathbf{l}(\mathcal{J}(p))$ tem, para todo $p \in V$, exactamente a mesma dimensão que V.

8.3 Divisores

Dado que o conjunto de zeros e de pólos caracterizam completamente as funções racionais sobre uma curva C, é conveniente introduzir uma noção que faça esta abstracção; isto é, represente os conjuntos de pólos e zeros com as suas ordens associadas. Esta é a noção de **divisor**.

234 DEFINIÇÃO
Um **divisor** *numa curva projectiva* C *é uma soma formal escrita*

$$D = \sum_{P \in C} n_P (P) \qquad com \quad n_p \in \mathbb{Z} \tag{150}$$

onde o número de inteiros n_P *diferentes de zero é finito.*

A **ordem** *do divisor* D *no ponto* P, *representada* $\mathsf{ord}_P(D)$, *é o inteiro* n_P. *O* **suporte** *de* D, $\mathsf{supp}(D)$, *é o conjunto dos pontos* $P \in C$ *em que* $\mathsf{ord}_P(D) \neq 0$. *A* **grau** *do divisor* (150) *é o inteiro*

$$\mathsf{deg}(D) = \sum_{p \in C} \mathsf{ord}_P(D)$$

O conjunto dos divisores de C *é representado por* Div_C *e o conjunto dos divisores de grau* 0 *(i.e., os que verificam* $(\sum_P n_P) = 0$ *) representa-se por* Div_C^0 .

Um divisor é **efectivo** *(e escreve-se* $D \geq 0$ *) se* $\mathsf{ord}_P(D) \geq 0$ *para todo* P. $D \geq D'$ *é uma abreviatura para* $D - D' \geq 0$.

Se $f \in \mathbb{K}(C)$, *o divisor de* f, *escrito como* (f) *ou* $\mathsf{div}(f)$ *é a soma formal*

$$(f) \doteq \sum_{P \in C} \mathsf{ord}_P(f)\,(P) \tag{151}$$

Divisores D *para os quais existe* $f \in \mathbb{K}(C)$ *tal que* $D = (f)$ *chamam-se* ***divisores principais***.

Como cada $f \in \mathbb{K}(C)$ tem um número finito de pólos e zeros, a soma formal (151) é um divisor.

Todo o divisor D pode ser escrito, de forma única, como $D_0 - D_\infty$ em que D_0 e D_∞ são divisores efectivos de suportes disjuntos. O par de divisores (D_0, D_∞) designa-se por **fraccionamento efectivo** de D.

235 FACTO
O conjunto dos divisores Div_C *determina um grupo abeliano que contém os divisores de ordem zero,* Div_C^0, *como sub-grupo.*

Esboço de prova Pode-se ver o conjunto dos divisores de C, Div_C embebido no espaço vectorial $\mathbb{Z}^C$: cada divisor é um vector de componentes em $\mathbb{Z}$ e com tantas componentes quantos os pontos $P \in C$. Os divisores D são, assim, os elementos de Div_C que têm um

número finito de componentes não nulas. A soma de vectores gera a operação de grupo $+$ nos divisores divisores

$$\sum_{P\in C} n_P P \;+\; \sum_{P\in C} m_P P \;\doteq\; \sum_{P\in C} (n_P + m_p)\, P \tag{152}$$

O elemento neutro é o divisor nulo $\mathcal{N} \doteq \sum_{P\in C} 0\, P$. Com tal soma e elemento neutro, Div_C tem a estrutura de um grupo.

O conjunto dos divisores de grau 0, Div_C^0 , formam um sub-grupo porque, como facilmente se verifica, a soma de dois divisores de grau zero gera de novo um divisor de grau zero.

Os divisores principais (divisores da forma $\mathrm{div}(f)$, com f uma função racional em $\mathbb{K}(C)$) têm um papel especial na teoria dos divisores.

Note-se que f é determinado por fracções homogéneas (onde o grau do numerador é igual ao grau do denominador); por isso é natural pensar-se que o número de zeros do numerador seja igual ao número de zeros do denominador.

A noção de divisor prende-se, obviamente, com a distribuição dos pólos e dos zeros das funções racionais; por isso faz sentido a seguinte definição:

236 DEFINIÇÃO
Para cada divisor $D \in \mathrm{Div}(C)$ *seja*

$$L(D) \;=\; \{0\} \cup \{\, f \in \mathbb{K}(C)^* \;\mid\; D + (f) \geq 0 \,\} \tag{153}$$

$L(D)$ contém, em primeiro lugar e como caso particular, a função constante 0; isto é essencial, como veremos adiante, para a estrutura vectorial que queremos impor a este espaço.

Essencialmente porém, $L(D)$ contém todas as funções racionais não-nulas que têm zeros que "anulam" os pólos de D e que não introduzem pólos adicionais. Note-se que, porque f é racional, o número de pólos de f deve ser igual ao número de zeros de f.

Para percebermos o papel fundamental que estes espaços $L(D)$ têm na construção de curvas, o seguinte exemplo ilustra alguns divisores e a construção do espaço respectivo.

EXEMPLO 48:

1. Vamos supor que se tem $D = (P) + (Q) - (R)$, em que $P, Q, R \in C$ são pontos distintos da curva C.

   Tome-se uma qualquer função racional f candidata pertencer a $L(D)$ com apenas um zero e um pólo; isto é, (f) tem a forma $(A) - (B)$ (com A e B por definir). Temos $D + (f) = (P) + (Q) + (A) - (R) - (B)$ e pretende-se que seja $D + (f) \geq 0$.
   Como nesta soma existem dois pólos que têm de ser anulados e os graus de liberdade são A e B, pode-se escolher $A = R$ e $B = Q$. Isto basta para que $D + (f) = (P) \geq 0$.
   Poderíamos também ter escolhido $B = P$ e obtínhamos $D + (f) = (Q) \geq 0$. Note-se que o valor de A não pode ser alterado.

Seria possível usar um $f \in L(D)$ que tivesse dois pólos e dois zeros?

$$(f) \;=\; (A) + (A') - (B) - (B')$$

Neste caso os 4 pontos A, A', B, B' têm de ser distintos e será

$$D + (f) \;=\; (P) + (Q) + (A) + (A') - (R) - (B) - (B')$$

Pode-se usar P e Q para anular B e B' e usar A ou A' para anular R.

Este é o caso limite: não existe nenhum $f \in L(D)$ com três zeros e três pólos porque D só tem 2 zeros para anular os pólos de f.

2. $D = n(P) - m(Q)$, com $n, m > 0$ e $P \neq Q$.

Considere-se uma função racional f tal que $(f) = k(A) - k(B)$. Note-se que o número de zeros tem de ser igual ao número de pólos.

Neste caso, $D + (f) = n(P) + k(A) - m(Q) - k(B)$; para este divisor ser efectivo, terá de ser

$$A = Q \quad \text{e} \quad k \geq m \quad \text{e} \quad B = P \quad \text{e} \quad k \leq n$$

Se for $n = m$ (isto é, se D tiver grau zero), então existe uma única possibilidade: f tem de ter o divisor $n(Q) - n(P) = -D$.

237 LEMA *Seja D um divisor de uma curva projectiva C e $L(D) \doteq \{ f \in \mathbb{K}(C)^* \mid D + (f) \geq 0 \} \cup \{0\}$. Então $L(D)$ é um espaço vectorial sobre $\bar{\mathbb{K}}$ cuja dimensão, denotada por $\ell(D)$, é finita.*

Prova Afirmar que $L(D)$ é um espaço vectorial é equivalente a dizer que, para todos $f, g \in L(D)$ e $a \in \bar{K}^*$, se verifica $f+g \in L(D)$ e $a\,f \in L(D)$.

Como af ou é zero (se $a = 0$) ou, se $a \neq 0$, tem os mesmos zeros e pólos que f, então $f \in L(D)$ implica $af \in L(D)$. Do mesmo modo, para todo ponto $P \in C$, a ordem $\mathrm{ord}_P(f+g)$ é sempre maior ou igual que $\mathrm{ord}_P(f)$ e $\mathrm{ord}_P(g)$. Por isso, $f, g \in L(D)$ implica $(f+g) \in L(D)$.

Provar que a dimensão do espaço vectorial é finita é mais complexo. No entanto basta recordar que, se fosse infinita, seria possível construir uma combinação linear infinita de funções racionais linearmente independentes.

238 FACTO
Se $D' = D + (h)$, para algum $h \in \mathbb{K}(C)^*$, então os espaços vectoriais $L(D)$ e $L(D')$ são isomórficos.

Prova Considere-se o morfismo $f \mapsto h\,f$ entre os espaços vectoriais $L(D')$ e $L(D)$. Como $D' = D + (h)$ então $f \in L(D')$, se não for 0, se e só se $(f) + (h) + D = (fh) + (D) \geq 0$. Portanto $f \in L(D')$ se e só se $fh \in L(D)$.

Este resultado justifica a seguinte definição

239 Definição
Dois divisores D, D' *numa curva projectiva* C *são equivalentes, e escreve-se* $D \sim D'$, *se existir* $h \in \mathbb{K}(C)$ *tal que* $D - D' = (h)$.

Esta relação (que facilmente se verifica ser uma relação de equivalência) induz um espaço quociente $\mathrm{Div}^0_C/\sim$ no conjunto de divisores de grau zero que vai ter um papel fundamental na construção das curvas elípticas. Como claramente $\mathrm{Div}^0_C/\sim$ herda de Div^0_C a estrutura do grupo abeliano, designa-se este espaço por **grupo de Picard** , normalmente representado por Pic_C .

O teorema que permite relacionar a estrutura de grupo das curvas abelianas com divisores.

240 Teorema (Riemann-Roch)
Dada uma curva projectiva absolutamente irredutível C *existe uma constante* $g \geq 0$ *tal que, para todo o divisor* $D \in \mathrm{Div}(C)$,

$$\ell(D) \geq \deg(D) + 1 - g$$

Adicionalmente, se $2g \leq \deg(D) + 1$, *verifica-se*

$$\ell(D) = \deg(D) + 1 - g \tag{154}$$

Prova A prova deste teorema requer noções que saem fora do âmbito deste trabalho. A estrutura essencial da prova (na sua forma mais recente) pode ser vista no artigo

* http://planetmath.org/encyclopedia/ProofOfRiemannRochTheorem.html.
Uma breve história do teorema e da sua importância pode ser vista em
* http://en.wikipedia.org/wiki/Riemann-Roch_Theorem.

A constante g é um invariante da curva C e designa-se por **genus** da curva. A informação essencial que resulta deste teorema é que g é independente do divisor D e a igualdade (154) verifica-se para todo o divisor cujo grau seja maior ou igual que $2\,g-1$.

Algumas consequência imediatas do teorema de Riemann-Roch

241 Proposição
Nas condições do teorema 240.

(1) Se C tem genus $g=0$ então existem pontos distintos $P\neq Q\in C$ tais que $(P)\sim(Q)$.

(2) Se C tem genus $g=1$ verifica-se $(P)\sim(Q)$ se e só se $P=Q$.

Prova Sejam P,Q dois pontos tais que $(P)\sim(Q)$ e seja $h\in\bar{\mathbb{K}}(C)$ tal que $(P)=(Q)+(h)$. Daqui conclui-se que $h\in L((Q))$ e, caso seja $P\neq Q$, o morfismo $f\mapsto hf$ estabelece um isomorfismo entre $L((P))$ e $L((Q))$ (ver lema 237). Como $(P)\geq 0$ e $(Q)\geq 0$, ambos os espaços $L((P))$ e $L((Q))$ contém a função constante 1 (já que 1 não tem zeros nem pólos).

Ambos os divisores (P) e (Q) têm grau 1. Se a curva tem genus 0, então $\deg((P))+1\geq 2g$ e a dimensão $\ell((P))=\ell((Q))$ é, pelo teorema de Riemann-Roch, igual a 2. Neste caso é possível existir $h\neq 1$ que mapeia a função $1\in L((P))$ na função $h\in L((Q))$; portanto pode ser $P\neq Q$.

Caso a curva tenha genus 1, já a dimensão $\ell((P)) = \ell((Q)) = 1$ e, por isso, tanto $L((P))$ como $L((Q))$ não podem conter outras funções que não sejam constantes; por isso h tem de ser constante e daí só pode ser $P = Q$.

242 PROPOSIÇÃO

Nas condições do teorema 240, se C tem genus 1 e um ponto $\mathcal{O}$ então existe um morfismo $\sigma : \mathrm{Div}_C^0 \longrightarrow C$ que para cada divisor $D \in \mathrm{Div}_C^0$, existe um único ponto da curva $\sigma(D)$ tal que $D \sim (\sigma(D)) - (\mathcal{O})$. Adicionalmente

(i) σ induz um isomorfismo entre o grupo de Picard Pic_C e a curva C.

(ii) $D \in \mathrm{Div}_C^0$ é principal se e só se $\sigma(D) = \mathcal{O}$.

Prova

(1) Seja D um qualquer divisor de grau 0; então $D + (\mathcal{O})$ tem grau 1 e, numa curva de genus 1, o teorema de Riemann-Roch diz-nos que $\ell(D + (\mathcal{O})) = 1$.
Seja f um gerador de $L(D + (\mathcal{O}))$. Então será simultaneamente, $\deg((f)) = 0$, porque f é racional, $\deg(D) = 0$, por hipótese, e $(f) + D + (\mathcal{O}) \geq 0$ porque $f \in L(D + (\mathcal{O}))$.
O único modo de compatibilizar estas três relações é existir um P tal que

$$(f) + D + (\mathcal{O}) \;=\; (P)$$

ou seja $D + (f) = (P) - (\mathcal{O})$ e, portanto

$$(P) - (\mathcal{O}) \;\sim\; D \tag{155}$$

Este P é único. De facto se tivermos $D \sim D'$ e $D' \sim (P') - (\mathcal{O})$, teríamos necessariamente

$$(P) - (\mathcal{O}) \sim (P') - (\mathcal{O}) \;\Rightarrow\; (P) \sim (P')$$

e, como acurva tem genus 1, tal implica (como acabámos de ver) $P = P'$.

Portanto fica bem definido uma função $\sigma : \mathrm{Div}_0(C) \to C$ que mapeia D no ponto P que verifica (155).

(2) Como consequência adicional vemos que esta construção associa dois divisores equivalentes exactamente ao mesmo ponto. Ou seja, $D \sim D'$ implica $\sigma(D) = \sigma(D')$. Por isso fica definido uma função que mapeia classes de equivalência de divisores em pontos da curva

$$\tilde{\sigma}\colon \mathrm{Pic}(C) \to C \qquad \tilde{\sigma}([D]) = \sigma(D)$$

Esta função tem uma inversa óbvia: a aplicação $\tilde{\sigma}^{-1}\colon P \mapsto [(P) - (\mathcal{O})]$ que associa um ponto $P \in C$ à classe de equivalência do divisor $(P) - (\mathcal{O})$. Assim, $\tilde{\sigma}$ é bijectiva.

(3) Se $\sigma(D) = O$ então $D \sim (\mathcal{O}) - (\mathcal{O})$. Isto significa que, para algum $f \in K(C)$,

$$D = (f) + (\mathcal{O}) - (\mathcal{O}) = (f)$$

Inversamente, se $D = (f)$, então $D + (f) = (\mathcal{O}) - (\mathcal{O})$ o que implica $D \sim (\mathcal{O}) - (\mathcal{O})$ e, por isso, $\sigma(D) = \mathcal{O}$.

243 DEFINIÇÃO

Seja C uma curva projectiva de genus 1 onde está identificado um ponto $\mathcal{O}$. Seja $\sigma\colon \mathrm{Div}^0_C \to C$ definido na proposição 242. Sejam $P, Q \in C$ pontos arbitrários da curva e $n \in \mathbb{Z}$ um inteiro arbitrário. Define-se

$$\begin{array}{lllll} P \oplus Q & = \sigma((P) + (Q) - 2(\mathcal{O})) & & -P & = \sigma((\mathcal{O}) - (P)) \\ [n]P & = \sigma(n(P) - n(\mathcal{O})) & [0]P = \mathcal{O} & [-n]P & = \sigma(n(\mathcal{O}) - n(P)) \end{array}$$

244 PROPOSIÇÃO

Nas condições da definição 243,

(i) $\langle C, \oplus, O\rangle$ *tem a estrutura de um grupo abeliano e o isomorfismo* $\mathrm{Pic}_C \tilde{\to} C$ *preserva a estrutura de grupos.*

(ii) Seja $D = \sum_{P\in C} n_P(P)$, *um divisor de grau* 0 *arbitrário; então* $\sigma(D) = \bigoplus_{P\in C} [n_P]P$.

Prova

(i) Vimos que $\tilde{\sigma}$ é uma bijecção. Esta função transforma-se num homomorfismo de grupos abelianos se, em C, se optar pela a estrutura mapeada por $\tilde{\sigma}$ a partir das operações de grupo de $\mathrm{Pic}(C)$. Isto é o que ocorre quando se define

$$P \oplus Q = \sigma((P) + (Q) - 2(\mathcal{O})) = \sigma((P) - (\mathcal{O}) + (Q) - (\mathcal{O})) = \sigma(\sigma^{-1}(P) + \sigma^{-1}(Q))$$

(ii) Note-se que a definição de $[n]P$ é equivalente a $([n]P) - (\mathcal{O}) \sim n(P) - n(\mathcal{O})$. Seja $Q \doteq \bigoplus_{P\in C} [n_P]P$. Pela definição da operação $\oplus$ temos

$$\begin{aligned}(Q) - (\mathcal{O}) \sim & \sum \left(([n_P]P) - (\mathcal{O})\right) \\ \sim & \sum n_P(P) - \sum n_P(\mathcal{O}) = D - \left(\sum n_p\right)(\mathcal{O}) = \\ = & D - 0(\mathcal{O}) \;=\; D\end{aligned}$$

Portanto temos $D \sim (Q) - (\mathcal{O})$ o que significa que $Q = \sigma(D)$.

Como consequência imediata de (ii) temos

245 COROLÁRIO *Seja C uma curva elíptica e $D = \sum_{P \in C} n_P (P)$ um qualquer divisor de grau 0. Então*

$$D \sim 0 \quad \text{sse} \quad \bigoplus_{P \in C} [n_P]P = \mathcal{O}$$

Vimos que uma função racional $f \in K(C)$ determina uma aplicação dos pontos da curva em $\bar{K}$: para cada ponto P é bem definido o valor $f(P)$.

Faz sentido tentar estender este conceito para divisores. Note-se que divisores representam, essencialmente, arranjos de zeros e de pólos de funções racionais; por isso faz sentido pensar que uma soma formal de zeros e pólos associamos o produto dos valores da função nestes pontos.

246 NOÇÃO
Seja C uma curva elíptica sobre K e $h \in K(C)$ uma qualquer função racional sobre essa curva. Para todo o divisor de grau zero $D = \sum_{P \in C} n_P (P)$ define-se

$$h(D) = \prod_{P \in C} h(P)^{n_P} \tag{156}$$

A valoração de uma função racional homogénea h num divisor de grau 0 mantém-se invariante se a função h, nos pontos da curva, sofrer uma "mudança de escala". Isto é,

247 Facto

Sejam $h, h' \in K(C)$ funções tais que, para alguma constante $\lambda \in K^*$, verifica-se $h'(P) = \lambda\, h(P)$, para todo o ponto $P \in C$. Então $h'(D) = h(D)$ para todo o divisor D de grau 0.

Prova Seja $D_0 = \sum_i n_i(P_i)$ e $D_\infty = \sum_j m_j\,(Q_j)$ (com $n_i, m_j > 0$) o fraccionamento efectivo de D. Seja k o grau destes divisores; isto é $k = \sum_i n_i = \sum_j m_j$.

$$h'(D) = \frac{\prod_i \lambda^{n_i}\, h(P_i)^{n_i}}{\prod_j \lambda^{m_j}\, h(Q_j)^{m_j}} = \frac{\lambda^{\sum_i n_i}\, \prod_i h(P_i)^{n_i}}{\lambda^{\sum_j m_j}\, \prod_j h(Q_j)^{m_j}} = \frac{\lambda^k\, \prod_i h(P_i)^{n_i}}{\lambda^k\, \prod_j h(Q_j)^{m_j}} = h(D)$$

O seguinte teorema é uma caracterização fundamental da valoração de funções racionais em divisores principais.

248 Teorema (Reciprocidade de Weil)

Seja C uma curva elíptica sobre K. Sejam $f, g \in K(C)$ funções racionais sobre C. Se o suporte de (f) e de (g) forem disjuntos, então

$$f((g)) \quad = \quad g((f))$$

□

Numa curva projectiva C de genus 1 onde está identificado um ponto específico O, são importantes os diferentes

divisores $n(\mathcal{O})$ com $n = 1, 2, \cdots$. Seja

$$L_n \;=\; L(n(\mathcal{O})) \;=\; \{\, f \in K(C) \;\mid\; (f) + n(\mathcal{O}) \geq 0 \,\} \cup \{0\}$$

Pode-se ver L_n como o espaço das funções racionais de C que não têm qualquer pólo a não ser em $\mathcal{O}$ e aí a ordem não é superior a n. Note-se que estes espaços vectoriais formam, por inclusão, uma cadeia ascendente

$$L_1 \subset L_2 \subset \cdots \subset L_n \subset \cdots$$

Como a curva tem genus 1, a dimensão de L_n é n (pelo teorema de Rieman-Roch). Portanto o espaço L_n tem n geradores linearmente independentes. Quais são estes geradores?

O espaço L_1 contém todas as funções racionais constantes e, como a sua dimensão é 1, estas definem todos os seus elementos. Deste modo não pode haver nenhuma função racional $f \in K(C)$ que tenha apenas um pólo simples em O: ou não tem qualquer pólo (e é uma constante) ou contém pelo menos outro pólo.

Portanto L_1 tem, por gerador a função unidade 1 : isto é,

$$L_1 \;=\; \{\, a\,1 \;\mid\; a \in K \,\}$$

L_2 tem dimensão 2 e contém L_1; portanto vai existir um gerador não constante g tal que

$$L_2 \;=\; \{\, a\,1 + b\,g \;\mid\; a, b \in K \,\}$$

Note-se, pelo que foi dito antes, que g tem um pólo único de ordem 2 em $\mathcal{O}$.

Considere-se, agora, L_3. Como contém L_2 e tem dimensão 3 será da forma

$$L_3 \;=\; \{\, a\,1 + b\,g + c\,h \;\mid\; a, b, c \in K \,\}$$

em que o novo gerador h é uma função racional com um pólo único de ordem 3 em $\mathcal{O}$.

Os geradores de L_3, $\{1, g, h\}$, são linearmente independentes uma vez que têm ordens dos pólos em $\mathcal{O}$ diferentes. Como consequência, este triplo define uma aplicação racional

$$[g, h, 1] \colon C \setminus \{O\} \to \mathbb{P}^2 \tag{157}$$

entre curva C e o espaço projectivo $\mathbb{P}^2$. Como g e h não têm pólos em C, para além de $\mathcal{O}$, esta aplicação é definida para todo $P \in C \setminus \{O\}$.

Escolham-se polinómios homogéneos do mesmo grau $u, v, w \in K[C]$ tais que w tem um zero triplo em $\mathcal{O}$ e mais nenhum zero em pontos de C, v/w é um representante de h e u/w é um representante de g. É possível escolher tais polinómios porque, em C, h e g só têm pólos em $\mathcal{O}$, sendo triplo o pólo de h e duplo o pólo de g. Assim, em $\mathcal{O}$, u tem de ter um zero simples (já que o pólo de g em $\mathcal{O}$ tem ordem 2) e v não tem nenhum zero.

Define-se agora $\varphi\colon C \longrightarrow \mathbb{P}^2$ por este triplo de polinómios

$$\varphi = [u, v, w] \quad \text{com} \quad g = [u/w] \ , \ h = [v/w] \tag{158}$$

249 LEMA *φ definido em* (158) *é um morfismo injectivo* $\varphi\colon C \longrightarrow \mathbb{P}^2$ *tal que* $\varphi(\mathcal{O}) = P_\infty$ *e, para* $P \neq \mathcal{O}$, $\varphi(P) = [g(P), h(P), 1]$.

Prova Se $P = \mathcal{O}$ tem-se $\varphi(P) = [u(\mathcal{O}), v(\mathcal{O}), w(\mathcal{O})] = [0, v(\mathcal{O}), 0] = [0, 1, 0] = P_\infty$. Se $P \neq \mathcal{O}$ tem-se $w(P) \neq \mathcal{O}$ e, por isso, $\varphi(P) = [u(P), v(P), w(P)] = [u(P)/w(P), v(P)/w(P), 1] = [g(P), h(P), 1]$. Resta provar que ϕ é injectivo. Vamos supor que existiam dois pontos $P \neq Q$ tais que $\varphi(P) = \varphi(Q)$. Então necessariamente, para qualquer $f \in L_3$, seria $f(P) = f(Q)$ já que f é uma combinação linear de g e h. Tome-se agora um qualquer ponto $A \in C$ distinto de O, P ou Q e considere-se duas funções distintas $u, v \in L_3$ que partilhem o mesmo zero A. Então, como $u(P) = u(Q)$ e $v(P) = v(Q)$, a função racional $(u - v)$ pertence a L_3 e tem zeros em A, P e Q; logo $(A) + (P) + (Q) \sim 3(\mathcal{O})$; como A é arbitrário , isto não é possível. Consequentemente, φ é um morfismo injectivo.

O seguinte lema estabelece uma relação particular entre divisores de C efectivos de ordem 3 e rectas em $\mathbb{P}^2$.

250 LEMA *Seja* $D \geq 0$ *um divisor efectivo sobre* C *de grau* 3 *que verifica* $D \sim 3(\mathcal{O})$. *Então* φ, *definido em* (158), *mapeia todos os pontos de* C *de ordem não nula em* D *sobre uma mesma recta de* $\mathbb{P}^2$.

Prova Seja f tal que $D = (f) + 3(\mathcal{O})$; porque $D \geq 0$, a função f é um elemento de $L_3 = L(3(\mathcal{O}))$. Então f pode-se escrever como uma combinação linear dos geradores $\{1, g, h\}$; isto é, $f = ag + bh + c$ para alguns $a, b, c \in K$.

Seja $\mathbf{l}$ a recta em $\mathbb{P}^2$ determinada pelo polinómio $aX + bY + cZ$. Como, para todo $P \in C$, se tem $\mathbf{l}(\varphi(P)) = f(P)$, concluímos que P é um zero de f se e só se $\varphi(P)$ for um ponto da recta $\mathbf{l}$. Mas os zeros de f são precisamente os pontos de C que têm ordem não nula em D. Portanto todos os pontos de ordem não nula de D são pontos da recta $\mathbf{l}$.

A partir dos geradores $\{1, g, h\}$ de L_3 constrói-se os geradores dos espaços seguintes. Por exemplo, g^2 tem um pólo único de ordem 4 em $K(C)$; mais nenhum polinómio construído com estas 3 funções tais pólos. Logo os geradores de L_4 são $\left\{1, g, h, g^2\right\}$.

Da mesma forma se conclui que $g\,h$ tem um pólo único de ordem 5 em $\mathcal{O}$ e mais nenhuma combinação polinomial das três funções tem tais pólos. Logo os geradores de L_5 são $\left\{1, g, h, g^2, g\,h\right\}$.

Quando se chega a L_6, porém, algo de novo ocorre. Pode-se construir o pólo de ordem 6 de dois modos diferentes: ou com g^3 ou, então, com h^2. Desta forma existem 7 candidatos a geradores, $\left\{1, g, h, gh, g^2, g^3, h^2\right\}$. Como o espaço só tem dimensão 6, as 7 funções não podem ser linearmente independentes. Como as 5 primeiras têm de pertencer à base de geradores (porque são geradores de L_5), então h^2 (ou g^3) devem ser representáveis como combinação linear dos restantes 6 elementos.

Por isso tem de existir coeficientes $c_i \in K$ tais que

$$h^2 = g^3 + c_4 g\,h + c_3 g^2 + c_2 h + c_1 g + c_0 \tag{159}$$

O coeficiente de g^3 tem de ser $\neq 0$ porque não seria possível, de outra forma, que esta igualdade se verificasse e que h^2 tivesse o pólo de ordem 6 no ponto $\mathcal{O}$; sendo assim, pode-se assumir que o coeficiente é 1.

Tradicionalmente esta equação escreve-se (usando uma outra sequência de coeficientes) de forma algo diferente

$$h^2 + a_1 g\, h + a_3 h = g^3 + a_2 g^2 + a_4 g + a_6 \tag{160}$$

que se designa por **forma de Weierstraß**. Isto permite-nos enunciar um segundo lema

251 LEMA *Seja E a curva em $\mathbb{P}^2$ determinada pelo polinómio*

$$\phi = Y^2\, Z + a_1\, X\, Y\, Z + a_3\, Y\, Z^2 - X^3 - a_2\, X^2\, Z - a_4\, X\, Z^2 - a_6\, Z^3 \tag{161}$$

E é uma curva não-singular e φ definido no lema 249 é um isomorfismo entre C e E

Prova Substituindo h por v/w e g por u/w a igualdade (160) pode-se escrever

$$v^2\, w + a_1\, u\, v\, w + a_3\, v\, w^2 - u^3 - a_2\, u^2 w - a_4\, u\, w^2 - a_6\, w^3 \;=\; 0$$

Isto é equivalente à afirmação de que $\phi(\varphi(P)) = 0$ para todo o ponto P da curva; portanto φ, definido no lema 249, é um morfismo de C para E. O referido lema diz-nos que φ é um isomorfismo entre C e a sua imagem; como é surjectivo, concluímos que a imagem tem de coincidir com E e que φ é um isomorfismo entre C e E.

A consequência essencial destes lemas é

252 TEOREMA
Qualquer curva elíptica C/K sobre o espaço projectivo $\mathbb{P}^2$ é isomórfica com uma curva plana não singular determinada por uma polinómio $\phi \in \mathbb{K}[X,Y,Z]$ da forma (161).

No que se segure C/K é uma curva de genus 1 em $\mathbb{P}^2$ com ponto identificado $\mathcal{O}$.

253 COROLÁRIO *As funções racionais $g = x/z$ e $h = y/z$ são geradores g e h de L_3.*

Como consequência do lema 250 tem-se ainda,

254 LEMA *Seja $\langle C, \oplus, \mathcal{O}\rangle$ a estrutura de grubo abeliano definido em C (definição 243). Então os pontos P, Q e R de C são mapeados por φ em pontos sobre uma mesma recta de $\mathbb{P}^2$ se e só se $-R = P \oplus Q$.*

Prova Seja D o divisor $(P)+(Q)+(R)$ que é efectivo e tem grau 3. Pela definição das operações de grupo tem-se $(P)+(Q)-2(\mathcal{O}) \sim (\mathcal{O})-(R)$ o que é equivalente a ser $D = (P)+(Q)+(R) \sim 3(\mathcal{O})$. Pelo lema 250 tem-se $D \sim 3(\mathcal{O})$ se e só se os pontos P, Q e R são mapeados em pontos sobre uma mesma recta de $\mathbb{P}^2$.

O seguinte lema é verdadeiramente "multiusos"

255 LEMA *Sejam P, Q, R, S pontos de C tais que tanto P como Q são distintos de R ou S e tais que $P \oplus Q = R \oplus S$.*

(i) *Se* $P \neq Q$ *seja* $p = \mathbf{l}(P \otimes Q)$ *a recta que passa pelos pontos* P *e* Q*. Se for* $P = Q$ *seja* $p = \mathbf{l}(\mathcal{J}^C(P))$ *a recta tangente à curva em* P*.*

(ii) *Se* $R \neq S$ *seja* $q = \mathbf{l}(R \otimes S)$ *a recta que passa pelos pontos* R *e* S*. Se for* $R = S$ *seja* $q = \mathbf{l}(\mathcal{J}^C(R))$ *a recta tangente à curva em* R*.*

Então $(P) + (Q) = (R) + (S) + (p/q)$*.*

Prova

1. No caso em que todos os pontos são distintos. Pelo lema 250 a recta $p = \mathbf{l}(P \otimes Q)$ verifica $(p) = (P)+(Q)+(-(P \oplus Q))-3(\mathcal{O})$. Pela mesma razão a recta $q = \mathbf{l}(R \otimes S)$ verifica $(q) = (R) + (S) + (-(R \oplus S)) - 3(\mathcal{O})$. Dado que, por hipótese, se tem $P \oplus Q = R \oplus S$ conclui-se que $(p/q) = (p) - (q) = (P) + (Q) - (R) - (S)$.
2. Se $P = Q$, e pelo mesmo motivo, a recta p verifica $(p) = 2(P) + (-(P \oplus P)) - 3(\mathcal{O})$. O resto da prova é idêntica.

Quando $S = P \oplus Q$, $R = \mathcal{O}$ a função racional p/q é determinada por P e Q (a menos da multiplicação por uma constante) e faz sentido representá-la por um símbolo apropriado. Assim

256 NOÇÃO

Dados pontos P, Q *numa curva elíptica* C *com ponto no infinito* $\mathcal{O}$*; Define-se* $\mu(P, Q) = p/q$ *em que o par de rectas* p *e* q *é dado por:*

(i) *Se* $P \neq Q$ *então* $p = \mathrm{l}(P \otimes Q)$ *é a recta que passa pelos pontos* p *e* Q.

(ii) *Se* $P = Q$, *então* $p = \mathrm{l}(\mathcal{J}^C(P))$ *é a recta tangente à curva em* P.

(iii) *Se* $P \neq -Q$ *então* $q = \mathrm{l}((P \oplus Q) \otimes \mathcal{O})$.

(iv) *Se* $P \oplus Q = \mathcal{O}$ *então* $q = \mathrm{l}(\mathcal{J}^C(\mathcal{O}))$ *é a recta tangente à curva em* $\mathcal{O}$.

257 PROPOSIÇÃO
Para todo $P, Q \in C$ *verifica-se* $(\mu(P, Q)) = (P) + (Q) - (P \oplus Q) - (\mathcal{O})$.

Prova Consequência imediata do lema 255.

EXEMPLO 49: Considere-se uma curva elíptica sobre o corpo $\mathbb{Q}$ aqui determinada pela sua parte afim

$$E\colon y^2 = x^3 - x + 1$$

Nessa curva tomemos por referência um "ponto central" R de coordenadas afins $(0, 1)$.

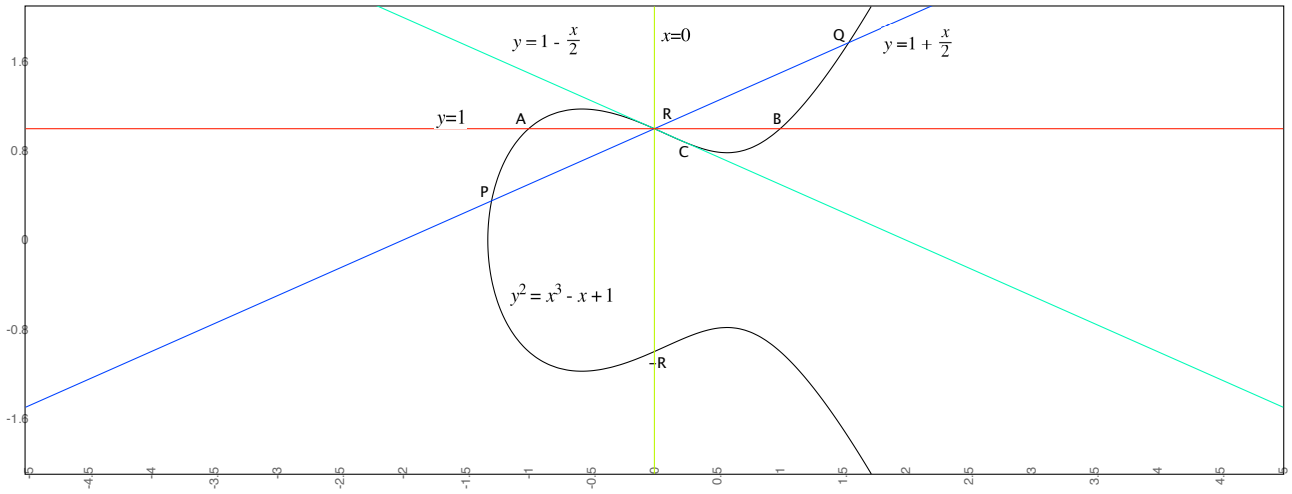


Figura 7: Rectas sobre uma curva elíptica

Vamos considerar a família das rectas que passam por este pontos, como se ilustra na figura 7. Contando com o ponto no infinito P_∞ cada uma das rectas "intersecta" a curva em mais outros 2 pontos.

Na figuras estão indicadas 4 dessas rectas:

1. Uma recta $y = 1 + \frac{x}{2}$ que intersecta a curva em outros dois pontos que designaremos por P e Q.

A recta é determinada pelo polinómio homogéneo

$$x - 2y + 2z$$

que, como elemento de $K[C]$, tem zeros precisamente nesses três pontos. Portanto

$$(x - 2y + 2z) \;=\; (P) + (R) + (Q)$$

Resolvendo o sistema de equações definido pela recta e pela equação da curva pode-se calcular as coordenadas de P e Q. Verifica-se facilmente que

$$P = [\frac{1 - \sqrt{129}}{8} \;,\; \frac{15 + \sqrt{129}}{16} \;,\; 1] \qquad Q = [\frac{1 + \sqrt{129}}{8} \;,\; \frac{17 + \sqrt{129}}{16} \;,\; 1]$$

2. Uma recta $y = 1$ que intersecta a curva em outros dois pontos A e B.
   Em coordenada projectivas o polinómio homogéneo definidor da recta é

$$y - z$$

e os pontos A e B têm coordenadas $[-1, 1, 1]$ e $[1, 1, 1]$ respectivamente. Neste caso temos

$$(y - z) \;=\; (A) + (R) + (B)$$

3. Uma recta $x = 0$ que intersecta a curva (para além de R) no ponto $-R = [0, -1, 1]$ e no ponto do infinito $P_\infty = [0, 1, 0]$.
   O polinómio homogéneo que define esta recta é simplesmente x. Por isso tem-se

$$(x) \;=\; (R) + (-R) + (P_\infty)$$

4. Finalmente temos uma recta $y = 1 - \frac{x}{2}$ que é tangente à curva no ponto R.
   Isto equivale a dizer que o polinómio homogéneo correspondente

$$x + 2y - 2z$$

   tem um zero duplo em R. Resolvendo o sistema de equações verifica-se que tem um terceiro zero no ponto C de coordenadas $[1/4, 7/8, 1]$. Por isso

$$(x + 2y - 2z) \;=\; 2(R) + (C)$$

A soma dos três pontos de uma curva elíptica que estão sobre uma mesma recta é sempre P_∞. Em cada uma destas 4 rectas, um dos pontos é sempre R; logo, a soma dos dois restantes tem de ser constante e igual a $-R$.

$$P \oplus Q = A \oplus B = R \oplus C = -R \oplus P_\infty = -R$$

Combinando as rectas duas a duas construímos várias funções racionais e determinamos os respectivos divisores; por

exemplo

$$\left(\frac{x-2y+2z}{y-z}\right) = (P)+(Q)-(A)-(B)$$

$$\left(\frac{x-2y+2z}{x}\right) = (P)+(Q)-(-R)-(P_\infty)$$

$$\left(\frac{x+2y-2z}{y-z}\right) = (R)+(C)-(A)-(B)$$

etc $\cdots$

8.4 Isogenias e Grupos de Torsão

Vamos continuar a considerar curvas projectivas de genus 1 com um ponto $\mathcal{O}$ definidas no espaço projectivo $\mathbb{P}^2$ gerado por um corpo finito K. Uma tal curva genérica, que designamos por **curva elíptica**, é representada por E/K.

No que se segue vamos sempre assumir que o corpo K é finito e, por isso, o número de pontos de E/K, representado por $|E/K|$ é finito.

Vimos que estas curvas estava definida uma estrutura de um grupo abeliano $\langle E/K, \oplus, \mathcal{O}\rangle$, com a operação do grupo apresentada na definição 243 (ver página 514). Temos, por isso, um grupo abeliano finito.

O objectivo do uso de curvas elípticas em Criptografia reside na possibilidade de construção de grupos cíclicos que sejam sub-grupos deste grupo finito. Para isso vamos considerar o **produto escalar** também apresentado na definição atrás referida.

Nessa mesma definição, para cada $n \in \mathbb{Z}$, definimos uma função $[n]\colon E/K \to E/K$ que mapeia um ponto genérico $P \in E/K$ num ponto $[n]\,P$.

Não é difícil verificar que esta função preserva a estrutura do grupo abeliano. Isto é $[n]\,(P \oplus Q) = [n]\,P \oplus [n]\,Q$ e $[n]\,\mathcal{O} = \mathcal{O}$. De facto esta função pertence a uma classe de transformações entre pontos que se designa por **isogenias** que, por seu lado, estão dentro da classe dos **homomorfismos** de curvas.

258 NOÇÃO

Dada uma curva elíptica $C = E/K$ *uma* **aplicação racional** *é um triplo de polinómios homogéneos do mesmo grau* $\phi = [\phi_1, \phi_2, \phi_3] \in \overline{\mathbb{K}}\,[x, y, z]^3$ *em que pelo menos um deles não pertence a* I_C .

A aplicação ϕ *é equivalente à aplicação* $\psi = [\psi_1, \psi_2, \psi_3]$, *e escreve-se* $\phi \cong \psi$, *quando,*

$$\phi_i\,\psi_j - \phi_j\,\psi_i \;\in\; I_{E/K} \qquad \textit{para todo} \quad i, j \in 1, 2, 3$$

As classes de equivalência definidas no espaço das aplicações racionais pela relação de equivalência $\cong$, *formam a espaço dos* **homomorfismos** $\mathrm{Homo}(C)$.

É fácil verificar que, dado um qualquer ponto da curva $P \in C$, cada homomorfismos $\phi \in \mathrm{Homo}(C)$ associa P a um ponto bem definido do espaço $\mathbb{P}^2$. Para a determinação desse ponto é indiferente qual a aplicação racional que se escolhe (dentro da mesma classe) ou qual o triplo de coordenadas que usamos para P. Fica definida assim uma função $\phi\colon C \longrightarrow \mathbb{P}^2$.

Interessa-nos estender esta noção da definir homomorfismos entre duas curvas elípticas. Temos assim

259 NOÇÃO

No seguimento da definição 258 seja C' *for uma segunda curva elíptica sobre o mesmo corpo* K. *Um homomorfismo* ϕ *determina um* **homomorfismo de curvas** *se se verifica* $\phi(P_\infty) = P_\infty$ *e*

$$p(\phi_1(x, y, z)\ ,\ \phi_2(x, y, z)\ ,\ \phi_3(x, y, z)) \in I_C \qquad \textit{para todo} \quad p \in I_{C'} \tag{162}$$

O conjunto dos homomorfismos entre C *e* C' *representa-se por* $\mathsf{Homo}(C, C')$.

Se $\phi \in \mathsf{Homo}(C, C')$ *é surjectivo então designa-se por* **isogenia** *entre curvas.*

As condições aqui impostas, para além de assegurar que o ponto no infinito seja sempre mapeado no ponto no infinito, asseguram que qualquer ponto $P \in C$ é mapeado num ponto $\phi(P) \in C'$.

O resultado fundamental, que se pode provar recorrendo aos divisores, é

260 TEOREMA
Se $\phi \colon C \to C'$ *é uma isogenia entre curvas elípticas* C *e* C' *então* ϕ *preserva a estrutura dos grupos abelianos.*

Vimos que as funções $[n]\cdot \colon C \to C$ são isogenias dentro da mesma curva C. Um outro exemplo particularmente importante de isogenia é a **isogenia de Frobenius**.

Recordemos que K é um corpo finito, por hipótese. Assim terá a forma $K = \mathbb{F}_{p^d}$ em que o primo p é a sua característica e d a sua sua dimensão. Recordemos que a função $\sigma_p \colon x \mapsto x^p$ é designada por **morfismo de Frobenius** no corpo K e é um endomorfismo (preserva a estrutura algébrica e é um isomorfismos) que fixa os elementos de $\mathbb{F}_p$ nesse corpo.

□

No que se segue vamos considerar uma curva elíptica $C = E/K'$ definida numa extensão K' de K. Note-se que K' continua a ter característica p e o polinómio que determina a curva é um elemento de $K[x, y, z]$.

A **isogenia de Forbenius** estende este morfismo aplicando σ_p componente-a-componente. Ou seja

$$\sigma_p : (x, y, z) \mapsto (x^p , y^p , z^p) \tag{163}$$

Não é verdade, normalmente, que σ_p seja uma isogenia de uma curva C para a mesma curva C. No entanto é fácil construir uma segunda curva C' de tal forma que σ_p seja uma isogenia entre estas duas curvas.

EXEMPLO 50: Suponhamos que $K = \mathbb{F}_{2^n}$ é um corpo de característica 2 e que que C é uma curva elíptica cuja componente afim é determinada pelo polinómio

$$y^2 + x\,y + x^3 + \upsilon \qquad \text{com} \quad \upsilon \in K$$

Se for $y^2 + x\,y + x^3 + \upsilon = 0$, elevando ao quadrado temos

$$(y^2)^2 + (x^2)\,(y^2) + (x^2)^3 + \upsilon^2 = 0$$

Então, se (x, y) define uma raiz do polinómio original, o par (x^2, y^2) define uma raiz do polinómio $y^2 + x\,y + x^3 + \upsilon^2$ que é idêntico ao anterior excepto no facto de a constante μ ser substituída por μ^2.

Porém, considerando $K = \mathbb{F}_p$ e atendendo que E/K' é definida por um polinómio $p \in \mathbb{F}_p[x, y, z]$ (i.e, todos os coeficientes do polinómio pertencem a $\mathbb{F}_p$), então, dado que σ_p fixa os elementos de $\mathbb{F}_p$, a isogenia de Frobenius

$(x, y) \mapsto (x^p, y^p)$ preserva o polinómio. Por isso σ_p é, neste caso, uma **endo-isogenia** ; isto é, uma isogenia da curva C para, de novo, a curva C.

Uma generalização simples consiste em considerar o homomorfismo σ_P^d (a potência de ordem d da isogenia de Frobenius). Neste caso qualquer polinómio $p \in K[x, y, z]$ é fixado por esta aplicação e, por isso, ela define uma endo-isogenia.

Note-se que, como as coordenadas x, y estão contidas na extensão K', elas não são fixadas pelo morfismo; por isso, normalmente, será $(x, y) \neq (x^{p^d}, y^{p^d})$.

EXEMPLO 51: Neste exemplo vamos usar curvas elípticas sobre o corpo $\mathbb{F}_4$ e sobre a sua extensão $\mathbb{F}_{16}$. Para determinar os elementos de $\mathbb{F}_4$ usaremos polinómio característico $\beta^2 + \beta + 1$. Assim os elementos de $\mathbb{F}_4$ serão $\{0, 1, \beta, 1 + \beta\}$.

Considere-se agora a curva $E/\mathbb{F}_4 : y^2 + x\,y + x^3 + 1$.

Pode-se verificar que esta curva tem 7 pontos afins, para além do ponto no infinito P_∞. São eles

$$\{ (0, 1) \ , \ (1, 0) \ , \ (1, 1) \ , \ (\beta, 0) \ , \ (\beta, \beta) \ , \ (\beta + 1, 0) \ , \ (\beta + 1, \beta + 1) \}$$

O morfismo de Frobenius é, neste caso, $x \mapsto x^2$. Notando que $\beta^2 = \beta + 1$ e que $(\beta + 1)^2 = \beta$ neste corpo, a

isogenia de Frobenius $(x, y) \mapsto (x^2, y^2)$ mapeia os pontos da lista anterior, respectivamente, em

$$\{ (0,1) \ , \ (1,0) \ , \ (1,1) \ , \ (\beta+1, 0) \ , \ (\beta+1, \beta+1) \ , \ (\beta, 0) \ , \ (\beta, \beta)\}$$

Portanto, neste caso, a isogenia mapeia pontos da curva em pontos da mesma curva.

Considere-se agora uma outra curva $E/\mathbb{F}_4 : y^2 + x\,y + x^3 + \beta$.

Os seus pontos afins são apenas

$$\{(0, \beta+1) \ , \ (\beta, 1) \ , \ (\beta, \beta+1)\}$$

A isogenia de Frobenius $(x, y) \mapsto (x^2, y^2)$ estabelece-se entre esta curva e a curva $E/\mathbb{F}_4 : y^2 + x\,y + x^3 + (\beta+1)$ cujos pontos são

$$\{(0, \beta) \ , \ (\beta+1, 1) \ , \ (\beta+1, \beta)\}$$

□

Vamos agora considerar curvas sobre a extensão $\mathbb{F}_{16}/\mathbb{F}_4$ usando o polinómio característico $\alpha^4 + \alpha + 1$.

A imersão de $\mathbb{F}_4$ em $\mathbb{F}_{16}$ faz-se pelo morfismo que mapeia $\beta \mapsto \alpha^2 + \alpha$; de facto, calculando $\beta^2 + \beta + 1$ tem-se

$$\beta^2 + \beta + 1 \quad \to \quad (\alpha^4 + \alpha^2) + (\alpha^2 + \alpha) + 1 \quad \to \quad \alpha^4 + \alpha + 1 \quad \to \quad 0$$

Vamos considerar, nesta extensão, curvas definidas pelos dois polinómios considerados atrás (tendo em atenção a substituição $\beta \longrightarrow \alpha^2+\alpha$). É óbvio que as curvas $E/\mathbb{F}_{16} : y^2+x\,y+x^3+1$ e $E/\mathbb{F}_{16} : y^2+x\,y+x^3+(\alpha^2+\alpha)$ contêm todos os pontos das curvas correspondentes em $\mathbb{F}_4$ e ainda alguns pontos adicionais.

A componente afim de $E/\mathbb{F}_{16} : y^2 + x\,y + x^3 + 1$ contém 15 pontos em vez dos 7 pontos em $\mathbb{F}_4$

$(0,1)$, $(1,0)$, $(1,1)$, $(\alpha^3, \alpha^2+\alpha+1)$, $(\alpha^3, \alpha^3+\alpha^2+\alpha+1)$, $(\alpha^2+\alpha, 0)$, $(\alpha^2+\alpha, \alpha^2+\alpha)$, $(\alpha^3+\alpha^2, \alpha^2+\alpha)$, etc

Na componente afim de $E/\mathbb{F}_{16} : y^2 + x\,y + x^3 + \alpha^2 + \alpha$ a diferença é mais substancial; em vez dos 3 pontos em $\mathbb{F}_4$ tem-se 23 pontos em $\mathbb{F}_{16}$.

Ambos os polinómios mantêm-se invariantes pela transformação $x \mapsto x^4$; por isso o morfismo $(x, y) \mapsto (x^4, y^4)$ é uma endo-isogenia.

Regressemos às isogenias sobre uma curva elíptica $E/K : \phi$, com $\phi \in K_0[x, y, z]]$ e K um extensão K/K_0 . Seja p a característica de K_0 (e também de K).

261 NOÇÃO
O núcleo de $[n]\colon E/K \longrightarrow E/K$ *(isto é, o conjunto* $\{\, P \in E/K \mid [n]P = \mathcal{O} \,\}$*) é representado por* $E/K[n]$ *e designa-se por* **grupo de torção de** E/K **de ordem** n*. Os pontos de* $E/K[n]$ *designam-se por* K-**pontos de torção** *de ordem* n*.*

O seguinte resultado é fundamental ao nosso estudo.

262 TEOREMA

Se K é algebricamente fechado e a característica p é primo relativamente a n, então $E/K[n] \simeq \mathbb{Z}_n \times \mathbb{Z}_n$. Se $n = p^s$, para algum $s \geq 1$, então um de dois casos ocorre: ou $E/K[n] = \{\mathcal{O}\}$ ou então $E/K[n] \simeq \mathbb{Z}_{p^s}$.

Se ocorrer a primeira hipótese $E/K[p^s] = \{\mathcal{O}\}$, a curva diz-se **super-singular** e esta propriedade é independente do valor de s. No caso contrário ($E/K[p^s] \simeq \mathbb{Z}_{p^s}$) a curva diz-se **ordinária**.

É importante notar-se que este teorema exige que K coincida com $\bar{K_0}$ (o fecho algébrico do corpo onde característica p onde o polinómio gerador ϕ está definido). Quando K é uma outra qualquer extensão de K_0, contida em $\bar{K_0}$, o K-grupo de torção tem, naturalmente, menos pontos.

Obviamente, se escolhermos um qualquer $P \neq \mathcal{O} \in E/K[n]$, qualquer ponto $Q = [k]P$ continua a ser um elemento $E/K[n]$. Por isso a órbita de P é um sub-grupo cíclico de $E/K[n]$.

Sabe-se, da teoria genérica dos grupos de torção, que $E/K[n]$ é a soma directa dos seus subgrupos primos. Isto é a soma directa de subgrupos de ordem da forma q^s, sendo q um primo. Nomeadamente em criptografia são extremamente importantes os sub-grupos de ordem prima dos grupos de torção.

8.5 Aritmética nas Curvas Elípticas

Vimos na secção anterior que uma **curva elíptica** sobre o corpo $\mathbb{K}$ é determinada, em coordenadas afins, por um polinómio $\phi \in \overline{\mathbb{K}}[x, y]$ da forma de Weitstraß que, de forma simplificada, se pode escrever

$$\phi = y^2 + y\,h(x) + f(x) \tag{164}$$

com $h, g \in \mathbb{K}[x]$ sendo $\deg(h) \leq 1$ e $\deg(f) = 3$ de tal forma que as derivadas $\partial\phi/\partial x$ e $\partial\phi/\partial y$ não se anulam simultâneamente.

Vimos também que as raízes deste polinómio definem a chamada **parte afim** da curva. Existe ainda um outro ponto da curva, que representamos por P_∞ ou $\mathcal{O}$, que completa a curva e que não pertence à parte afim.

□

Sendo $h = a_1\,x + a_3$ e $f = x^3 + a_2\,x^2 + a_4\,x + a_6$, a condição de não anulação simultânea das derivadas parciais ocorre se e só se

$$16\,{a_2}^2 - 8\,a_2{a_1}^2 + {a_1}^4 - 48\,a_4 + 24\,a_1a_3 \;<\; 0$$

Se $\mathbb{K}$ tem característica diferente de 2 ou 3 então, através de substituição de variáveis $y \leftarrow 2\,y + h$ e $f \leftarrow f - h^2/4$, transforma a forma genérica de Weitsrass em (164) simplificando-a em

$$\phi = y^2 + f(x) \tag{165}$$

Se $\mathbb{K}$ tem característica 3 a mudança de variáveis $y \leftarrow y + h$ e $f \leftarrow f + h^2$ conduz à mesma forma equivalente $\phi = y^2 + f(x)$. Em ambos os casos ϕ define uma curva elíptica se e só se f não tem raízes múltiplas; isto é, todas as raízes de f têm de ser distintas.

Quando a característica do corpo K é 2, a forma de Weierstraß pode ainda ser simplificada. Para isso vamos definir $\xi \doteq \partial h/\partial x$. Como h tem grau 0 ou 1, o valor ξ é um elemento de $\mathbb{K}$ que pode ser nulo (se h tiver grau 0) ou não. Vamos considerar separadamente estes dois casos.

$\xi = \partial h/\partial x = 0$ Estas curvas dizem-se **super-singulares**.

Neste caso $h(x)$ é uma constante e, escrevendo $f(x) = x^3 + a\,x^2 + b\,x + c$, pode-se efectuar a mudança de variáveis $x \leftarrow x + a$, $\mu = a^2 + b$, $\upsilon = ab + c$ que conduz à curva equivalente

$$\phi = y^2 + hy + x^3 + \mu x + \upsilon \tag{166}$$

Nesta curva tem-se $\partial\phi/\partial y = h$ e a curva será não-singular (isto é, ϕ determina uma curva elíptica) se e só se for $h \neq 0$.

$\xi = \partial h/\partial x \neq 0$ Neste caso tem-se $h(x) = \kappa + \xi\,x$. A curva diz-se **ordinária**.

Usando a mesma representação de f existe uma mudança de variáveis que conduz à forma simplificada,

$$\phi = y^2 + xy + x^3 + \mu x^2 + \upsilon \tag{167}$$

Aqui $\partial\phi/\partial x = y + x^2$ e $\partial\phi/\partial y = x$. Isto significa que a curva é não-singular desde que não contenha o ponto $(0,0)$.

Para as curvas ordinárias existe ainda uma simplificação adicional. Suponhamos que se toma $c = \mu$ ou o seu complemento $c = 1 + \mu$ consoante o traço de μ é 0 ou 1. Em qualquer dos casos tem-se $\mathrm{Tr}(c) = 0$.

Neste caso a equação $\lambda^2 + \lambda + c = 0$ tem solução. A mudança de variáveis $y \mapsto y + \lambda\, x$ conduz à curva equivalente

$$\phi' \;=\; y^2 + xy + x^3 + (c+\mu)\, x^2 + \upsilon$$

Escolhendo $c = \mu$ ou $c = 1 + \mu$ obtém-se as curvas

$$\begin{aligned} \phi &= y^2 + xy + x^3 + \upsilon \qquad \text{ou} \qquad (168)\\ \phi &= y^2 + xy + x^3 + x^2 + \upsilon \end{aligned}$$

que são as formas mais genéricas de curvas ordinárias em corpos de característica 2. Qualquer destas formas pode ser adoptada escolhendo uma ou outra consoante se pretende um coeficiente de x^2 com traço 0 ou com traço 1.

□

Na secção anterior vimos que as curvas elípticas $E/\mathbb{K}$ se identificam, no contexto geral do estudas das curvas

planas, com as curvas de genus 1 que têm um ponto identificado $\mathcal{O}$. Desta interpretação resultaram, na secção anterior, dois resultados essenciais sobre a estrutura algébrica das curvas elípticas:

1. Em primeiro lugar a proposição 244 (ver pag. 514) identifica em cada curva $E/\mathbb{K}$ a estrutura de um grupo abeliano $\langle E/\mathbb{K} \ , \ \oplus \ , \ \mathcal{O} \rangle$.
2. Em segundo lugar que a operação de grupo $\oplus$ tem uma simples interpretação geométrica; o lema 254 diz-nos que, se for $S = P \oplus Q$ então $P, Q, -S$ estão sobre uma mesma recta (são colineares). O mesmo lema diz-nos também que, para todo ponto P, o triplo de pontos $P, -P, \mathcal{O}$ também está sempre sobre uma mesma recta. Se P tiver coordenadas $[P_1, P_2, P_3]$, tem-se $P \otimes \mathcal{O} = [P_3, 0, -P_1]$ e a recta respectiva será $xP_3 - zP_1$

Esta interpretação geométrica permite facilmente encontrar fórmulas explícitas para calcular as coordenas afins de $P \oplus Q$ e de $-P$ em função das coordenadas afins de P e Q. Assumimos a forma genérica de Weierstraß em coordenadas afins

$$y^2 + a_1\, x\, y + a_3\, y - x^3 - a_2\, x^2 - a_4\, x - a_6 \tag{169}$$

1. **Determinar $-P$**
   Se P tem coordenadas afins $[p_1, p_2]$ então a recta $\mathbf{l}(P \otimes \mathcal{O})$ é $xp_3 - zp_1$.
   O terceiro ponto de intersecção com a curva é $-P$. Atendendo a que P pertence à curva, verifica-se que

$$-P \ = \ (p_1, -\mu) \qquad \text{sendo} \quad \mu = p_2 + a_1\, p_1 + a_3 \tag{170}$$

2. **Determinar $P \oplus Q$**
   Sekam $P = (p_1, p_2)$ e $Q = (q_1, q_2)$ as coordenadas afins dos pontos.
   Determina-se a recta $p = \mathbf{l}(P \oplus Q)$ que passa por P e Q. Caso seja $P = Q$ essa recta é a tangente à curva em P. Determina-se o terceiro ponto R de intersecção da recta com a curva e faz-se $P \oplus Q = -R$.
   Temos duas situações para cálculo do declive λ da recta p.

$$\lambda = (p_2 - q_2)/(p_1 - q_1) \qquad \text{quando} \quad P \neq \pm Q \tag{171}$$

$$\lambda = (3\,p_1^2 + 2\,a_2\,p_1 + a_4 - p_2)/(2\,p_2 + a_1\,p_1 + a_3) \qquad \text{quando} \quad P = Q \tag{172}$$

   Então

$$P \oplus Q = (\,\eta\ ,\ \lambda\,(p_1 - \eta) - \mu\,) \tag{173}$$

$$\text{sendo} \quad \eta = \lambda^2 + a_1\,\lambda - a_2 - p_1 - p_2 \qquad \text{e} \qquad \mu = p_2 + a_1\,\eta + a_3$$

Esta é a forma mais geral para determinar o valor da soma $P \oplus Q$. Consoante a carcaterística do corpo K e as formas simplificadas de curvas que daí resultam várias simplificações e optimizações são possíveis.

8.6 Emparelhamentos de Tate e Weil

Sejam G_1, G_2 dois sub-grupos de curvas elípticas ambos de expoente n; isto é, para todo $p \in G_1, G_2$ tem-se $[n]P = \mathcal{O}$. Considere-se ainda um grupo cíclico Γ de ordem n escrito de forma multiplicativa. Recordemos que

263 NOÇÃO

Um **emparelhamento** *é uma função* $e\colon G_1 \times G_2 \to \Gamma$ *que é*

- ***bilinear:*** *para todo* $P, P' \in G_1$ *e* $Q, Q' \in G_2$ *tem-se* $e(P \oplus P', Q) = e(P,Q) \cdot e(P',Q)$ *e* $e(P, Q \oplus Q') = e(P,Q) \cdot e(P,Q')$.
- ***não-degenerado:*** *para todo* $P \neq \mathcal{O} \in G_1$ *existe* $Q \in G_2$ *tal que* $e(P,Q) \neq 1$ *e, dualmente, para todo* $Q \neq 0 \in G_2$ *existe* $P \in G_1$ *tal que* $e(P,Q) \neq 0$.

Como consequência imediata da definição, temos

264 FACTO

Se $e\colon G_1 \times G_2 \to \Gamma$ *é um emparelhamento, então para todo* $P \in G_1$ *e todo* $Q \in G_2$

- $e(P,0) = e(0,Q) = 1$.
- $e(-P,Q) = e(P,-Q) = e(P,Q)^{-1}$
- $e([k]P, [j]Q = e(P\,Q)^{k\,j}$ *para todos* $k, j \in \mathbb{Z}$.

Emparelhamento de Tate

Escolha do corpo

1. *Escolha-se um primo p e um* ***corpo base*** $K_0 = \mathbb{F}_q$ *de característica p.*
2. *Escolha-se um primo r distinto de p. Seja k a ordem de q em $\mathbb{Z}_r^*$: isto é, o menor inteiro k tal que $q^k = 1 \mod r$. Seja $l = s \cdot (s^{-1} \mod r)$ sendo $s = (q^k - 1)/r$.*
3. *Seja $\boldsymbol{\mu}_r$ o conjunto de todas as raízes do polinómio $(X^n - 1) \in \overline{K_0}[X]$; isto é, as* ***r-raízes da unidade*** *de K_0.*
4. *Define-se $K = K_0(\boldsymbol{\mu}_r)$ como a menor extensão de K_0 que contém $\boldsymbol{\mu}_r$; isto é, a* ***r-extensão ciclotómica*** *de K_0.*
5. *Seja $(K^*)^r = \{ u^r \mid u \in K \}$ o subgrupo de K^* formado pelas r-potências de K. O grupo quociente $K^*/(K^*)^r$ é representado por K_r^*.*

O estudo das raízes da unidade, extensões ciclotómicas, polinómios ciclotómicos, etc, é uma tema da Álgebra bastante analisado[71]. Os principais resultados que nos interessam podem ser sumariados no seguinte teorema.

265 Teorema (Extensão ciclotómica)
Nas condições acima enumeradas,

[71] Consultar, por exemplo, o livro de *Steven Roman*, Field Theory, 2nd edn, Springer Verlag, nº 158 da série *Graduate Texts in Mathematics*, principalmente os Capítulos 11 e 12, para uma síntese desses resultados.

1. *O corpo K é uma extensão de grau k de $\mathbb{F}_q$ e identifica-se com $\mathbb{F}_{q^k}$.*
2. *O grupo de Galois, $\mathbb{G}(K/K_0)$ é um grupo cíclico de ordem k gerado pelo automorfismo $\sigma_q : x \mapsto x^q$.*
3. *O conjunto das r-raízes da unidade $\boldsymbol{\mu}_r$ forma um subgrupo ciclico de ordem r de K^* e o morfismo $x \mapsto x^l$ induz um isomorfismo entre o grupo quociente K_r^* e $\boldsymbol{\mu}_r$.*

Nota A relação de equivalência que gera o grupo quociente $K^*/(K^*)^r$ é, neste caso,

$$x \simeq_r y \quad \Leftrightarrow \quad (\exists u \in K^*)\,[\, x \cdot y^{-1} = u^r \,] \tag{174}$$

Pela definição de k, $(q^k - 1)$ é divisível por r; seja $s = (q^k - 1)/r$. Então, para qualquer $x \in K^*$, x^s é uma r-raíz da unidade. Sendo $l = s \cdot (s^{-1} \mod r)$, também x^l é uma r-raiz da unidade porque l é um múltiplo de s. Por outro lado, $l = 1 \mod r$ o que significa que $l - 1$ é um múltiplo de r e, por isso, $x^l \cdot x^{-1}$ é uma r-potência de um elemento de K^*. Ou seja, x e x^l são equivalentes.

Grau de embebimento

Vimos que, sendo k a ordem de q em $\mathbb{Z}_r^*$, o corpo K é uma extensão de grau k de $\mathbb{F}_q$. A constante k chama-se **grau de embebimento** de K_0 em K.

Na escolha do corpo, as várias constantes (q, r, k, l) podem-se determinar de vários modos. Por exemplo, pode-se fixar q e r e calcular grau de embebimento k como o menor inteiro k tal que r divide $q^k - 1$. Em alternativa pode-se fixar q e um grau de embebimento aceitável k, e determinar o maior primo r que divide $q^k - 1$.

Para uma implementação eficiente de emparelhamentos interessa-nos ter o grau de embebimento k tão pequeno quanto possível. Isto porque k pequeno implica que o número de elementos q^k do corpo K é relativamente pequeno e, consequentemente, são necessários poucos de bits para representar pontos de curvas elípticas E/K. Os valores ideais para k serão 2 ou 3; de facto 6 é considerado o limite superior para uma implementação razoável de emparelhamentos.

Por outro lado, r vai determinar a ordem dos grupos cíclicos e, por isso, convém que seja um primo tão grande quanto possível. Quanto maior for r mais complexo será a resolução dos problemas básicos dos grupos cíclicos (DLP, CDHP, etc.) e, por isso, mais seguras serão as técnicas criptográficas assentes nesses grupos. No mínimo r deve ser um primo só representável com 160 bits ou mais.

Estes objectivos contraditórios conduzem a uma escolha criteriosa de r que seja suficientemente grande para os grupos cíclicos serem seguros e, simultaneamente, determine uma valor de k pequeno.

EXEMPLO 52: Considere-se o corpo $K_0 = \mathbb{F}_7$. Pode-se verificar que a curva $E/\mathbb{F}_7 : y^2 - x^3 - x + 3$ tem exactamente 9 pontos e que esses pontos são gerados como múltiplos do ponto $P = (0, 2)$; os pontos $[k]P$, com $k = 1..9$, são

$$(0,2)\ ,\ (4,4)\ ,\ (5,6)\ ,\ (6,3)\ ,\ (2,0)\ ,\ (6,4)\ ,\ (5,1)\ ,\ (4,3)\ ,\ (0,5)\ ,\ P_\infty$$

Escolha-se uma ordem $r \neq p$ que seja um número primo; por exemplo $r = 13$. Neste caso $\boldsymbol{\mu}_{13}$ é formado pela unidade 1 e pelas raízes $\zeta \neq 1$ do polinómio ciclotómico $\Phi_{13}[X] = \frac{(X^{13}-1)}{(X-1)} \in \mathbb{F}_7[X]$; isto é, os ζ que verificam $\zeta^{12} + \zeta^{11} + \cdots + \zeta + 1 = 0$.

O grau de embebimento é o menor k tal que 13 divide $7^k - 1$; pode-se verificar que $k = 12$ e, portanto, K tem 7^{12} elementos. Neste caso, tem-se $l = 3194143200$. Podia-se também verificar que, aqui, tem de ser $k = r - 1$ porque o polinómio ciclotómico Φ_{13} é absolutamente irredutível em $\mathbb{F}_7$. A 13-extensão ciclotómica de $\mathbb{F}_7$, $\mathbb{F}_7(\boldsymbol{\mu}_{13})$ tem 7^{12} elementos cuja forma genérica é $a_0 + a_1\,\zeta + a_2\,\zeta^2 + \cdots + a_{11}\,\zeta^{11}$, com $a_k \in \mathbb{F}_7$.

Este valor para o grau de embebimento é péssimo: cada ponto da curva E/K exige 12 vezes mais bits que um ponto sobre a curva $E/\mathbb{F}_7$. E isto para ter apenas 13 elementos no grupo cíclico.

No entanto um grau de embebimento $k = 5$ (dentro da gama dos valores aceitáveis e bastante inferior ao valor de 12 atrás encontrado) conduz a um primo $r = 2801$ que divide $7^5 - 1$. Note-se que, mesmo para um k menor, o primo r resultante é bastante maior do que 13. O parâmetro l é também consideravelmente menor; tem-se $l = 2802 = r + 1$.

Escolha da curva

Seja $C = E/K : \phi$ uma curva elíptica cuja ordem $|E/K|$ é um múltiplo de r.

Para garantir que a ordem r divida a ordem da curva $E/K : \phi$, seria possível começar por exigir, na escolha de r, que a ordem da curva base $E/K_0 : \phi$ fosse já um múltiplo de r. Porém isso implica que o corpo de base K_0 tivesse, já à partida, um número de elementos suficientes para que tal ocorra.

Em alternativa pode-se tentar escolher (eventualmente, por tentativas sucessivas) a ordem r, o grau de embebimento k e o polinómio ϕ de modo que todas estas condições ocorram: o grau de embebimento k é pequeno, o corpo base $\mathbb{F}_q$ é pequeno, r é grande e r divide a ordem da curva definida no corpo $\mathbb{F}_{q^k}$.

□

A ordem r determina em C vários subgrupos com interesse:

- O grupo de torção $C[r] = \{ P \in C \mid [r]P = \mathcal{O} \}$.
- O grupo $r\,C = \{[r]U \mid U \in C\}$ dos r-múltiplos de pontos da curva; $r\,C$ é a imagem da isogenia $[r]\cdot$.
- O grupo quociente $C_r = C/rC$.

Note-se a analogia entre C_r e o grupo K_r^*: os elementos de C_r são as classes de equivalência geradas em C, pela relação $P \cong Q \Leftrightarrow (\exists U \in C)\,[\,P - Q = [r]U\,]$. Note-se também que as condições impostas em r e p, implicam que todos os grupos $C[r], C_r, K_r^*$ e $\boldsymbol{\mu}_r$ têm exactamente r elementos.

266 Definição (Emparelhamento de Tate)
O ***emparelhamento de Tate*** *e ordem r em C, é a função*

$$\mathbf{e}_r : C[r] \times C_r \to \boldsymbol{\mu}_r$$

tal que, para todo ponto $P \in C[r]$ e classe de equivalência $q \in C_r$, o valor de $\mathbf{e}_r(P, q)$ é o elemento de $\boldsymbol{\mu}_r$ gerado da seguinte forma:

1. *Determina-se $f \in K(C)$ tal que $(f) = r(P \oplus R) - r(R)$, para algum ponto $R \in C$.*

Porque $P \in C[r]$, a função (f) existe. Note-se que P verifica $[r]P = \mathcal{O}$ e, pela definição 243, tem-se $r(P) - r(\mathcal{O}) \sim 0$; logo, para todo R, será $r(P \oplus R) - r(R) \sim 0$. Usualmente escolhe-se $R = \mathcal{O}$.

2. *Escolhe-se $Q \in q$ e determina-se um divisor $D \sim (Q) - (\mathcal{O})$ que tenha um suporte disjunto do de (f).*

   Normalmente, basta escolher um ponto $S \in C$, tal que tanto S como $Q \oplus S$ não sejam nem zero nem pólo de f, e definir $D = (Q \oplus S) - (S)$. Pela definição 243, tem-se $(Q \oplus S) - (\mathcal{O}) \sim (Q) + (S) - 2\,(\mathcal{O})$ e, portanto, $(Q \oplus S) - (S) \sim (Q) - (\mathcal{O})$.

3. *Determina-se $f(D)$ e define-se $\mathbf{e}_r(P, q) = f(D)^l$; ou seja, como a r-raiz da unidade equivalente a $f(D)$.*

   Como D não contém pólos ou zeros de f, a função f é regular em D e tem-se $f(D) \neq 0$; logo $f(D) \in K^*$. O valor $f(D)^l$ determina a raiz da unidade $\mu \in \boldsymbol{\mu}_r$ tal que $f(D) \simeq_r \mu$.

No passo (1) temos várias funções racionais $f \in K(C)$ que verificam $(f) = r(P \oplus R) - r(R)$. O valor de $\mathbf{e}(P, q)$ deve ser independente do ponto R e da função f escolhidas. É também importante ter em atenção, no passo (2), que Q é um representante da classe de equivalência $q \in C_r$ e o valor $f(D)$ depende de Q; são possíveis vários pontos Q dentro da mesma classe de equivalência $q \in C_r$ e vários divisores $D \sim (Q) - (\mathcal{O})$. Escolhendo um diferente $Q' = Q \oplus [r]U$ e um diferente $D' \sim (Q') - (\mathcal{O})$, o valor para $f(D')$ e o valor de $f(D)$ devem conduzir, no final, ao mesmo valor de $\mathbf{e}_r(P, q)$.

Em resumo: para a correcção do resultado de $\mathbf{e}(P,q)$, deve ser indiferente o ponto R, a função f, o representante Q e o divisor D, escolhidos desde que verifiquem as condições estipuladas na respectiva escolha. No entanto, a liberdade na selecção de determinados valores específicos de R, f, Q e D é importante para a eficiência da implementação deste algoritmo.

Todos estes factos levam a que o resultado $f(D)$ seja visto como um representante de uma classe de equivalência em K_r^* e, consequentemente, um elemento de $\boldsymbol{\mu}_r$. A razão porque o algoritmo na noção 266 define correctamente uma função $C[r] \times C_r \longrightarrow \boldsymbol{\mu}_r$ é resultado dos seguintes lemas.

267 LEMA *Sejam $f, g \in K(C)$ funções racionais homogéneas tais que $(f) = r(P) - r(\mathcal{O})$ e, para um qualquer ponto $R \in C$, $(g) = r(P \oplus R) - r(R)$. Então, para todo o divisor de grau zero D sobre K com suporte disjunto do de (f) e do de (g), tem-se $f(D) \simeq_r g(D)$.*

268 LEMA *Seja $f \in K(C)$ tal que que $(f) = r(P) - r(\mathcal{O})$. Sejam D e D' divisores sobre K de grau zero tais que $D \sim D'$, e com suporte disjunto do de (f). Então $f(D) \simeq_r f(D')$.*

269 LEMA *Seja $f \in K(C)$ funções racional homogénea tal que $(f) = r(P) - r(\mathcal{O})$. Sejam D e D' divisores sobre K de grau zero tais que $D \sim (Q) - (\mathcal{O})$ e $D' \sim (Q \oplus [r]U) - (\mathcal{O})$, cujo suporte é disjunto do de (f). Então $f(D) \simeq_r f(D')$.*

Prova As provas destes três lemas são uma simples aplicação dos resultados da teoria dos divisores sobre curvas elípticas. Note-se que, em todas as provas, as funções racionais f e g estão sempre definidas, na curva, a menos da multiplicação por uma constante $\lambda \neq 0$. No entanto, pelo facto 247, quando aplicadas a divisores D de grau zero, os valores de $f(D)$ e $g(D)$ são independentes dessa constante.

Lema 267 Pela definição 243 temos $(P \oplus R) - (P) - (R) + (\mathcal{O}) \sim 0$. Seja $u \in K(C)$ tal que $(u) = (P \oplus R) - (P) - (R) + (\mathcal{O})$; então $(u^r) = r(u) = r(P \oplus R) - r(R) - r(P) + r(\mathcal{O})$ e consequentemente $(g) = (u^r) + (f) = (u^r\, f)$. Donde, para alguma constante $\lambda \neq 0$, tem-se $\lambda\, g(X) = u(X)^r\, f(X)$, para todo $X \in C$ onde g e f sejam regulares. Para qualquer divisor cujo suporte seja disjunto do suporte de (f) e de (g) temos $g(D) = f(D)\, u(D)^r$ e, consequentemente, $g(D) \simeq_r f(D)$.

Lema 268 Seja $u \in K(C)$ tal que $D = D' + (u)$. Então o suporte de u é disjunto do de f e $f(D) = f(D')\, f((u))$. Pela reciprocidade de Weil (teorema 248) temos $f((u)) = u((f)) = u(r(P) - r(\mathcal{O})) = u(P)^r / u(\mathcal{O})^r$. Consequentemente $f(D) \simeq_r f(D')$.

Lema 269 Temos $D' - D \sim (Q \oplus [r]U) - (Q) \sim r(U) - r(\mathcal{O})$ e, portanto, como o suporte de (f) é disjunto do de D e D', temos $f(D')/f(D) = f(U)^r / f(\mathcal{O})^r$. Logo $f(D') \simeq_r f(D)$.

Estamos agora em condições de provar o resultado fundamental.

270 Teorema (Emparelhamento de Tate)
O algoritmo apresentada na definição 266 determina uma função $\mathbf{e}_r : C[r] \times C_r \longrightarrow \boldsymbol{\mu}_r$ *e esta função:*

1. *É um emparelhamento (noção 263),*
2. *Para todo o automorfismo* $\sigma \in \mathbb{G}(K/K_0)$, *verifica* $\mathbf{e}_r(\sigma(P), \sigma(q)) = \sigma(\mathbf{e}_r(P, Q))$.

Esboço de Prova Os lemas (267), (268) e (269), dizem-nos que, independentemente do ponto R, da função f, do representante $Q \in q$ e do divisor D, $f(D)$ é sempre um elemento da mesma classe de equivalência em K_r^*; o isomorfismo entre K_r^* e $\boldsymbol{\mu}_r$ completa a definição da função.

Para provar (1) (isto é, ver que $(P,q) \mapsto \mathbf{e}_r(P,q)$ é um emparelhamento de acordo com a noção 263) temos de provar que é bilinear e não-degenerada.

Biliear no 1^{o} argumento, $\mathbf{e}(P \oplus P', q) = \mathbf{e}(P,q) \cdot \mathbf{e}(P',q)$: Sejam $f, f' \in K(C)$ tais que $(f) = r(P) - r(\mathcal{O})$ e $(f') = r(P') - r(\mathcal{O})$. Seja $u \in K(C)$ tal que $(u) = (P \oplus P') - (P) - (P') + (\mathcal{O})$ e seja $h = f \cdot f' \cdot u^r$. Então $(h) = (f) + (f') + r(u) = r(P \oplus P') - r(\mathcal{O})$. Para um qualquer divisor $D \sim (Q) - (\mathcal{O})$, com $Q \in q$, com suporte disjunto do de h, tem-se $h(D) \simeq_r f(D)\, f'(D)$ e este valor determina $\mathbf{e}_r(P \oplus P', q)$; como $f(D)$ e $f'(D)$ determinam, respectivamente, $\mathbf{e}_r(P,q)$ e $\mathbf{e}_r(P,q)$, tem-se $\mathbf{e}_r(P \oplus P', q) = \mathbf{e}_r(P,q) \cdot \mathbf{e}_r(P',q)$.

As restantes 3 condições do emparelhamento (bilinear no 2^{o} argumento e não-degenerado no 1^{o} e 2^{o} argumentos) provam-se de forma semelhante.

Para provar (2) (invariância por automorfismos de Galois), basta ver que $\sigma(f(P)) = f_\sigma(\sigma(P))$, sendo f_σ a aplicação do automorfismo σ aos coeficientes de f. Se $(f) = r(P) - r(\mathcal{O})$ então $(f_\sigma) = r(\sigma(P)) - r(\mathcal{O})$. Sendo $D \sim (Q) - (\mathcal{O})$, tem-se $\mathbf{e}_r(\sigma(P), \sigma(Q)) = f_\sigma(\sigma(D)) = \sigma(f(D)) = \sigma(\mathbf{e}_r(P,Q))$.

Emparelhamento de Weil

Fixemos um corpo base $K_0 = \mathbb{F}_q$, e uma ordem $r \neq p$. Como anteriormente $\boldsymbol{\mu}_r$ é o grupo cíclico das r-raízes da unidade em K_0.

Seja $E/\overline{K_0}$ uma curva elíptica sobre o fecho algébrico de K_0, cuja ordem $|E/\overline{K_0}|$ é um múltiplo de r. Como habitualmente $E/\overline{K_0}[r]$ denota o grupo de torção de ordem r.

Escolhe-se K como a mínima extensão de K_0 que contém as coordenadas de todos os pontos neste grupo de torção. Abusando um pouco da notação podemos escrever $K = K_0(E/\overline{K_0}[r])$.

271 Noção (Emparelhamento de Weil)
O ***emparelhamento de Weil*** *é a função* $\mathbf{w}_r \colon E[r] \times E[r] \to \boldsymbol{\mu}_r$ *com* $\mathbf{w}_r(P,Q)$ *gerado por:*

1. *Escolhe-se dois divisores* $D \sim (P) - (\mathcal{O})$ *e* $D' \sim (Q) - (\mathcal{O})$ *de suporte disjuntos.*

   Basta escolher pontos R e S apropriados e fazer $D = (P \oplus R) - (R)$ e $D' = (Q \oplus S) - (S)$.

2. *Escolhe-se funções* $f, g \in K(E)$ *tais que* $(f) = r\,D$ *e* $(g) = r\,D'$.

   Porque P e Q pertencem a $E[r]$ tem-se $[r]P = [r]Q = \mathcal{O}$. Logo $r(P) - r(\mathcal{O}) = r\,D \sim 0$ e $r(Q) - r(\mathcal{O}) = r\,D' \sim 0$. Consequentemente, existem $f, g \in K(E)$ tais que $(f) = r\,D$ e $(g) = r\,D'$.

3. *Calcula-se* $w = f(D')/g(D)$ *e faz-se* $\mathbf{w}_r(P,Q) = w^l$.

   Pelo lema 268, tem-se $f(D' + (h')) \simeq_r f(D')$ e $g(D + (h)) \simeq_r g(D)$ para quaisquer $h, h' \in K(E)$. Portanto, o valor de $\mathbf{w}_r(P,Q)$ é independente dos divisores D, D' desde que satisfaçam as condições em (1).

Como sabemos, funções racionais distintas com o mesmo divisor são determindas a menos da multiplicação por uma constante; isso não afecta o resultado da sua aplicação a divisores de grau 0. Por isso o valor de $\mathbf{w}_r(P,Q)$ é independente da escolha específica de funções f, g em (2).

As propriedades da função $\mathbf{w}_r$ podem ser sumariadas no seguinte resultado.

272 TEOREMA (EMPARELHAMENTO DE WEIL)
O algoritmo apresentado na noção 271 define um emparelhamento. Adicionalmente verifica:

1. *(*Invariância de Galois*) Para todo automorfismo* $\sigma \in \mathbb{G}(\overline{K}/K)$ *verifica-se*

$$\mathbf{w}_r(\sigma(P), \sigma(Q)) \;=\; \sigma(\mathbf{w}_r(P,Q))$$

2. *(*Simetria*)* $\mathbf{w}_r(,P,P) = 1$ *e* $\mathbf{w}_r(,P,Q) = \mathbf{w}_r(,Q,P)^{-1}$.

Esboço de prova A prova de que a função é um emparelhamento usa as mesmas técnicas que a prova equivalente no emparelhamento de Tate. A invariância de Galois é também provada do mesmo mdodo. A simetria é óbvia a partir da definição.

Existem semelhanças óbvias entre os emparelhamentos de Tate e de Weil. Para pontos P, Q na intersecção dos respectivos domínios é óbvio, pela definição, que

$$\mathbf{w}_r(P,Q) \quad = \quad \frac{\mathbf{e}_r(P,Q)}{\mathbf{e}_r(Q,P)} \tag{175}$$

Existem, no entanto, alguns detalhes que podem impedir esta relação óbvia. Em primeiro lugar, as curvas E/K são definidas sobre corpos K distintos. Depois os próprios domínios das funções são subgrupos distintos da curva.

Em ambos os casos o corpo de base K_0 é $\mathbb{F}_q$ com característica p; em ambos os casos a ordem r é um primo distinto de p. Porém,

(i) no emparelhamento de Tate, escolhe-se primeiro o corpo K como $\mathbb{F}_q(\boldsymbol{\mu}_r)$ e escolhe-se depois a curva E/K de forma a ter uma ordem que seja múltipla de r.

(ii) no emparelhamento de Weil, escolhe-se primeiro uma curva $E/\overline{\mathbb{F}_q}$ que tenha uma ordem múltipla de r e fixa-se o corpo K como a extensão $\mathbb{F}_q(E[r])$.

Geralmente, o corpo $\mathbb{F}_q(E[r])$ seria muito maior do que o corpo $\mathbb{F}_q(\boldsymbol{\mu}_r)$. No entanto, para muitas situações com interesse criptográfico, os dois coincidem. Isto é resultado do seguinte teorema.

273 Teorema (Balasubramanian e Kobliz)
Seja $E/\mathbb{F}_q$ uma curva elíptica definida dobre um corpo $\mathbb{F}_q$ de característica p. Seja $r \neq p$ um primo que não divide $q-1$ mas divide a ordem $|E/\mathbb{F}_q|$ da curva. Então $E[r] \subset E/\mathbb{F}_{q^k}$ se e só se r divide $q^k - 1$.

Note-se que as condições do teorema exigem que, à partida, a curva sobre o corpo base já contenha pontos suficientes para conter $E[r]$; nomeadamente a sua ordem tem de ser um múltiplo de r. Esta condição é mais forte das que foram colocadas na definição de curva em ambos os emparelhamentos, onde se requeria que apenas a curva sobre a extensão k verificasse uma condição análoga.

Se estas condições forem verificadas o domínio de ambos emparelhamentos é compatível (tendo em atenção que, no emparelhamento de Tate, os dois argumentos têm domínios diferentes) e a igualdade (175) pode ser usada.

□

No cálculo do emparelhamento de Tate, o passo que exige maior esforço computacional é a determinação da função racional f tal que $(f) = r(P) - r(\mathcal{O})$. Dado que o emparelhamento de Weil este passo é repetido para a função g, é natural pensar-se que, com domínios compatíveis, o esforço computacional do emparelhamento de Weil seja, aproximadamente, o dobro do de Tate.

Normalmente r é um número primo com, pelo menos 160 bits de representação e, por isso, a exponenciação directa de uma função não é abordagem razoável. O **algoritmo de Miller** baseia-se na usual estratégia de cálculo eficiente de exponenciais por sucessivas do expoente e cálculo de quadrados.

Para este algoritmo recordemos o lema 255 (página 523), a função racional $\mu(P,Q)$ definida na noção 256 (página 524), e o seu divisor $(\mu(P,Q)) = (P) + (Q) - (P \oplus Q) - (\mathcal{O})$.

Para um ponto P da curva, seja $P_i = [i]P$ e considere-se a sucessão de funções racionais f_i tais que $f_1 = 1$ e

$$(P_i) - (\mathcal{O}) + (f_i) \;=\; i(P) - i(\mathcal{O}) \tag{176}$$

Note-se que, se $P \in E[r]$, $P_r = \mathcal{O}$ e que, portanto, f_r é a função que se pretende calcular. Por outro lado,

$$(\mu(P_i, P_j)) = (P_i) + (P_j) - (P_{i+j}) - (\mathcal{O}) \tag{177}$$

dado que $P_{i+j} = P_i \oplus P_j$.

274 LEMA *Com a sucessão de funções f_i verificando* (176) *verifica-se, a menos de uma constante multiplicativa,*

$$f_{i+j} \;=\; f_i \cdot f_j \cdot \mu(P_i, P_j) \tag{178}$$

Em particular

$$f_{2\,i} \;=\; f_i^2 \cdot \mu(P_i, P_i) \qquad \textit{e} \qquad f_{i+1} \;=\; f_i \cdot \mu(P_i, P) \tag{179}$$

Prova Dado que $\mu(P_i, P_j)$ verifica (177) tem-se $(f_i \cdot f_j \cdot \mu(P_i, P_j)) \;=\; (f_i) + (f_j) + (\mu(P_i, P_j)) \;=\; (f_{i+j})$. Como as funções racionais são determinadas, a menos de uma constante multiplicativa, pelos seus divisores, f_{i+j} é determinada por (178).

O algoritmo de Miller determina f_r usando sucessivamente as igualdades (179).

Objectivo Determinar $f_r(D)$ sendo $D = (Q \oplus S) - (S)$ para um S apropriado.

1. Fazer $f \leftarrow 1$, $T \leftarrow P$ e $n \leftarrow r$
2. Enquanto $n > 0$ executar repetidamente os seguintes passos
3. $T \leftarrow [2]T \quad ; \quad \lambda \leftarrow \mu(T,T) \quad ; \quad f \leftarrow f^2 \cdot \lambda(Q \oplus S)/\lambda(S)$
4. Se n é impar fazer $T \leftarrow T + P \quad ; \quad \lambda \leftarrow \mu(T,P) \quad ; \quad f \leftarrow f \cdot \lambda(Q \oplus S)/\lambda(S)$
5. $n \leftarrow n/2$.

O valor final de f contém $f_r(D)$; para calcular o emparelhamento de Tate basta agora determinar em K, o valor f^l usando um algoritmo de exponenciação eficiente.

8.7 Curvas Super-singulares e Implementação de Emparelhamentos

As condições para a definição do emparelhamento de Tate exigem uma escolha apropriada do corpo $K = \mathbb{F}_q(\boldsymbol{\mu}_r)$ impondo um garu de embebimento k pequeno, uma ordem r suficientemente grande e uma curva elíptica E/K cuja ordem seja um multiplo de r.

A verificação simultânea de todas estas condições é difícil se as curvas forem escolhidas arbitrariamente. Porém, para alguns tipos de curvas esta escolha é mais simples.

275 Noção
Seja $K = \mathbb{F}_q$ um corpo finito de característica p. Uma curva elíptica E/K é **super-singular** *quando satisfaz uma seguintes condições equivalentes:*

1. *Verifica-se $|E/K| = 1 \mod p$; equivalentemente $|E/K| = q + 1 - t$ para algum múltiplo t de p.*
2. *E/K não tem pontos de ordem p em $\overline{K}$; equivalentemente o grupo de torsão $E/\overline{K}[p]$ reduz-se a $\{\mathcal{O}\}$.*

Curvas que não verificam qualquer destas condições dizem-se **ordinárias**.

Para curvas arbitárias E/K (supersingulares ou ordinárias), o seguinte teorema ajuda a caracterizar o seu grau de embebimento.

276 Teorema (Waterhouse)
Nas condições da definição 275, para cada $a \in \mathbb{N}$, seja

$$T_a \;=\; \left\{\, t \in \mathbb{Z} \;\mid\; |E| = p^a + 1 - t \quad \textit{para alguma curva } E/K \,\right\} \tag{180}$$

Então, para todo $t \in T_a$, verifica-se $\gcd(t,p) \neq 1$, $|t| \leq 2\sqrt{p^q}$ e uma das seguintes condições

1. *a é par e $t = \pm 2\, p^{a/2}$*
2. *a é par, $(p \neq 1 \mod 3)$ e $t = \pm p^{a/2}$*
3. *a é impar, $p = 2, 3$ e $t = \pm p^{(a+1)/2}$*
4. *a é ímpar e $t = 0$*
5. *a é par, $(p \neq 1 \mod 4)$ e $t = 0$.*

Como consequência pode-se construir a seguinte tabela de curvas super-singulares para graus de embebimento $k = 1, 2, 3, 4, 6$. A tabela contém uma coluna q com o número de elementos de $K = \mathbb{F}_q$, a ordem $|E/K|$ da curva e a dimensão n tal que estrutura do grupo $E/\mathbb{F}_{q^k}$ é isomórfico com $\mathbb{Z}_n \times \mathbb{Z}_n$.

k	q	$\lvert E/K\rvert$	n
1	$p^{2\,b}$	$q \pm 2\sqrt{q} + 1$	$\sqrt{q} \pm 1$
2	$*$	$q + 1$	$q + 1$
3	$**$	$q + \sqrt{q} + 1$	$q^{3/2} - 1$
3	$**$	$q - \sqrt{q} + 1$	$q^{3/2} + 1$
4	$2^{2\,b+1}$	$q \pm \sqrt{2\,q} + 1$	$q^2 + 1$
6	$3^{2\,b+1}$	$q \pm \sqrt{3\,q} + 1$	$q^3 + 1$

O caso $(*)$ corresponde às entradas (4) e (5) no teorema 276. Os casos $(**)$ correspondem à entrada (2).