Números p-ádicos e aplicações

Nuno Arala

Conteúdo

1. Valores absolutos em corpos

§1.1. Motivação: o papel da completude

Para motivar um pouco os objetos que vamos introduzir, vamos falar um pouco sobre Análise. A maior parte de nós já teve algum contacto com Análise ao longo da vida académica; estamos todos mais ou menos familiares com Análise Real e até, quem sabe, com Análise Complexa, mas nunca ninguém nos tentou ensinar "Análise Racional". *Porquê?* O que é que $\mathbb{R}$ e $\mathbb{C}$ têm que $\mathbb{Q}$ não tem, e que faz com que ninguém esteja interessado em fazer Análise no último?

Vamos ver algumas patologias que aparecem naturalmente quando tentamos fazer Análise em $\mathbb{Q}$.

Exemplo 1.1.1 (Patologias racionais)**.**

Em $\mathbb{Q}$ nem sequer é fácil definir funções "não algébricas". Podemos definir funções racionais: funções da forma $f(x) = \frac{P(x)}{Q(x)}$ onde P e Q são polinómios com coeficientes racionais. De facto podemos definir funções deste tipo em qualquer corpo, não necessariamente $\mathbb{Q}$. Em Análise queremos mais do que isso, e queremos poder definir funções por "aproximação" com relativa facilidade. Mas em $\mathbb{Q}$ isso é um pesadelo! Por exemplo, vamos tentar definir a função exponencial. Em $\mathbb{C}$ podemos definir

$$\exp(z) = 1 + z + \frac{z^2}{2} + \frac{z^3}{6} + \cdots = \sum_{n=0}^{\infty} \frac{z^n}{n!}. \tag{1.1}$$

Claro que precisamos de nos certificar de que esta série converge, mas isso é assegurado pelo facto de a série dos *valores absolutos* ser limitada:

$$\sum_{n=1}^{\infty} \frac{|z|^n}{n!} < \infty.$$

Em $\mathbb{Q}$, este critério falha! Se tentarmos definir $\exp : \mathbb{Q} \to \mathbb{Q}$ da mesma maneira, temos o problema de que a série (de números racionais)

$$\sum_{n=1}^{\infty} \frac{x^n}{n!}$$

não converge necessariamente para um racional quando x é racional, apesar de a série "moralmente convergir" (afinal, a série dos valores absolutos continua a ser limitada!)

O leitor pode tentar por si e verá que não é fácil sequer construir uma função, digamos, *contínua* de $\mathbb{Q}$ em $\mathbb{Q}$ que não seja essencialmente uma função racional. Fazer Análise num mundo destes parece extremamente pouco promissor!

O problema, como podemos intuir a partir deste exemplo, é que $\mathbb{Q}$ tem "buracos". Por exemplo, há um "buraco" no sítio onde devia estar o número $\sum_{n=1}^{\infty} \frac{1}{n!}$! Em Análise gostamos de poder definir objetos como *limites*, portanto é útil trabalhar em espaços onde limites de sucessões existam sob condições bastante gerais. E existe um conceito na linguagem dos espaços métricos que formaliza precisamente esta ideia de "não ter buracos"; os espaços "bons" dessa perspetiva são os chamados *espaços completos*. Formulamos assim o seguinte princípio geral:

Se queremos fazer Análise em algum espaço, então queremos que ele seja completo.

Vamos recordar brevemente como se formaliza este conceito.

Definição 1.1.2 (Sucessão de Cauchy)**.** Seja (X, d) um espaço métrico. Uma sucessão $(x_n)_{n\geq 1}$ de elementos de X diz-se uma *sucessão de Cauchy* se para todo o $\varepsilon > 0$ existe um natural N tal que, se $m, n \geq N$, então

$$d(x_m, x_n) < \varepsilon.$$

Definição 1.1.3 (Espaço completo)**.** Um espaço métrico (X, d) diz-se *completo* se qualquer sucessão de Cauchy de elementos de X converge em X.

Porque é que espaços completos são "espaços sem buracos"? A ideia intuitiva é que a definição de sucessão de Cauchy é uma tentativa de definir "sucessão moralmente convergente", ou seja, é uma tentativa de definir sucessão convergente sem mencionar o limite da sucessão. Mas uma sucessão convergente continua a ser de Cauchy se retirarmos o limite do nosso espaço, portanto sucessões de Cauchy não convergentes detetam "buracos".

Mais formalmente, uma construção clássica a partir de espaços métricos dá-nos o seguinte resultado:

Teorema 1.1.4. *Seja (X, d) um espaço métrico. Então existe um espaço métrico completo $(\widetilde{X}, \widetilde{d})$ que estende (X, d), de tal modo que X é denso em $\widetilde{X}$. Além disso, $(\widetilde{X}, \widetilde{d})$ é único a menos de isometria. Chamamos a $(\widetilde{X}, \widetilde{d})$ o* completamento *de X.*

Com isto, podemos provar o seguinte:

Proposição 1.1.5. *Seja (X, d) um espaço métrico. Então*

(i) Uma sucessão $(x_n)_{n\geq 1}$ de elementos de X é uma sucessão de Cauchy se e só se existe um espaço métrico (Y, d') que estende (X, d) tal que $(x_n)_{n\geq 1}$ converge em Y. (Por outras palavras: uma sucessão de Cauchy é o mesmo que uma sucessão convergente, possivelmente fora do nosso espaço.)

(ii) O espaço (X, d) é completo se e só se é universalmente fechado*, ou seja, se e só se X é fechado em Y para qualquer espaço métrico (Y, d') que estende (X, d).*

Demonstração. Para provar (i), comecemos por supor que $(x_n)_{n\geq 1}$ converge para $a \in Y$. Fixemos $\varepsilon > 0$, e seja N tal que $d(x_n, a) < \frac{\varepsilon}{2}$ para $n \geq N$. Então, se $m, n \geq N$,

$$d(x_m, x_n) \leq d(x_m, a) + d(a, x_n) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Logo $(x_n)_{n\geq 1}$ é uma sucessão de Cauchy. Reciprocamente, se $(x_n)_{n\geq 1}$ é uma sucessão de Cauchy, considere-se o espaço $(Y, d') = (\widetilde{X}, \widetilde{d})$ dado pelo Teorema 1.1.4. Então $(x_n)_{n\geq 1}$ é uma sucessão de Cauchy em $\widetilde{X}$, que é completo, logo converge em $\widetilde{X}$.

Para provar (ii), suponhamos primeiro que (X, d) é universalmente fechado. Seja $(x_n)_{n\geq 1}$ uma sucessão de Cauchy. Então (por (i)) existe uma extensão (Y, d') de (X, d) tal que $(x_n)_{n\geq 1}$ converge em Y. Seja a o limite da sucessão. Então a, sendo o limite de uma sucessão de elementos de X, que é fechado em Y, pertence necessariamente a X. Ou seja, qualquer sucessão de Cauchy em X converge em X, e portanto X é completo. Reciprocamente, se X é completo e está mergulhado no espaço Y, considere-se uma sucessão $(x_n)_{n\geq 1}$ de elementos de X que converge em Y; por (i) esta sucessão é de Cauchy, e portanto, como X é completo, converge em X. Logo X é fechado em Y, e isto mostra que X é universalmente fechado. □

A moral da história é:

Se um espaço não é completo, então há pontos fora do espaço que merecem ser acrescentados, e que são importantes para fazer Análise.

Os nossos antepassados resolveram o problema da incompletude de $\mathbb{Q}$ "completando-o" através da construção que leva ao Teorema 1.1.4, partindo da métrica em $\mathbb{Q}$ definida por $d(x, y) = |x-y|$, e obtiveram $\mathbb{R}$. O nosso objetivo aqui é estudar outras maneiras de completar os racionais, a partir de outras métricas. Por exemplo, dado um primo p e um racional $x \neq 0$, podemos escrever

$$x = p^n \frac{a}{b}$$

onde a e b são inteiros não divisíveis por p. Então definimos

$$|x|_p = p^{-n}$$

e $|0|_p = 0$. Definindo $d(x, y) = |x - y|_p$, obtemos uma métrica em $\mathbb{Q}$ diferente da métrica usual! De facto vamos ver mais à frente que estas são essencialmente as *únicas* métricas para além da usual que satisfazem certas condições de compatibilidade com a estrutura de corpo de $\mathbb{Q}$.

Note-se que a noção de "proximidade" em relação a esta métrica é muito diferente da usual. A ideia aqui é que dois inteiros estão muito "próximos" um do outro se são congruentes módulo uma potência muito grande do primo p. E podemos completar $\mathbb{Q}$ em relação a esta métrica também, pelo processo que leva ao Teorema 1.1.4; ao fazê-lo, obtemos um corpo que cumpre os requisitos para fazer Análise, e deste modo podemos utilizar ideias analíticas para tratar questões de Teoria dos Números. Este corpo chama-se o *corpo dos números p-ádicos*, e é denotado na literatura por $\mathbb{Q}_p$.

Vamos fazer um passeio informal por $\mathbb{Q}_p$, antes de começar a trabalhar rigorosamente com ele. Uma característica curiosa dos completamentos, que os distingue de $\mathbb{Q}$, é que têm "poucas" extensões algébricas. Isto não é muito surpreendente: para estender algebricamente um corpo devemos acrescentar-lhe uma raiz de um polinómio que ainda não tenha raízes no corpo. Ora, quando completamos um corpo, torna-se mais "fácil" resolver equações polinomiais nele. Pensemos em $\mathbb{R}$: intuitivamente, é muito mais fácil a equação $x^3 - 3x + 1 = 0$ ter solução em

$\mathbb{R}$ do que em $\mathbb{Q}$, pois em $\mathbb{R}$ basta, por exemplo, encontrar a e b tais que $a^3 - 3a + 1 < 0$ e $b^3 - 3b + 1 < 0$; garantir soluções racionais é mais delicado.

Por exemplo, $\mathbb{Q}$ tem infinitas extensões algébricas de grau 2: $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5}), \ldots$. Por outro lado, $\mathbb{R}$ só tem uma (que é $\mathbb{C}$), e pode-se provar que $\mathbb{Q}_5$ só tem 3 extensões algébricas de grau 2.

Vamos tentar brincar um pouco com esta afirmação. Porque é que extensões de grau 2 de $\mathbb{Q}_5$ são tão "raras"? Para obter uma extensão quadrática (de grau 2) de $\mathbb{Q}_5$, devemos acrescentar a $\mathbb{Q}_5$ uma raiz quadrada de um elemento de $\mathbb{Q}_5$ que ainda não exista em $\mathbb{Q}_5$. Vamos tentar fazer isso. Que tal, digamos, $\sqrt{6}$? Será que $\mathbb{Q}_5(\sqrt{6})$ é uma extensão de grau 2 de $\mathbb{Q}_5$? Ou será que $\sqrt{6}$ já existe em $\mathbb{Q}_5$?

Para responder a isto, vamos utilizar o *binómio de Newton generalizado*. Em $\mathbb{R}$, tem-se a identidade

$$(1+x)^\alpha = \sum_{n\geq 0} \binom{\alpha}{n} x^n$$

para $|x| < 1$, onde

$$\binom{\alpha}{n} = \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}.$$

Em particular, a série

$$\sum_{n\geq 0} \binom{1/2}{n} x^n = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 - \frac{5}{128}x^4 + \frac{7}{256}x^5 + \cdots \tag{1.2}$$

converge para uma raiz quadrada de $1+x$ quando $|x| < 1$.

Analogamente, em $\mathbb{Q}_5$, devemos então ter

$$\sqrt{6} = \sqrt{1+5} = \sum_{n\geq 0} \binom{1/2}{n} 5^n. \tag{1.3}$$

Pode parecer estranho substituir $x = 5$, já que a série em (1.2) apenas converge quando $|x| < 1$. Mas isso é porque estamos formatados para pensar no valor absoluto *usual*; em $\mathbb{Q}_5$, o valor absoluto certo a usar é $|\cdot|_5$, e de facto

$$|5|_5 = \frac{1}{5} < 1.$$

Portanto é de esperar que a série em (1.3) convirja em $\mathbb{Q}_5$ para uma raiz quadrada de 6! Há no entanto um pequeno problema. Embora a condição $|5|_5 < 1$ ajude à convergência da série, nada nos garante que, em $\mathbb{Q}_5$, os coeficientes binomiais $\binom{1/2}{n}$ não são demasiado grandes, a ponto de cancelarem o decaimento das potências de 5. Vamos então provar que isso não acontece, pois isso dá-nos uma excelente desculpa para mostrar o tipo de raciocínios que os métodos p-ádicos permitem. Provaremos o seguinte

Lema 1.1.6. *Para todo o inteiro positivo n,*

$$\left|\binom{1/2}{n}\right|_5 \leq 1.$$

Observemos que, tendo em conta a definição de $|\cdot|_5$, o que o Lema nos diz é que, quando escrevemos $\binom{1/2}{n}$ como uma fração irredutível, o denominador não é divisível por 5. Isto não é imediato a partir da definição de $\binom{1/2}{n}$; à partida não é óbvio que os fatores 5 do denominador

$n!$ cancelem todos com os do numerador. Mas não é mais do que um resultado puramente aritmético, que até uma criança seria capaz de entender. E, no entanto, vamos prová-lo usando análise p-ádica.

O conjunto $\mathbb{Z}$ dos inteiros não é fechado em $\mathbb{Q}_p$. Isto é diferente do que acontece em $\mathbb{R}$, onde $\mathbb{Z}$ é fechado. O fecho dos inteiros em $\mathbb{Q}_p$ é um subanel de $\mathbb{Q}_p$ habitualmente denotado por $\mathbb{Z}_p$: são os *inteiros p-ádicos*.

$$\begin{array}{ccc} \mathbb{Z}_5 & \hookrightarrow & \mathbb{Q}_5 \\ \uparrow & & \uparrow \\ \mathbb{Z} & \hookrightarrow & \mathbb{Q} \end{array}$$

Prova do Lema. Afirmamos primeiro que $\frac{1}{2} \in \mathbb{Z}_5$. Para o provar, note-se que

$$1 + 5 + 5^2 + 5^3 + \cdots = \frac{1}{1-5} = -\frac{1}{4}$$

usando a fórmula usual para a soma de uma progressão geométrica (que é válida pois $|5|_5 < 1$!). E portanto

$$\frac{1}{2} = -2 - 2 \cdot 5 - 2 \cdot 5^2 - 2 \cdot 5^3 - \cdots$$

Logo $\frac{1}{2}$ é o limite de uma sucessão de elementos de $\mathbb{Z}$, e, como $\mathbb{Z}_5$ é o fecho de $\mathbb{Z}$, $\frac{1}{2} \in \mathbb{Z}_5$.

Ou seja, vimos que existe uma sucessão $(\alpha_k)_{k \geq 1}$ de inteiros tal que

$$\frac{1}{2} = \lim_{k \to \infty} \alpha_k.$$

Notemos que a função

$$x \mapsto \binom{x}{n}$$

é polinomial, e portanto é contínua. Mas então

$$\binom{1/2}{n} = \lim_{k \to \infty} \binom{\alpha_k}{n}$$

e portanto

$$\left| \binom{1/2}{n} \right|_5 = \lim_{k \to \infty} \left| \binom{\alpha_k}{n} \right|_5 . \tag{1.4}$$

Mas, como os α_k são todos inteiros, todos os coeficientes binomiais $\binom{\alpha_k}{n}$ são inteiros, e, portanto,

$$\left| \binom{\alpha_k}{n} \right|_5 \leq 1.$$

Assim, decorre de (1.4) que $\left| \binom{1/2}{n} \right|_5 \leq 1$, como pretendido. □

§1.2. Valores absolutos: definições e propriedades básicas

Para completar um corpo, precisamos primeiro de ter uma métrica nesse corpo. As métricas mais agradáveis (do ponto de vista da compatibilidade com a estrutura de corpo) são as que se obtêm a partir de *valores absolutos*, que definimos a seguir.

Definição 1.2.1. Seja K um corpo. Um *valor absoluto* em K é uma função $|\cdot| : K \to \mathbb{R}_{\geq 0}$ com as seguintes propriedades:

- Dado $x \in K$, tem-se $|x| = 0$ se e só se $x = 0$;
- $|x + y| \leq |x| + |y|$ para quaisquer $x, y \in K$ (desigualdade triangular);
- $|xy| = |x| \cdot |y|$ para quaisquer $x, y \in K$.

Ao par $(K, |\cdot|)$ chama-se um *corpo valorado*.

Exemplo 1.2.2.

(i) O valor absoluto usual em $\mathbb{Q}$ (ou $\mathbb{R}$, ou $\mathbb{C}$) é um valor absoluto.

(ii) Dado qualquer corpo K, podemos definir

$$|x| = \begin{cases} 0 & \text{se } x = 0 \\ 1 & \text{caso contrário.} \end{cases}$$

Este é um valor absoluto em K, o chamado *valor absoluto trivial*.

Se $(K, |\cdot|)$ é um corpo valorado, então K é automaticamente um espaço métrico, sendo a distância entre x e y dada por $|x - y|$. Deste modo, um valor absoluto induz uma *topologia* em K. Vamos agora definir um tipo especial de valor absoluto que terá um papel especialmente importante para nós.

Definição 1.2.3. Um valor absoluto $|\cdot|$ num corpo K diz-se *não arquimediano* se verifica a seguinte condição extra:

- $|x + y| \leq \max\{|x|, |y|\}$ para quaisquer $x, y \in K$ (desigualdade triangular ultramétrica).

Caso contrário, $|\cdot|$ diz-se *arquimediano*.

Para definir os valores absolutos não-arquimedianos que terão maior importância para nós, começamos por uma definição preliminar:

Definição 1.2.4 (Valoração p-ádica)**.** Seja p um primo. Dado um racional $x \neq 0$, podemos escrever

$$x = p^n \frac{a}{b}$$

onde n é um inteiro e a e b são inteiros não divisíveis por p. Definimos então a *valoração p-ádica de x* como sendo

$$v_p(x) = n.$$

Definimos ainda $v_p(0) = \infty$. Assim, por exemplo, $v_2(8) = 3$, $v_3(54) = 3$ e $v_3(12/7) = 1$.

Proposição 1.2.5. *Para quaisquer racionais x e y e para qualquer primo p,*

(i) $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$;

(ii) $v_p(xy) = v_p(x) + v_p(y)$.

Demonstração. O caso em que $0 \in \{x, y, x+y\}$ é trivial. Caso contrário, comecemos por (i): sejam $x = p^m \frac{a}{b}$ e $y = p^n \frac{c}{d}$, onde p não divide nenhum dos inteiros a, b, c, d. Suponhamos sem perda de generalidade que $m \leq n$. Então

$$x + y = p^m \frac{ad + p^{n-m}bc}{bd}.$$

Como p não divide bd resulta que $v_p(x+y) \geq m = \min\{m, n\}$, como pretendido.

Para (ii), observamos que

$$xy = p^{m+n} \frac{ac}{bd}$$

e portanto $v_p(xy) = m + n$. □

Definição 1.2.6 (Valor absoluto p-ádico)**.** Seja p um primo. Dado $x \in \mathbb{Q}$, definimos

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{se } x \neq 0 \\ 0 & \text{se } x = 0. \end{cases}$$

Proposição 1.2.7. *A função $|\cdot|_p$ define um valor absoluto não arquimediano em $\mathbb{Q}$.*

Demonstração. É uma reformulação imediata da Proposição 1.2.5. □

Para concluir esta secção, vamos provar dois lemas genéricos sobre valores absolutos. O primeiro diz-nos que a topologia induzida por um valor absoluto num corpo essencialmente determina o valor absoluto. O segundo dá-nos um critério útil para um valor absoluto num corpo ser não arquimediano.

Definição 1.2.8. Dois valores absolutos $|\cdot|_1$ e $|\cdot|_2$ num corpo K dizem-se *equivalentes* se induzem a mesma topologia em K.

Lema 1.2.9. *Seja K um corpo, e sejam $|\cdot|_1$ e $|\cdot|_2$ valores absolutos em K. As seguintes condições são equivalentes:*

(i) $|\cdot|_1$ *e* $|\cdot|_2$ *são equivalentes;*

(ii) Para qualquer $x \in K$, tem-se $|x|_1 < 1$ se e só se $|x|_2 < 1$;

(iii) Existe um número real $\alpha > 0$ tal que $|x|_2 = |x|_1^\alpha$ para todo o $x \in K$.

Demonstração. Vamos provar (i)⇒(ii), (ii)⇒(iii) e (iii)⇒(i).

- (i)⇒(ii): Suponhamos que $|\cdot|_1$ e $|\cdot|_2$ são equivalentes, e seja $x \in K$ tal que $|x|_1 < 1$. Então, para todo o inteiro positivo n, tem-se $|x^n|_1 = |x|_1^n$, logo

$$\lim_{n\to\infty} |x^n|_1 = 0$$

(pois $|x|_1 < 1$). Portanto a sucessão das potências $1, x, x^2, x^3, \ldots$ tende para 0 em K, em relação à topologia induzida por $|\cdot|_1$. Como a topologia induzida por $|\cdot|_1$ é igual à topologia induzida por $|\cdot|_2$, esta sucessão também tende para 0 em relação à topologia induzida por $|\cdot|_2$. Logo,

$$0 = \lim_{n\to\infty} |x^n|_2 = \lim_{n\to\infty} |x|_2^n.$$

Isto implica $|x|_2 < 1$, e a implicação contrária é análoga.

- (ii)⇒(iii): Suponhamos que $|x|_1 < 1$ se e só se $|x|_2 < 1$. Então também temos $|x|_1 > 1$ se e só se $|x|_2 > 1$ (basta aplicar a afirmação anterior a $\frac{1}{x}$). Em particular, se $|x|_1 = 1$ para todo o $x \neq 0$ também $|x|_2 = 1$ para todo o $x \neq 0$, e o resultado é trivial. Suponhamos portanto que $|\cdot|_1$ não é o valor absoluto trivial, e seja $y \in K$ tal que $|y|_1 > 1$. Então $|y|_2 > 1$, logo existe um real $\alpha > 0$ tal que $|y|_2 = |y|_1^\alpha$. Vamos provar que $|x|_2 = |x|_1^\alpha$ para qualquer $x \in K$ (podemos supor $x \neq 0$). Seja $|x|_1 = |y|_1^b$, com $b \in \mathbb{R}$; basta provar que $|x|_2 = |y|_2^b$, pois então

$$|x|_2 = |y|_1^{\alpha b} = |x|_1^b.$$

Seja $\frac{m}{n}$ um número racional arbitrário maior do que b, onde m e n são inteiros e $n > 0$. Então

$$|x|_1 = |y|_1^b < |y|_1^{\frac{m}{n}}$$

e portanto, usando a multiplicatividade de $|\cdot|_1$,

$$\left|\frac{x^n}{y^m}\right|_1 < 1.$$

Portanto, por (ii), vem que

$$\left|\frac{x^n}{y^m}\right|_2 < 1$$

e então

$$|x|_2 < |y|_2^{\frac{m}{n}}.$$

Isto é verdade para qualquer *racional* $\frac{m}{n} > b$, e portanto conclui-se que

$$|x|_2 \leq |y|_2^b.$$

De modo análogo (usando racionais *menores* do que b desta vez), provamos que $|x|_2 \geq |y|_2^b$, e portanto $|x|_2 = |y|_2^b$, como pretendido.

- (iii)⇒(i) é trivial.

□

Observação 1.2.10. Não é necessariamente verdade que, se $|\cdot|_1$ é um valor absoluto e $\alpha > 0$ é real, então a função $|\cdot|_2$ definida por $|x|_2 = |x|_1^\alpha$ também é um valor absoluto (é verdade no caso não arquimediano, mas pode falhar no caso arquimediano).

Lema 1.2.11. *Seja $|\cdot|$ um valor absoluto num corpo K. Suponha-se que existe uma constante $M > 0$ tal que*

$$|n| \leq M \quad \textit{para todo o inteiro positivo } n.$$

Então $|\cdot|$ é não arquimediano.

Demonstração. O objetivo é, usando a condição do Lema, provar que a desigualdade triangular $|x+y| \leq |x|+|y|$ se melhora a si própria para a desigualdade ultramétrica $|x+y| \leq \max\{|x|, |y|\}$. Sejam $x, y \in K$ quaisquer, e seja n um inteiro positivo. Então

$$|x+y|^n = |(x+y)^n| = \left|\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right| \leq \sum_{k=0}^{n} \left|\binom{n}{k}\right| |x|^k |y|^{n-k}.$$

Por hipótese tem-se $\left|\binom{n}{k}\right| \leq M$, e além disso $|x|^k|y|^{n-k} \leq \max\{|x|, |y|\}^n$. Portanto

$$|x+y|^n \leq (n+1)M \max\{|x|, |y|\}^n, \quad \text{ou seja, } |x+y| \leq \sqrt[n]{(n+1)M}\, \max\{|x|, |y|\}.$$

Isto é verdade para *qualquer* inteiro positivo n, e como

$$\lim_{n\to\infty} \sqrt[n]{(n+1)M} = 1$$

resulta que $|x+y| \leq \max\{|x|, |y|\}$, como pretendido. □

§1.3. Valores absolutos em $\mathbb{Q}$

Nesta secção vamos denotar por $|\cdot|_\infty$ o valor absoluto usual em $\mathbb{Q}$ (ou $\mathbb{R}$), para reservar a notação $|\cdot|$ para um valor absoluto genérico.

Mencionámos no início que, se queremos fazer Análise em $\mathbb{Q}$, então devemos "completá-lo" em relação à métrica induzida por um valor absoluto. Sabemos que, se usarmos o valor absoluto $|\cdot|_\infty$, obtemos $\mathbb{R}$; já mencionámos também os valores absolutos p-ádicos, que conduzem aos corpos $\mathbb{Q}_p$. Será que existem outros valores absolutos não triviais em $\mathbb{Q}$? O teorema seguinte afirma que, essencialmente, não.

Teorema 1.3.1 (Teorema de Ostrowski)**.** *Seja $|\cdot|$ um valor absoluto não trivial em $\mathbb{Q}$. Então $|\cdot|$ é equivalente a $|\cdot|_\infty$ ou a $|\cdot|_p$ para algum primo p.*

Demonstração. Comecemos por observar que um valor absoluto em $\mathbb{Q}$ é determinado pela sua restrição aos inteiros, uma vez que

$$\left|\frac{m}{n}\right| = \frac{|m|}{|n|}.$$

Assim, $|\cdot|$ é determinado pelos seus valores nos inteiros. Mais ainda, como $|1|^2 = |1^2| = |1|$ vem que $|1| = 1$, e portanto $|-1|^2 = |(-1)^2| = |1| = 1$, pelo que $|-1| = 1$; então $|-n| = |n|$, logo $|\cdot|$ é determinado pela sua restrição aos inteiros *positivos*.

Sejam m e n inteiros positivos quaisquer com $n > 1$. Escrevendo m na base n, obtemos uma igualdade

$$m = a_0 + a_1 n + \cdots + a_r n^r \quad \text{onde} \quad 0 \leq a_i < n.$$

Note-se que $n^r \leq m$, e portanto $r \leq \frac{\log(m)}{\log(n)}$. Seja $N = \max\{1, |n|\}$. Aplicando valores absolutos à igualdade acima, obtemos

$$|m| \leq |a_0| + |a_1||n| + \cdots + |a_r||n|^r,$$

e como $|a_i| \leq a_i$ (porquê?) todos os termos $|a_i|$ são menores que n, e todas as potências de N são menores ou iguais a N^r, pelo que

$$|m| \leq (1+r)nN^r \leq \left(1 + \frac{\log(m)}{\log(n)}\right) nN^{\frac{\log(m)}{\log(n)}}.$$

Esta desigualdade vale para *quaisquer* inteiros positivos m e n com $n > 1$, logo mantém-se válida se substituirmos m por m^t, sendo t um inteiro positivo arbitrário. Obtemos assim

$$|m|^t \leq \left(1 + \frac{t\log(m)}{\log(n)}\right) nN^{\frac{t\log(m)}{\log(n)}},$$

ou seja (extraindo a t-ésima raiz),

$$|m| \leq \sqrt[t]{\left(1 + \frac{t\log(m)}{\log(n)}\right)}\sqrt[t]{n}N^{\frac{\log(m)}{\log(n)}}.$$

Fixados m e n, esta desigualdade é válida para qualquer t, e como

$$\lim_{t\to\infty} \sqrt[t]{\left(1 + \frac{t\log(m)}{\log(n)}\right)}\sqrt[t]{n} = 1$$

obtemos

$$|m| \leq N^{\frac{\log(m)}{\log(n)}}. \tag{1.5}$$

Agora vemos dois casos:

Caso 1: $|n| > 1$ para todo o inteiro $n > 1$.

Então, na notação anterior, tem-se $N = |n|$, e a desigualdade (1.5) dá-nos $|m| \leq |n|^{\frac{\log(m)}{\log(n)}}$, o que, para $m, n \geq 2$, equivale a

$$|m|^{\frac{1}{\log(m)}} \leq |n|^{\frac{1}{\log(n)}}.$$

Sendo isto verdade para quaisquer inteiros positivos $m, n \geq 2$, conclui-se que $|n|^{\frac{1}{\log(n)}}$ é constante (e maior do que 1 uma vez que $|n| > 1$); portanto existe $C > 1$ tal que $|n|^{\frac{1}{\log(n)}} = C$ para todo o $n \geq 2$. Conclui-se que

$$|n| = C^{\log(n)} = n^{\log(C)} = |n|_\infty^{\log(C)}$$

para todo o inteiro $n \geq 2$. Como $|1| = 1$ isto também vale para $n = 1$, e portanto $|\cdot|$ coincide com $|\cdot|_\infty^{\log(C)}$ nos inteiros positivos (e portanto em todos os racionais). Como $\log(C) > 0$, pelo Lema 1.2.9 vem que $|\cdot|$ é equivalente a $|\cdot|_\infty$.

Caso 2: $|n| \leq 1$ para algum inteiro $n > 1$.

Então, usando esse valor de n em (1.5), vem que

$$|m| \leq 1$$

para todo o inteiro positivo m. Logo, pelo Lema 1.2.11, resulta que $|\cdot|$ é não arquimediano.

Seja $\mathfrak{m}$ o conjunto dos inteiros x tais que $|x| < 1$. Obviamente $\mathfrak{m}$ é não vazio pois $0 \in \mathfrak{m}$. Além disso, se $x, y \in \mathfrak{m}$, então

$$|x - y| \leq \max\{|x|, |y|\} < 1$$

pelo que $x - y \in \mathfrak{m}$. Ou seja, $\mathfrak{m}$ é um subgrupo de $\mathbb{Z}$, e portanto $\mathfrak{m} = p\mathbb{Z}$ para algum inteiro não negativo p.

Comecemos por observar que $p \neq 0$, caso contrário $|m| = 1$ para todo o inteiro $m \geq 1$ e portanto $|\cdot|$ é o valor absoluto trivial. Afirmamos que p é primo. Caso contrário, podemos escrever $p = bc$ com b e c inteiros positivos menores do que p. Logo b e c não pertencem a $p\mathbb{Z} = \mathfrak{m}$, e portanto $|b| = |c| = 1$. Mas então

$$|p| = |b| \cdot |c| = 1,$$

o que é absurdo pois $p \in \mathfrak{m}$. Logo p é primo, e $|m| = 1$ precisamente quando m não é divisível por p.

Por fim, seja $|p| = p^{-\alpha}$ com $\alpha > 0$. Então, dado qualquer inteiro positivo n, podemos escrevê-lo na forma $n = mp^{v_p(n)}$ com m não divisível por p, e

$$|n| = |m||p|^{v_p(n)} = p^{-\alpha v_p(n)}.$$

Ou seja, $|\cdot|$ coincide com $|\cdot|_p^\alpha$ nos inteiros positivos, e portanto nos racionais, sendo portanto equivalente a $|\cdot|_p$, como pretendido. □

§1.4. O mundo não arquimediano

Vamos começar por fazer algumas considerações genéricas sobre propriedades gerais topológicas e/ou métricas de corpos valorados não arquimedianos. Em particular vamos ver como a desigualdade ultramétrica torna certos aspetos da Análise "mais simples", mas ao mesmo tempo mais contra-intuitivos.

Proposição 1.4.1 (Patologias não arquimedianas)**.** *Seja $(K, |\cdot|)$ um corpo valorado não arquimediano. Então*

(i) Qualquer triângulo com vértices em K é isósceles, sendo o "terceiro lado" menor ou igual em comprimento aos dois lados iguais;

(ii) Qualquer ponto no interior de uma bola aberta é um centro da bola;

(iii) Qualquer bola aberta é fechada.

Demonstração. (i) Sejam $x, y, z \in K$. Então

$$|x - y| = |(x - z) + (z - y)| \leq \max\{|x - z|, |z - y|\}.$$

Ou seja, no triângulo com vértices x, y, z qualquer lado tem comprimento menor ou igual ao máximo dos outros dois. Se os três lados tiverem comprimentos diferentes, então isto claramente é falso para o maior dos três lados! Logo há dois lados com o mesmo comprimento. Se z for o vértice comum a estes dois lados, a desigualdade anterior implica que o terceiro lado seja menor ou igual aos outros dois.

(ii) Seja $B(x, r)$ a bola aberta de centro x e raio $r > 0$, e seja $x' \in B(x, r)$. Dado $y \in B(x', r)$, tem-se

$$|x - y| \leq \max\{|x - x'|, |x' - y|\} < r$$

uma vez que tanto $|x - x'|$ como $|x' - y|$ são menores que r por hipótese. Logo $B(x', r) \subseteq B(x, r)$. A inclusão contrária é análoga, logo $B(x, r) = B(x', r)$ para *qualquer* $x' \in B(x, r)$!

(iii) Vamos provar que o complementar de $B(x, r)$ é aberto. Seja y um elemento de K fora de $B(x, r)$, ou seja, tal que $B(x, y) \geq r$. Seja $z \in B(y, r)$. Afirmamos que z também pertence ao complementar de $B(x, r)$, mostrando assim que esse complementar contém a bola aberta de centro y e raio r e portanto é aberto, dado que y é arbitrário.

Para isso, observamos que

$$|x - y| \leq \max\{|y - z|, |x - z|\},$$

ou seja, $|x - y|$ é menor ou igual a $|y - z|$ ou a $|x - z|$. Mas não pode ser menor ou igual a $|y - z|$, pois $|y - z| < r$ e $|x - y| \geq r$. Logo $|x - y| \leq |x - z|$. Como $|x - y| \geq r$ segue que $|x - z| \geq r$, como pretendido.

□

A próxima propriedade que vamos apresentar depende de supormos que o nosso corpo valorado é completo. Qualquer aluno que já tenha estudado séries sabe que, se uma série converge, então o termo geral tende para 0. Mas o recíproco não é verdadeiro (como qualquer pessoa

que já tenha dado disciplinas de Cálculo já repetiu vezes sem conta!): por exemplo, a série harmónica

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

não converge em $\mathbb{R}$, apesar de $\frac{1}{n}$ tender para 0. Num corpo valorado (completo) não-arquimediano, passamos a ter uma equivalência!

Proposição 1.4.2. *Seja $(K, |\cdot|)$ um corpo valorado não arquimediano completo em relação à métrica induzida por $|\cdot|$, e seja $(a_n)_{n\geq 1}$ uma sucessão de elementos de K. Então*

$$\sum_{n=1}^{\infty} a_n \text{ converge se e só se } \lim_{n\to\infty} a_n = 0.$$

Demonstração. O "só se" é análogo ao caso real. Para provar a implicação da direita para a esquerda, suponha-se que $\lim_{n\to\infty} a_n = 0$. Fixemos $\varepsilon > 0$, e seja N tal que $|a_n| < \varepsilon$ para $n \geq N$. Seja ainda

$$s_n = a_1 + \cdots + a_n.$$

Então, para $m, n \geq N$ (com $m > n$), tem-se

$$|s_m - s_n| = |a_{n+1} + \cdots + a_m| \leq \max\{|a_{n+1}|, \cdots, |a_m|\} < \varepsilon.$$

Logo $(s_n)_{n\geq 1}$ é uma sucessão de Cauchy, logo converge uma vez que K é completo. Isto significa precisamente que a série $\sum_{n=1}^{\infty} a_n$ converge. □

§1.5. Completamentos

Como mencionado na introdução, os números p-ádicos são obtidos a partir dos números racionais por *completamento* em relação ao valor absoluto p-ádico; essencialmente acrescentamos aos racionais limites das sucessões de Cauchy que não convergem. De facto, dado qualquer corpo valorado $(K, |\cdot|)$, podemos considerar o seu completamento no sentido do Teorema 1.1.4, e vamos ver de seguida que esse completamento também é um corpo.

Proposição 1.5.1. *Seja $(K, |\cdot|)$ um corpo valorado. Então*

(i) O seu completamento $\widetilde{K}$ também admite uma estrutura de corpo que estende a estrutura de corpo em K;

(ii) O valor absoluto $|\cdot|$ pode ser estendido a $\widetilde{K}$, de tal modo que a distância entre $x, y \in \widetilde{K}$ é igual a $|x-y|$. Além disso, se $|\cdot|$ é não arquimediano a sua extensão também é.

Nada disto é difícil de provar. De facto, tanto a estrutura de corpo em $\widetilde{K}$ como a extensão do valor absoluto são definidas da maneira mais imediata possível. O que se segue é apenas uma verificação quase mecânica de que estas operações estão bem definidas e satisfazem as propriedades que queremos.

Demonstração. Para provar (i), sejam x e y elementos arbitrários de $\widetilde{K}$. Como K é denso em $\widetilde{K}$, existem sucessões $(x_n)_{n\geq 1}$ e $(y_n)_{n\geq 1}$ de elementos de K tais que

$$x = \lim_{n\to\infty} x_n \quad \text{e} \quad y = \lim_{n\to\infty} y_n.$$

Definimos então

$$x + y = \lim_{n\to\infty} (x_n + y_n) \quad \text{e} \quad xy = \lim_{n\to\infty} (x_n y_n). \tag{1.6}$$

Precisamos de verificar que estes limites de facto existem, que não dependem das sucessões (x_n) e (y_n) consideradas, e por fim que $\widetilde{K}$ é um corpo com a soma e multiplicação definidas por (1.6).

Para provar que existe o primeiro limite, observamos que (x_n) e (y_n) são sucessões de Cauchy em K (pois convergem em $\widetilde{K}$). Assim, fixado $\varepsilon > 0$, existe N tal que $|x_n - x_m| < \frac{\varepsilon}{2}$ e $|y_n - y_m| < \frac{\varepsilon}{2}$ quando $m, n \geq N$. Logo, se $m, n \geq N$,

$$|(x_n + y_n) - (x_m + y_m)| \leq |x_n - x_m| + |y_n - y_m| < \varepsilon.$$

Isto mostra que $(x_n + y_n)_n$ é uma sucessão de Cauchy, que portanto converge em $\widetilde{K}$, que é completo. Para provar que existe o segundo limite, observamos que (x_n) e (y_n), sendo sucessões de Cauchy, são certamente limitadas, e existe $M > 0$ tal que $|x_n| < M$ e $|y_n| < M$ para todo o n. Escolhemos agora N tal que $|x_n - x_m| < \frac{\varepsilon}{2M}$ e $|y_n - y_m| < \frac{\varepsilon}{2M}$ quando $m, n \geq N$. Assim, se $m, n \geq N$,

$$\begin{aligned} |x_n y_n - x_m y_m| &= |x_n(y_n - y_m) + y_m(x_n - x_m)| \\ &\leq |x_n| \cdot |y_n - y_m| + |y_m| \cdot |x_n - x_m| \\ &< M \cdot \frac{\varepsilon}{2M} + M \cdot \frac{\varepsilon}{2M} = \varepsilon. \end{aligned}$$

Portanto $(x_n y_n)_n$ é uma sucessão de Cauchy e converge em $\widetilde{K}$.

Vamos agora provar que as operações estão bem definidas. Consideramos para isso uma segunda sucessão $(x'_n)_{n\geq 1}$ de elementos de K que converge para x. Como $(x_n)_n$ e $(x'_n)_n$ têm o mesmo limite, a distância entre x_n e x'_n tende para 0 (isto é válido em qualquer espaço métrico), ou seja,

$$\lim_{n\to\infty} |x_n - x'_n| = 0.$$

Mas então

$$\lim_{n\to\infty} |(x_n + y_n) - (x'_n + y_n)| = 0,$$

ou seja, a distância entre $x_n + y_n$ e $x'_n + y_n$ tende para 0. Isto implica que os limites das duas sucessões, a existirem, são iguais. Além disso,

$$\lim_{n\to\infty} |x_n y_n - x'_n y_n| = \lim_{n\to\infty} |y_n| \cdot |x_n - x'_n| = 0$$

uma vez que $(y_n)_n$ é limitada, logo os limites das sucessões $(x_n y_n)_n$ e $(x'_n y_n)_n$, a existirem, são iguais.

Falta provar que as operações definidas por (1.6) definem um corpo. Todas as propriedades das operações que não a existência de inversos aditivos e multiplicativos são obtidas pelas propriedades correspondentes em K "passando ao limite". Vamos provar apenas a propriedade distributiva para exemplificar, deixando as restantes como exercício. Sejam $x, y, z \in \widetilde{K}$. Considerem-se sucessões $(x_n)_{n\geq 1}$, $(y_n)_{n\geq 1}$ e $(z_n)_{n\geq 1}$ de elementos de K que tendem para x, y e z respetivamente. Então

$$x(y+z) = \lim_{n\to\infty} x_n(y_n + z_n) = \lim_{n\to\infty} (x_n y_n + x_n z_n) = xy + xz.$$

Seja agora $x \in \widetilde{K}$ e seja $(x_n)_{n\geq 1}$ uma sucessão de elementos de K que converge para x. Consideremos a sucessão $(-x_n)_n$; como

$$|(-x_n) - (-x_m)| = |x_n - x_m|$$

e a sucessão $(x_n)_n$ é de Cauchy, a sucessão $(-x_n)_n$ também é, logo converge em $\widetilde{K}$. O seu limite $-x$ satisfaz

$$x + (-x) = \lim_{n\to\infty} (x_n + (-x_n))_n = \lim_{n\to\infty} 0 = 0.$$

Isto mostra a existência de inversos aditivos.

Por fim, seja $x \neq 0$ um elemento de $\widetilde{K}$, e seja $(x_n)_n$ uma sucessão de elementos de K que converge para x. Aqui a situação é ligeiramente mais delicada. Não podemos simplesmente considerar a sucessão $\left(\frac{1}{x_n}\right)_n$; nada nos garante que todos os x_n são diferentes de 0. Rodeamos esta dificuldade da seguinte forma: apenas um número finito dos termos x_n são iguais a 0, caso contrário $(x_n)_n$ teria uma subsucessão formada por termos iguais a 0 e portanto o seu limite teria que ser igual a 0. Logo existe p tal que $x_n \neq 0$ para $n \geq p$. Substituindo a sucessão $(x_n)_{n\geq 1}$ pela sucessão $(x_{n+p})_{n\geq 1}$ obtemos outra sucessão que converge para x e não tem termos iguais a 0.

Podemos assim supor que $x_n \neq 0$ para todo o n; considere-se então a sucessão $\left(\frac{1}{x_n}\right)_n$. Afirmamos que é uma sucessão de Cauchy. Para o provar, observe-se que existe $\delta > 0$ tal que $|x_n| > \delta$ para todo o n, caso contrário $(x_n)_n$ teria uma subsucessão convergente para 0 (porquê?) e portanto o seu limite seria 0. Por fim, como $(x_n)_n$ é de Cauchy, existe N tal que $|x_m - x_n| < \varepsilon\delta^2$ para quaisquer $m, n \geq N$. Assim, se $m, n \geq N$,

$$\left|\frac{1}{x_m} - \frac{1}{x_n}\right| = \left|\frac{x_n - x_m}{x_m x_n}\right| = \frac{|x_n - x_m|}{|x_m| \cdot |x_n|} < \frac{\varepsilon\delta^2}{\delta \cdot \delta} = \varepsilon.$$

Portanto $\left(\frac{1}{x_n}\right)_n$ é de Cauchy, e converge em $\widetilde{K}$. Denotando o seu limite por x^{-1}, temos

$$xx^{-1} = \lim_{n\to\infty} x_n \cdot \frac{1}{x_n} = \lim_{n\to\infty} 1 = 1.$$

Isto mostra a existência de inversos multiplicativos.

Para provar (ii), dado $x \in \widetilde{K}$ definimos $|x| = d(x, 0)$, onde d é a métrica em $\widetilde{K}$. Sejam x e y quaisquer elementos de $\widetilde{K}$, e sejam $(x_n)_{n\geq 1}$ e $(y_n)_{n\geq 1}$ sucessões de elementos de K convergentes para x e y, respetivamente. Então

$$d(x, y) = \lim_{n\to\infty} d(x_n, y_n) = \lim_{n\to\infty} |x_n - y_n| = \lim_{n\to\infty} d(x_n - y_n, 0) = d(x - y, 0) = |x - y|.$$

Falta verificar que esta extensão de $|\cdot|$ define de facto um valor absoluto. Isso é obtido a partir das propriedades de $|\cdot|$ em K "passando ao limite". Por exemplo, como

$$|x_n + y_n| \leq |x_n| + |y_n|$$

para todo o n, o limite do lado esquerdo é menor ou igual ao limite do lado direito. Mas estes limites são $|x + y|$ e $|x| + |y|$ respetivamente. A compatibilidade com o produto é análoga. □

Não é difícil ver que esta é de facto a *única* maneira de definir as operações de corpo em $\widetilde{K}$ e a extensão do valor absoluto. De facto, num corpo valorado, as operações de soma e multiplicação são contínuas em relação à topologia induzida pelo valor absoluto. Isto garante que as operações de soma e multiplicação em $\widetilde{K}$ *têm que ser definidas* por 1.6. Podemos assim falar *no* corpo valorado $(\widetilde{K}, |\cdot|)$ que se obtém completando um corpo valorado $(K, |\cdot|)$.

Para terminar, vamos provar um Lema que nos diz algo sobre os valores tomados em $\mathbb{R}$ pelo valor absoluto do completamento de um corpo no caso não arquimediano.

Lema 1.5.2. *Seja $(K, |\cdot|)$ um corpo valorado não arquimediano, e seja $(\widetilde{K}, |\cdot|)$ o seu completamento[1]. Então os valores tomados por $|x|$ quando x percorre $\widetilde{K}$ são precisamente os valores tomados por $|x|$ quando x percorre K (por outras palavras, o contradomínio de $|\cdot|$ não adquire "valores novos" quando passamos ao completamento).*

A prova é essencialmente uma consequência do seguinte resultado auxiliar.

Proposição 1.5.3. *Seja $(a_n)_{n\geq 1}$ uma sucessão num corpo valorado não arquimediano $(K, |\cdot|)$ que converge para um limite $a \in K \setminus \{0\}$. Então existe um inteiro positivo N tal que, se $n \geq N$, então $|a_n| = |a|$.*

Demonstração. Como (a_n) converge para a e $|a| > 0$, existe um inteiro positivo N tal que, se $n \geq N$, então $|a_n - a| < |a|$. Para $n \geq N$ tem-se então

$$|a_n| \leq \max\{|a_n - a|, |a|\} = |a|$$

mas também

$$|a| = |a - a_n + a_n| \leq \max\{|a - a_n|, |a_n|\}.$$

Da segunda desigualdade decorre que $|a| \leq |a_n|$, já que $|a| > |a_n - a|$ por hipótese. Mas então da primeira vem que $|a_n| = |a|$, e isto vale para todo o $n \geq N$. □

[1] Cometemos aqui, como é frequente, o ligeiro abuso de notação de designar por $|\cdot|$ tanto o valor absoluto em K como a sua extensão ao completamento $\widetilde{K}$.

Prova do Lema 1.5.2. Seja x um elemento de $\widetilde{K}$. Queremos provar que existe $y \in K$ tal que $|y| = |x|$. Se $x = 0$ isso é óbvio. Caso contrário, considere-se uma sucessão $(x_n)_{n\geq 1}$ de elementos de K que converge para x. Pela proposição anterior tem-se $|x_n| = |x|$ para todo o n suficientemente grande, logo podemos tomar $y = x_n$ para um n apropriado. □

2. Os números p-ádicos

§2.1. A aritmética dos inteiros p-ádicos

A seguinte definição, nesta altura, não deve ser surpreendente.

Definição 2.1.1. Seja p um primo. O corpo $\mathbb{Q}_p$ é o completamento de $\mathbb{Q}$ em relação ao valor absoluto p-ádico $|\cdot|_p$, e chama-se o *corpo dos números p-ádicos*.

Neste momento, a definição de $\mathbb{Q}_p$ que temos é demasiado abstrata para podermos trabalhar facilmente com ela; nesta secção vamos tentar ganhar alguma intuição mais concreta sobre "com que se parecem" os p-ádicos.

Observação 2.1.2. Pelo Lema 1.5.2, para todo o $x \in \mathbb{Q}_p \setminus \{0\}$ temos $|x| = p^{-n}$ para algum inteiro n. Podemos assim definir $v_p(x) = n$, estendendo a definição da valoração p-ádica em $\mathbb{Q}$ (Definição 1.2.4).

De modo a estudar propriedades algébricas dos p-ádicos, vamos focar-nos num subanel especial, os *inteiros p-ádicos*.

Definição 2.1.3. Seja p um primo. O *anel dos inteiros p-ádicos* $\mathbb{Z}_p$ é definido por

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

É imediato verificar que $\mathbb{Z}_p$ é de facto um anel, e que $\mathbb{Z} \subseteq \mathbb{Z}_p$; de facto podemos pensar em $\mathbb{Z}_p$ como o "completamento p-ádico" de $\mathbb{Z}$ da mesma forma que $\mathbb{Q}_p$ é o completamento p-ádico de $\mathbb{Q}$. Esse é essencialmente o conteúdo da proposição seguinte.

Proposição 2.1.4. *$\mathbb{Z}_p$ é a aderência topológica de $\mathbb{Z}$ em $\mathbb{Q}_p$.*

Demonstração. É imediato que $\mathbb{Z}_p$ é fechado, sendo uma bola fechada no espaço métrico $\mathbb{Q}_p$. Resta mostrar que é de facto o *menor* fechado em $\mathbb{Q}_p$ que contém $\mathbb{Z}$.

Para isso, basta provar que, para qualquer $x \in \mathbb{Z}_p$ (sem perda de generalidade, $x \neq 0$) e qualquer $\varepsilon > 0$, existe $n \in \mathbb{Z}$ tal que $|x - n|_p < \varepsilon$. Para tal, notamos que, como $\mathbb{Q}$ é denso em $\mathbb{Q}_p$, existe uma sucessão $(x_k)_{k\geq 1}$ de racionais que converge para x. Pela Proposição 1.5.3 existe N tal que, se $k \geq N$, então $|x_k| = |x| \leq 1$. Como a sucessão converge para x existe $k \geq N$ tal que $|x - x_k| < \varepsilon$.

Portanto, em resumo, sendo $m = x_k$, m é um racional com $|x - m|_p < \varepsilon$ e $|m|_p \leq 1$. Será que m é o inteiro n que procurávamos? Infelizmente, não necessariamente, pois a condição $|m|_p \leq 1$ não garante que m seja um inteiro. Na verdade, tendo em conta a definição de $|\cdot|_p$, só garante que

$$m = \frac{a}{b} \text{ com } a \text{ e } b \text{ inteiros e } p \nmid b.$$

Então precisamos de aproximar m por sua vez por um inteiro. Para isso, seja r um inteiro não negativo tal que $p^{-r} < \varepsilon$, e observemos que, como p não divide b, p^r e b são coprimos, e pelo Teorema de Bézout existem inteiros y e z com

$$by + p^r z = 1.$$

Logo

$$|m - ay|_p = \left|\frac{a}{b} - ay\right|_p = \left|\frac{a(1-by)}{b}\right|_p = \left|\frac{ap^r z}{b}\right|_p \leq p^{-r} < \varepsilon.$$

Ou seja, sendo $n = ay$, n é de facto um inteiro e $|m - n|_p < \varepsilon$. Por fim,

$$|x - n|_p \leq \max\{|x - m|_p, |m - n|_p\} < \varepsilon$$

concluindo a prova. □

Vamos então estudar algumas propriedades algébricas do anel $\mathbb{Z}_p$. Começamos por determinar os elementos invertíveis:

Proposição 2.1.5 (Unidades de $\mathbb{Z}_p$)**.** *O grupo $\mathbb{Z}_p^\times$ dos elementos invertíveis de $\mathbb{Z}_p$ é*

$$U_p = \{x \in \mathbb{Z}_p : |x|_p = 1\}.$$

Demonstração. Seja x um elemento invertível de $\mathbb{Z}_p$, e seja y o seu inverso. Então

$$1 = |xy|_p = |x|_p |y|_p.$$

Como $|x|_p$ e $|y|_p$ são menores ou iguais a 1, a igualdade anterior só pode ocorrer se $|x|_p = |y|_p = 1$. Em particular, $x \in U_p$.

Reciprocamente, suponha-se que $x \in U_p$. Então $x \neq 0$ e existe $y \in \mathbb{Q}_p$ tal que $xy = 1$. Mas então $1 = |xy|_p = |x|_p |y|_p$, pelo que, como $|x|_p = 1$, também se tem $|y|_p = 1$. Logo $y \in \mathbb{Z}_p$, e x é invertível em $\mathbb{Z}_p$. □

Isto implica em particular que muitos inteiros que não são invertíveis em $\mathbb{Z}$ passam a ser invertíveis em $\mathbb{Z}_p$; de facto, todos os inteiros não divisíveis por p são invertíveis em $\mathbb{Z}_p$. Portanto, de certo modo, os primos diferentes de p perdem "peso aritmético" quando passamos de $\mathbb{Z}$ para $\mathbb{Z}_p$.

Vamos sentir agora o efeito dessa perda ao estudar os ideais de $\mathbb{Z}_p$. De facto, os ideais em $\mathbb{Z}$ gerados por elementos não divisíveis por p vão "perder-se" (no sentido de deixarem de ser ideais próprios) quando passamos de $\mathbb{Z}$ para $\mathbb{Z}_p$, e sobram apenas os ideais gerados por potências de p.

Proposição 2.1.6 (Ideais de $\mathbb{Z}_p$)**.** *Os ideais de $\mathbb{Z}_p$ são (0) e os conjuntos da forma*

$$p^n \mathbb{Z}_p = \{p^n x : x \in \mathbb{Z}_p\}$$

com n inteiro não negativo.

Demonstração. Que estes conjuntos são de facto ideais é imediato. Suponha-se agora que $\mathfrak{a}$ é um ideal não nulo de $\mathbb{Z}_p$, e seja x um elemento de valor absoluto p-ádico máximo em $\mathbb{Z}_p$ (por que razão existe x?)

Seja $|x| = p^{-n}$, com $n \geq 0$. Afirmamos que $\mathfrak{a} = p^n \mathbb{Z}_p$.

Em primeiro lugar, se $y \neq 0$ pertence a $\mathfrak{a}$ então $|y| \leq |x| = p^{-n}$ por definição de x. Logo,

$$\left|\frac{x}{p^n}\right|_p \leq 1$$

e portanto $\frac{x}{p^n} \in \mathbb{Z}_p$, e $x \in p^n\mathbb{Z}_p$. Isto mostra que $\mathfrak{a} \subseteq p^n\mathbb{Z}_p$.

Reciprocamente, seja $y \in p^n\mathbb{Z}_p$. Então $|y|_p \leq p^{-n} = |x|_p$, logo $\left|\frac{y}{x}\right|_p \leq 1$. Então $\frac{y}{x} \in \mathbb{Z}_p$, e como $x \in \mathfrak{a}$ resulta que $y = x \cdot \frac{y}{x} \in \mathfrak{a}$ (porque $\mathfrak{a}$ é um ideal). Isto mostra que $p^n\mathbb{Z}_p \subseteq \mathfrak{a}$.

Logo $\mathfrak{a} = p^n\mathbb{Z}_p$. □

Em particular, conclui-se da proposição anterior que $\mathbb{Z}_p$ é um domínio de ideais principais (todos os ideais são principais), e além disso que possui um único ideal maximal, que é $p\mathbb{Z}_p$. Anéis com um único ideal maximal são conhecidos como *anéis locais*.

Vamos de seguida descrever os quocientes de $\mathbb{Z}_p$ pelos seus ideais.

Proposição 2.1.7 (Quocientes de $\mathbb{Z}_p$)**.** *Para todo o inteiro não negativo n, existe um isomorfismo*

$$\mathbb{Z}/p^n\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}_p/p^n\mathbb{Z}_p$$

$$a + p^n\mathbb{Z} \longmapsto a + p^n\mathbb{Z}_p.$$

Demonstração. Consideramos o homomorfismo composto $f : \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ dado por

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathbb{Z}_p \\ & & \downarrow \\ & & \mathbb{Z}_p/p^n\mathbb{Z}_p \end{array}$$

onde o primeiro homomorfismo é a inclusão natural e o segundo é a projeção canónica de $\mathbb{Z}_p$ em $\mathbb{Z}_p/p^n\mathbb{Z}_p$.

Este homomorfismo envia $a \in \mathbb{Z}$ em $a + p^n\mathbb{Z}_p$. Temos portanto $a \in \mathrm{Ker}(f)$ se e só se $a \in p^n\mathbb{Z}_p$. Isto equivale a ter-se $v_p(a) \geq n$, o que para um inteiro a significa precisamente que $a \in p^n\mathbb{Z}$. Logo $\mathrm{Ker}(f) = p^n\mathbb{Z}$, e o primeiro teorema do isomorfismo dá-nos um homomorfismo injetivo φ que encaixa no diagrama abaixo.

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathbb{Z}_p \\ \downarrow & & \downarrow \\ \mathbb{Z}/p^n\mathbb{Z} & \xhookrightarrow{\varphi} & \mathbb{Z}_p/p^n\mathbb{Z}_p \end{array}$$

É imediato que $\varphi(a + p^n\mathbb{Z}) = a + p^n\mathbb{Z}_p$, logo resta-nos verificar que φ é sobrejetivo. Essa é na verdade a essência da prova. Queremos provar que qualquer classe de congruência em $\mathbb{Z}_p/p^n\mathbb{Z}_p$ tem um representante inteiro; ou seja, que dado qualquer $x \in \mathbb{Z}_p$ existe $a \in \mathbb{Z}$ tal que $x - a$ é divisível por p^n em $\mathbb{Z}_p$.

Mas pela Proposição 2.1.4 $\mathbb{Z}$ é denso em $\mathbb{Z}_p$, e em particular existe $a \in \mathbb{Z}$ tal que $|x-a|_p \leq p^{-n}$. Isto equivale precisamente a ter-se $p^n \mid x - a$ em $\mathbb{Z}_p$, como pretendido. □

Portanto, embora $\mathbb{Z}_p$ seja estritamente maior do que $\mathbb{Z}$, quando vemos módulo p^n não conseguimos ver a diferença, por muito grande que seja n. Vamos ver como a proposição anterior nos dá uma maneira muito concreta de pensar nos elementos de $\mathbb{Z}_p$.

Proposição 2.1.8 (Expansão em base p em $\mathbb{Z}_p$)**.** *Qualquer $a \in \mathbb{Z}_p$ pode ser escrito de maneira única na forma*

$$a = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots = \sum_{j=0}^{\infty} a_j p^j \tag{2.1}$$

onde os a_i's são inteiros com $0 \leq a_j < p$. Reciprocamente, para quaisquer a_i's nestas condições, a série anterior converge para um inteiro p-ádico.

Demonstração. Seja $a \in \mathbb{Z}_p$. Pela Proposição 2.1.7, existe $a_0 \in \mathbb{Z}$ tal que $a \equiv a_0 \pmod{p}$, e podemos escolher a_0 de modo que $0 \leq a_0 < p$. Desta forma $a - a_0 = x_1 p$ para algum $x_1 \in \mathbb{Z}_p$, e temos

$$a = a_0 + x_1 p.$$

Novamente, temos $x_1 \equiv a_1 \pmod{p}$ para algum inteiro a_1 com $0 \leq a_1 < p$, pela Proposição 2.1.7, e assim podemos escrever $x_1 = a_1 + x_2 p$ com $x_2 \in \mathbb{Z}_p$. Assim temos

$$a = a_0 + a_1 p + x_2 p^2.$$

Continuando este processo, obtemos para cada k uma igualdade

$$a = a_0 + a_1 p + \cdots + a_{k-1} p^{k-1} + x_k p^k$$

com $0 \leq a_i < p$ para cada i, e desta forma

$$|a - (a_0 + a_1 p + \cdots + a_{k-1} p^{k-1})|_p \leq p^{-k}$$

pelo que $|a - (a_0 + a_1 p + \cdots + a_{k-1} p^{k-1})|_p$ tende para 0 quando k tende para infinito. Isto significa precisamente que a série

$$\sum_{j=0}^{\infty} a_j p^j$$

converge para a.

Para provar unicidade, provamos por indução em k que a_k é unicamente determinado por a. Obviamente a_0 é unicamente determinado pois em (2.1) temos $a \equiv a_0 \pmod{p}$ e cada classe de congruência em $\mathbb{Z}/p\mathbb{Z}$ (e, portanto, pela Proposição 2.1.7, em $\mathbb{Z}/p\mathbb{Z}$) tem um único representante inteiro em $\{0, \ldots, p-1\}$. Suponha-se agora que $a_0, \ldots, a_{k-1}$ são unicamente determinados, e observemos que (2.1) se pode reescrever como

$$\frac{a - (a_0 + \cdots + a_{k-1} p^{k-1})}{p^k} = a_k + a_{k+1} p + a_{k+2} p^2 + \cdots.$$

Portanto temos

$$a_k \equiv \frac{a - (a_0 + \cdots + a_{k-1} p^{k-1})}{p^k} \pmod{p}$$

e, como vimos antes, só existe um inteiro $a_k \in \{0, \ldots, p-1\}$ com essa propriedade.

Por fim, a convergência de uma série do tipo apresentado em (2.1) é uma consequência trivial da Propisição 1.4.2. □

Como sabemos, qualquer inteiro positivo a admite uma representação em base p; isso equivale a ter-se uma igualdade do tipo (2.1) em que a soma do lado direito é *finita*, ou seja, $a_i = 0$ para todo o i suficientemente grande. Para os inteiros p-ádicos, temos uma representação do mesmo tipo, mas potencialmente infinita.

Outra maneira de pensar em $\mathbb{Z}_p$

Consideremos os anéis $\mathbb{Z}/p^n\mathbb{Z}$, com n inteiro positivo. Para cada n, temos um homomorfismo natural $\pi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ (essencialmente, dado um inteiro reduzido módulo p^{n+1}, podemos "reduzi-lo ainda mais", módulo p^n). Podemos encaixar estes homomorfismos uns nos outros, como no seguinte diagrama:

$$\cdots \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}/p^5\mathbb{Z} \xrightarrow{\pi_4} \mathbb{Z}/p^4\mathbb{Z} \xrightarrow{\pi_3} \mathbb{Z}/p^3\mathbb{Z} \xrightarrow{\pi_2} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\pi_1} \mathbb{Z}/p\mathbb{Z}$$

Vamos dizer que uma sequência $(x_n)_{n\geq 1}$, com $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ para cada n, é *compatível* se $\pi_n(x_{n+1}) = x_n$ para cada n, ou seja, se x_n for obtido "reduzindo x_{n+1} módulo p^n" para cada n.

Seja agora x um inteiro, e considere-se a sequência $x_n = x + p^n\mathbb{Z}$. Então obviamente $(x_n)_{n\geq 1}$ é uma sequência compatível. Será que qualquer sequência compatível pode ser obtida desta forma? O exemplo seguinte mostra que não.

Exemplo 2.1.9. Seja $p = 3$, e seja $x_n = 1 + 3 + 3^2 + \cdots + 3^{n-1}$. Afirmamos que esta sequência não se obtém reduzindo um mesmo inteiro módulo 3^n para cada n, ou seja, que não existe um inteiro x tal que

$$x \equiv x_n \pmod{3^n} \quad \text{para cada } n.$$

Suponhamos por absurdo que existe um tal inteiro. Então, para cada n, temos $2x + 1 \equiv 2x_n + 1 \pmod{3^n}$. Mas

$$2x_n + 1 = 2 \cdot \frac{3^n - 1}{2} + 1 = 3^n \equiv 0 \pmod{3^n}.$$

Portanto temos $2x + 1 \equiv 0 \pmod{3^n}$ para *qualquer* n, ou seja, $2x + 1$ é divisível por todas as potências de 3. Isto é absurdo porque o único inteiro divisível por todas as potências de 3 é 0, que não é da forma $2x + 1$ com x inteiro!

O leitor já deve estar a imaginar para onde estamos a caminhar; se substituirmos $\mathbb{Z}$ por $\mathbb{Z}_p$, o caso muda de figura. Mantendo a sequência $(x_n)_n$ do exemplo anterior, o inteiro 3-ádico

$$1 + 3 + 3^2 + 3^3 + \cdots$$

(que é igual a $-\frac{1}{2}$, mas isso não interessa) reduz-se módulo 3^n para x_n para cada n! E, de facto, isso não é coincidência; se substituirmos inteiros por inteiros p-ádicos, *qualquer* sequência compatível $(x_n)_{n\geq 1}$ com $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ para cada n passa a ser obtida reduzindo um mesmo número módulo p^n para cada n, considerando a identificação natural da Proposição 2.1.7 entre $\mathbb{Z}/p^n\mathbb{Z}$ e $\mathbb{Z}_p/p^n\mathbb{Z}_p$ (reparando assim um "defeito" de $\mathbb{Z}$).

Proposição 2.1.10. *Seja $(x_n)_{n\geq 1}$ uma sequência compatível (com $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ para cada n). Então existe $x \in \mathbb{Z}_p$ tal que*

$$x \equiv x_n \pmod{p^n}$$

para todo o inteiro positivo n.

Ideia da prova. Para cada n, seja X_n um elemento *qualquer* de $\mathbb{Z}_p$ tal que a projeção de X_n em $\mathbb{Z}/p^n\mathbb{Z}$ é igual a x_n. A condição de compatibilidade garante que

$$X_n \equiv X_m \pmod{p^m} \quad \text{sempre que } n \geq m.$$

Ou seja, $|X_n - X_m|_p \leq p^{-m}$, e isto mostra que $(X_n)_{n\geq 1}$ é uma sucessão de Cauchy. Como $\mathbb{Z}_p$ é completo, esta sucessão converge em $\mathbb{Z}_p$, e o seu limite x tem a propriedade pretendida. □

Vamos olhar novamente para o diagrama seguinte:

$$\cdots \twoheadrightarrow \mathbb{Z}/p^5\mathbb{Z} \xrightarrow{\pi_4} \mathbb{Z}/p^4\mathbb{Z} \xrightarrow{\pi_3} \mathbb{Z}/p^3\mathbb{Z} \xrightarrow{\pi_2} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{\pi_1} \mathbb{Z}/p\mathbb{Z}$$

Uma maneira de interpretar a proposição anterior é imaginar que $\mathbb{Z}_p$ está no "extremo esquerdo" deste diagrama. Num certo sentido, $\mathbb{Z}_p$ é o *limite* dos anéis $\mathbb{Z}/p^n\mathbb{Z}$ quando n tende para infinito. Existe um conceito de Teoria das Categorias (o conceito de *limite inverso* ou *limite projetivo*, denotado $\varprojlim$) que formaliza esta intuição:

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

Mais uma curiosidade: usando a proposição anterior, podemos identificar elementos de $\mathbb{Z}_p$ com sequências compatíveis $(x_n)_n$. Essas sequências podem ser vistas como elementos do produto cartesiano

$$\prod_n \mathbb{Z}/p^n\mathbb{Z}.$$

Ora, neste produto cartesiano temos uma topologia natural: a topologia produto resultante de munir cada fator com a topologia discreta. O conjunto das sequências compatíveis fica assim com uma topologia induzida, e essa topologia coincide com a topologia p-ádica em $\mathbb{Z}_p$! A prova fica como exercício para o leitor...

§2.2. O Lema de Hensel

Nesta secção e na próxima vamos abordar o problema de resolver equações polinomiais em $\mathbb{Q}_p$ e $\mathbb{Z}_p$. O instrumento principal será um resultado fundamental sobre o anel $\mathbb{Z}_p$ (que também é válido para outros anéis com propriedades semelhantes), conhecido como o *Lema de Hensel* (em homenagem ao inventor/descobridor dos p-ádicos, Kurt Hensel).

Suponhamos que temos um polinómio $f \in \mathbb{Z}_p[X]$ e queremos saber se a equação

$$f(x) = 0$$

tem uma solução em $\mathbb{Z}_p$. Se tiver, então em particular a congruência

$$f(x) \equiv 0 \pmod{p}$$

tem uma solução. Por outras palavras, se $\overline{f}$ designar o polinómio em $(\mathbb{Z}_p/p\mathbb{Z}_p)[X] = \mathbb{F}_p[X]$ obtido reduzindo os coeficientes de f módulo p, então a equação $\overline{f}(x) = 0$ tem uma solução em $\mathbb{F}_p$.

À partida não temos nenhuma razão para esperar que a implicação contrária seja verdadeira. Afinal, a afirmação "$f(x)$ é múltiplo de p" parece à primeira vista muito mais fraca do que a afirmação "$f(x)$ é igual a 0". A magia dos inteiros p-ádicos é que, surpreendentemente, esta implicação é de facto "quase verdadeira"; isto é, é verdadeira em condições bastante gerais! Esse é o conteúdo do Lema de Hensel.

Vamos começar por refletir um pouco sobre um exemplo muito concreto deste fenómeno. Quem já estudou Teoria dos Números está familiarizado com o problema de decidir se um inteiro é ou não um *resíduo quadrático* módulo um primo p. Isto é, dado um primo p e um inteiro a, podemos perguntar-nos se a é um quadrado módulo p, ou seja, se existe x tal que $x^2 \equiv a \pmod{p}$. Por outras palavras, queremos saber se a equação $f(x) = 0$ tem solução em $\mathbb{F}_p$, onde

$$f(X) = X^2 - a.$$

Existe uma vasta teoria sobre estas equações quadráticas módulo primos, e em particular existe uma maneira bastante rápida de decidir se a equação/congruência anterior tem solução ou não, usando autênticas jóias da Teoria dos Números como a fantástica Lei da Reciprocidade Qudrática. Mas a maior parte dos textos introdutórios de Teoria dos Números deixa de lado uma questão natural: *e se o módulo não for primo*?

Usando o Teorema Chinês dos Restos é fácil reduzir a questão da solubilidade de $x^2 \equiv a \pmod{n}$ ao caso em que n é uma potência de um primo, digamos $n = p^k$. Portanto a questão natural é a seguinte: dá para desenvolver uma teoria análoga para decidir se a congruência $x^2 \equiv a \pmod{p^k}$ tem solução?

A resposta é um pouco inesperada: sim, dá, e na verdade, em geral, ao decidirmos se a congruência $x^2 \equiv a \pmod{p}$ já tem solução já fazemos praticamente o trabalho todo. Ou seja, em geral, se a congruência $x^2 \equiv a \pmod{p}$ tem solução, então a congruência $x^2 \equiv a \pmod{p^k}$ tem solução para todo o k! Vamos ver um exemplo para ganhar alguma intuição sobre o que acontece.

Exemplo 2.2.1. Suponhamos que queremos resolver a congruência $x^2 \equiv 2 \pmod{7^4}$. A congruência "mais simples" $x^2 \equiv 2 \pmod{7}$ tem a solução $x = 3$. Vamos tentar resolver

um problema intermédio, e procurar uma solução de $x^2 \equiv 2 \pmod{7^2}$. Como em particular queremos $x^2 \equiv 2 \pmod 7$, é natural procurar x de modo que $x \equiv 3 \pmod 7$, e portanto procuramos soluções da forma $x = 3 + 7k$. A congruência fica assim

$$(3+7k)^2 \equiv 2 \pmod{7^2} \quad \text{ou seja,} \quad 3^2 + 42k + 7^2k^2 \equiv 2 \pmod{7^2}.$$

Podemos simplificar um pouco; a parcela 7^2k^2 é 0 módulo 7^2 e pode ser eliminada, ficando-se assim com

$$42k + 7 \equiv 0 \pmod{7^2} \quad \text{ou, dividindo por 7,} \quad 6k + 1 \equiv 0 \pmod 7.$$

Ou seja, a nossa congruência quadrática módulo 7^2 transformou-se numa congruência linear módulo 7! E congruências como a anterior têm sempre solução, que pode ser facilmente encontrada com o Algoritmo de Euclides; neste caso uma solução é $k = 1$, e obtemos a solução

$$x = 3 + 7k = 10$$

para a congruência $x^2 \equiv 2 \pmod{7^2}$!

Isto funcionou muito bem, portanto vamos levar tudo um nível acima e tentar adaptar o método para resolver $x^2 \equiv 2 \pmod{7^3}$. Tendo em conta que em particular queremos que a congruência se verifique módulo 7^2 e o nosso resultado anterior, é natural escolher $x \equiv 10 \pmod{7^2}$; procuramos então uma solução da forma $x = 10 + 7^2k$. A congruência fica

$$(10 + 7^2k)^2 \equiv 2 \pmod{7^3} \quad \text{ou seja,} \quad 980k + 98 \equiv 0 \pmod{7^3}.$$

As parcelas do lado esquerdo são divisíveis por 7^2 (e isso não é concidência!), portanto podemos dividir tudo por 7^2 e ficamos com

$$20k + 2 \equiv 0 \pmod 7.$$

Mais uma congruência linear simplicíssima! Desta vez $k = 2$ resolve isto, e obtemos a solução

$$x = 10 + 7^2k = 108.$$

Estamos quase; só precisamos de subir mais um nível para resolver a congruência original $x^2 \equiv 2 \pmod{7^4}$. Naturalmente, procuramos uma solução da forma $x = 108 + 7^3k$, e a congruência fica

$$11662 + 74088k \equiv 0 \pmod{7^4}$$

mas as parcelas do lado esquerdo são divisíveis por 7^3, e então obtemos

$$34 + 216k \equiv 0 \pmod 7 \text{ ou seja, } 6 + 6k \equiv 0 \pmod 7.$$

Desta vez a solução é $k = 6$, e obtemos

$$x = 108 + 7^3k = 2166$$

que é uma solução da congruência original!

Notemos que, tendo em conta os passos pelos quais obtivemos a solução x final, é natural reescrevê-la como

$$x = 3 + 1 \times 7 + 2 \times 7^2 + 6 \times 7^3.$$

Isto é a cauda de uma expansão em base p, e podemos imaginar que, ao iterar este processo, estamos a construir passo a passo um inteiro 7-ádico! E esse inteiro 7-ádico vai ser uma solução da equação $x^2 = 2$ em $\mathbb{Z}_7$. É essa a ideia por detrás do Lema de Hensel; algo tão simples como uma solução em $\mathbb{F}_7$ leva a uma solução em $\mathbb{Z}_7$.

Encontrar uma raiz de um polinómio permite-nos fatorizar um polinómio; se α é uma raiz de $f(X)$ então $f(X)$ é divisível por $X - \alpha$. Portanto podemos pensar no problema de fatorizar polinómios como um problema que generaliza o de resolver equações polinomiais. Vamos assim enunciar e provar a nossa primeira versão do Lema de Hensel neste contexto mais geral: uma fatorização de um polinómio em $\mathbb{F}_p$ leva a uma fatorização de um polinómio em $\mathbb{Z}_p$.

Lema 2.2.2 (Lema de Hensel, versão 1)**.** *Seja p um primo e seja $f \in \mathbb{Z}_p[X]$ um polinómio. Seja $\overline{f}$ o polinómio em $\mathbb{F}_p[X]$ obtido reduzindo f módulo p coeficiente a coeficiente. Suponha-se que existem polinómios ϕ_1 e ϕ_2 em $\mathbb{F}_p[X]$, primos entre si, tais que*

$$\overline{f} = \phi_1 \phi_2.$$

Então existem polinómios $f_1, f_2 \in \mathbb{Z}_p[X]$ tais que $f_1 \equiv \phi_1 \pmod{p}$, $f_2 \equiv \phi_2 \pmod{p}$, $\deg(f_1) = \deg(\phi_1)$, e

$$f = f_1 f_2.$$

(Em poucas palavras: se um polinómio em $\mathbb{Z}_p[X]$ "fatoriza módulo p (em fatores coprimos!)" então fatoriza mesmo em $\mathbb{Z}_p[X]$.)

Demonstração. Vamos construir duas sucessões de polinómios em $\mathbb{Z}_p[X]$, digamos $(f_1^{(n)})_{n\geq 1}$ e $(f_2^{(n)})_{n\geq 1}$, com as seguintes propriedades:

(i) $\deg(f_1^{(n)}) = \deg(\phi_1)$ e $\deg(f_2^{(n)}) \leq \deg(f) - \deg(\phi_1)$ para cada $n \geq 1$;

(ii) $f_1^{(n)} \equiv \phi_1 \pmod{p}$ e $f_2^{(n)} \equiv \phi_2 \pmod{p}$ para cada n (as congruências são consideradas coeficiente a coeficiente);

(iii) $f \equiv f_1^{(n)} f_2^{(n)} \pmod{p^n}$ para cada n;

(iv) $f_1^{(n+1)} \equiv f_1^{(n)} \pmod{p^n}$ e $f_2^{(n+1)} \equiv f_2^{(n)} \pmod{p^n}$ para cada n.

Se conseguirmos construir estes polinómios, o Lema segue: a sucessão de polinómios $f_1^{(n)}$ é uma sucessão de Cauchy em $\mathbb{Z}_p$ pela condição (iv), no sentido de que a sucessão dos coeficientes de cada grau é uma sucessão de Cauchy, e portanto a sucessão $f_1^{(n)}$ converge para um polinómio, no sentido de que a sucessão dos coeficientes de cada grau converge, pela completude de $\mathbb{Z}_p$. Seja esse polinómio f_1. O mesmo acontece com os polinómios $f_2^{(n)}$: a sucessão que formam converge para um polinómio f_2, no sentido de que a convergência ocorre coeficiente a coeficiente. (Para isto é essencial a condição (i), que garante que os graus dos $f_i^{(n)}$ são limitados; caso contrário não teríamos a garantia de que f_1 e f_2 só têm um número finito de coeficientes diferentes de 0.) A condição (iii) garante que os produtos $f_1^{(n)} f_2^{(n)}$ convergem para f, o que garante que $f_1 f_2 = f$. Por fim, a condição $f_1 \equiv \phi_1 \pmod{p}$ e $f_2 \equiv \phi_2 \pmod{p}$ resulta de (ii).

Vamos então provar que existem os $f_1^{(n)}$ e $f_2^{(n)}$. A construção será feita por indução. Para $n = 1$, simplesmente escolhemos *quaisquer* polinómios $f_1^{(1)}$ e $f_2^{(1)}$ que módulo p sejam iguais a ϕ_1 e ϕ_2 respetivamente (tendo o cuidado de garantir a condição (i)).

Suponhamos agora que já escolhemos $f_1^{(n)}$ e $f_2^{(n)}$. Procuramos polinómios $f_1^{(n+1)}$ e $f_2^{(n+1)}$ da forma

$$f_1^{(n+1)} = f_1^{(n)} + p^n g_1,\ f_2^{(n+1)} = f_2^{(n)} + p^n g_2. \tag{2.2}$$

Isto garante automaticamente a condição (iv), logo resta-nos provar que podemos escolher g_1 e g_2 de tal modo que as condições (i) e (iii) sejam satisfeitas. Queremos assim que

$$f \equiv (f_1^{(n)} + p^n g_1)(f_2^{(n)} + p^n g_2) \pmod{p^{n+1}}$$

e expandindo e notando que $p^{2n} \equiv 0 \pmod{p^{n+1}}$, isto simplifica para

$$f - f_1^{(n)} f_2^{(n)} \equiv p^n (f_2^{(n)} g_1 + f_1^{(n)} g_2) \pmod{p^{n+1}}.$$

Pela hipótese de indução $f - f_1^{(n)} f_2^{(n)}$ é divisível por p^n, logo podemos escrever $f - f_1^{(n)} f_2^{(n)} = p^n h$ para algum polinómio h, e a congruência fica

$$p^n h \equiv p^n (f_2^{(n)} g_1 + f_1^{(n)} g_2) \pmod{p^{n+1}},$$

o que, cancelando p^n, fica

$$h \equiv f_2^{(n)} g_1 + f_1^{(n)} g_2 \pmod{p}.$$

Esta é uma congruência módulo p, e temos $f_1^{(n)} \equiv \phi_1 \pmod{p}$ e $f_2^{(n)} \equiv \phi_2 \pmod{p}$, portanto a condição fica

$$\overline{h} = \phi_2 \overline{g_1} + \phi_1 \overline{g_2} \text{ em } \mathbb{F}_p[X]$$

onde a barra superior indica redução módulo p. E agora estamos quase: os polinómios ϕ_1 e ϕ_2 em $\mathbb{F}_p[X]$ são coprimos por hipótese, logo qualquer polinómio em $\mathbb{F}_p[X]$ (em particular, $\overline{h}$) se pode escrever como combinação linear deles. Isso garante que conseguimos encontrar g_1 e g_2. Só precisamos de nos assegurar de que podemos fazê-lo de tal modo que $\deg(g_1) \leq \deg(\phi_1)$ e $\deg(g_2) \leq \deg(f) - \deg(\phi_1)$ (de modo a garantir (ii), tendo em conta (2.2)). Este é apenas um detalhe técnico; o núcleo da prova já acabou.

Portanto sabemos que podemos escrever

$$\overline{h} = \phi_2 \psi_1 + \phi_1 \psi_2 \tag{2.3}$$

em $\mathbb{F}_p[X]$ para alguns polinómios ψ_1 e ψ_2, mas queremos fazê-lo com certas limitações nos graus de ψ_1 e ψ_2. A ideia é que, dados ψ_1 e ψ_2 que cumpram a igualdade anterior, podemos substituí-los por $\psi_1' = \psi_1 - q\phi_1$ e $\psi_2' = \psi_2 + q\phi_2$ para qualquer polinómio $q \in \mathbb{F}_p[X]$ e a igualdade continua a verificar-se; ora, usando divisão com resto, podemos escolher q de modo que

$$\deg(\psi_1') = \deg(\psi_1 - q\phi_1) < \deg(\phi_1).$$

Ou seja, temos uma solução de (2.3) com $\deg(\psi_1) < \deg(\phi_1)$. Está quase; falta só ver que a restrição no grau de ψ_2 segue automaticamente. Mas isso é fácil: tendo em conta a definição de h e a hipótese de indução, é claro que $\deg(h) \leq \deg(f)$. Além disso, $\deg(\phi_2\psi_1) < \deg(\phi_2) + \deg(\psi_1) \leq \deg(\phi_1\phi_2) \leq \deg(f)$. Portanto

$$\deg(\overline{h} - \phi_2\psi_1) \leq \deg(f), \text{ ou seja, } \deg(\phi_1\psi_2) \leq \deg(f).$$

Isto significa precisamente que $\deg(\psi_2) \leq \deg(f) - \deg(\phi_1)$, e isto conclui a prova. □

Depois desta prova longa e com notação carregada, vamos ver algumas consequências curiosas. A primeira é um critério de irredutibilidade de polinómios em $\mathbb{Q}_p[X]$.

Proposição 2.2.3. *Seja $f(X) = a_nX^n + \cdots + a_0$ um polinómio em $\mathbb{Q}_p[X]$. Se f é irredutível, então o coeficiente de f com maior valor absoluto p-ádico (ou com menor v_p) é a_n ou a_0.*

Demonstração. Seja $\nu_i = v_p(a_i)$ para $i = 0, \ldots, n$. Seja k tal que $\nu = \nu_k$ é mínimo (se houver vários, escolhemos o menor k), e suponha-se por absurdo que $\nu_k < \nu_0$ e $\nu_k < \nu_n$. Consideramos o polinómio

$$g(X) = p^{-\nu} f(X) = b_nX^n + \cdots + b_0$$

onde $b_i = p^{-\nu}a_i$ para cada i. Basta provar que $g(X)$ não é irredutível (multiplicar por $p^{-\nu}$ não afeta a irredutibilidade), mas agora $v_p(b_i) = \nu_i - \nu$ para cada i; ou seja, tendo em conta a definição de ν, todos os $v_p(b_i)$ são maiores ou iguais a 0 (portanto $b_i \in \mathbb{Z}_p$), e além disso $v_p(b_k) = 0$ e $v_p(b_i) > 0$ para $i < k$, pela minimalidade de k.

Portanto b_k *não* se reduz a 0 em $\mathbb{F}_p$, mas $b_0, \ldots, b_{k-1}$ reduzem-se, e assim a redução de g módulo p é

$$\overline{g}(X) = \overline{b_n}X^n + \cdots + \overline{b_k}X^k = X^k(\overline{b_n}X^{n-k} + \cdots + \overline{b_k}).$$

Ou seja, módulo p fatorizámos g como produto de dois polinómios primos entre si! O Lema de Hensel garante portanto que podemos escrever $g = g_1g_2$ em $\mathbb{Z}_p[X]$, com $\deg(g_1) = \deg(X^k) = k$. Como $k \neq 0, n$ isto garante que g não é irredutível. □

Vamos agora adaptar o Lema de Hensel ao nosso objetivo original de resolver equações polinomiais. O resultado que vamos apresentar também é referido muitas vezes como o Lema de Hensel.

Lema 2.2.4 (Lema de Hensel, versão 2)**.** *Seja $f(X) \in \mathbb{Z}_p[X]$ um polinómio. Suponha-se que o polinómio $\overline{f}(X) \in \mathbb{F}_p[X]$ obtido reduzindo os coeficientes de f módulo p tem uma raiz $a \in \mathbb{F}_p$ que é uma* raiz simples*, ou seja, com multiplicidade* 1*. Então existe $\alpha \in \mathbb{Z}_p$, com $\alpha \equiv a \pmod{p}$, tal que $f(\alpha) = 0$.*

Demonstração. Como a é uma raiz simples de $\overline{f}$, podemos escrever

$$\overline{f}(X) = (X - a)g(X)$$

para algum polinómio g; a condição de a ser uma raiz simples garante que os polinómios $X - a$ e g são coprimos em $\mathbb{F}_p[X]$! Logo, pela versão 1 do Lema de Hensel, podemos escrever

$$f(X) = f_1(X)f_2(X)$$

onde f_1 é um polinómio de grau 1 que se reduz a $X - a$ módulo p. A raiz α de f_1 é a raiz que procuramos! □

Chegando a este ponto impõe-se relembrar o seguinte: existe uma maneira prática de verificar que uma raiz de um polinómio com coeficientes num corpo é uma raiz simples. De facto, se $f \in K[X]$ é um polinómio e $a \in K$ é tal que $f(a) = 0$, então a é uma raiz simples de f se e só se $f'(a) \neq 0$, onde f' é a *derivada formal* de f: se $f(X) = a_nX^n + \cdots + a_1X + a_0$, então

$$f'(X) = na_nX^{n-1} + \cdots + a_1.$$

Assim a condição do Lema 2.2.4 pode reescrever-se na forma: existe $a \in \mathbb{Z}_p$ tal que $f(a) \equiv 0 \pmod{p}$ e $f'(a) \not\equiv 0 \pmod{p}$.

Exemplo 2.2.5. Vamos ver alguns exemplos de aplicação desta forma do Lema de Hensel.

(i) Seja $p > 2$ um primo, e suponha-se que $u \in \mathbb{Z}_p^\times$ é um quadrado módulo p, ou seja, que a congruência $x^2 \equiv u \pmod{p}$ tem solução. Então u é de facto um quadrado em $\mathbb{Z}_p$! De facto, sendo $f(X) = X^2 - u$, sabemos que a congruência $f(x) \equiv 0 \pmod{p}$ tem uma solução a, e além disso

$$f'(a) = 2a \not\equiv 0 \pmod{p}$$

uma vez que $p \neq 2$ e a não é divisível por p (pois $a^2 \equiv u \pmod{p}$ e u não é divisível por p). Isto justifica a nossa afirmação na introdução de que $\sqrt{6}$ existe em $\mathbb{Q}_5$; temos $6 \equiv 1 \pmod{5}$, e 1 é um quadrado!

(ii) Se $p = 2$, o argumento anterior falha. Vamos tentar determinar os quadrados em $\mathbb{Q}_2$. Qualquer $x \in \mathbb{Q}_2$ pode escrever-se na forma $2^n y$ onde $y \in \mathbb{Z}_2^\times$ (com $n = v_2(x)$) e portanto $x^2 = 4^n y^2$; basta portanto determinar os quadrados em $\mathbb{Z}_2^\times$.

Uma verificação direta mostra que todos os quadrados em $(\mathbb{Z}/8\mathbb{Z})^\times$ são iguais a 1 (temos $1^2, 3^3, 5^2, 7^2 \equiv 1 \pmod{8}$). Portanto, se $u \in \mathbb{Z}_2^\times$ é um quadrado, então $u \equiv 1 \pmod{8}$. Vamos mostrar que o recíproco também se verifica, ou seja, que se $u \equiv 1 \pmod{8}$ então u é um quadrado em $\mathbb{Z}_2$.

Não podemos usar diretamente o Lema de Hensel com o polinómio $X^2 - u$, pois a sua derivada $2X$ anula-se em $\mathbb{F}_2$. Utilizamos então um truque; como qualquer raiz de $X^2 - u$ está em $\mathbb{Z}_2^\times$, qualquer tal raiz é $1 \pmod{2}$, e portanto podemos escrevê-la na forma $2a + 1$, com $a \in \mathbb{Z}_2$. Ou seja, queremos na verdade provar que o polinómio $(2X + 1)^2 - u$ tem uma raiz em $\mathbb{Z}_2$. Mas

$$(2X + 1)^2 - u = 4X^2 + 4X + 1 - u = 4\left(X^2 + X + \frac{1 - u}{4}\right).$$

Aqui $\frac{1-u}{4}$ é inteiro 2-ádico pois por hipótese $u \equiv 1 \pmod{8}$. Sendo $u = 8v + 1$, queremos portanto provar que o polinómio $f(X) = X^2 + X - 2v$ tem uma raiz em $\mathbb{Z}_2$. Mas agora

$$f'(X) = 2X + 1$$

nunca se anula em $\mathbb{F}_2$! E 0 é uma raiz de f módulo 2, portanto pelo Lema de Hensel f tem uma raiz em $\mathbb{Z}_2$, logo u é um quadrado.

Provámos assim que os quadrados em $\mathbb{Q}_2$ são os números da forma

$$4^n(8v + 1), \text{ com } v \in \mathbb{Z}_2.$$

Talvez o leitor já tenha visto números de uma forma parecida com a anterior antes. De facto, os inteiros positivos da forma

$$4^n(8k + 7)$$

são precisamente os inteiros positivos que *não* se podem escrever como soma de três quadrados! Isso não é coincidência. Usando ferramentas mais sofisticadas (nomeadamente o *Teorema de*

Hasse-Minkowski e alguns resultados sobre formas quadráticas em $\mathbb{Q}_p$), prova-se que um inteiro positivo n *não* é uma soma de três quadrados se e só se $-n$ é um quadrado em $\mathbb{Q}_2$! Esta é talvez a maneira mais conceptual de provar o teorema que classifica os inteiros que são soma de três quadrados perfeitos.

§2.3. O Método de Newton

O objetivo desta secção é mostrar uma generalização da segunda versão do Lema de Hensel. O interesse desta generalização está em grande parte no método que é utilizado para a provar. Na introdução mencionámos que parte do potencial dos números p-ádicos está na possibilidade de usar ideias de Análise para tratar questões de Teoria dos Números. Vamos agora mostrar uma dessas ideias em ação, desta vez vinda da Análise Numérica: o Método de Newton.

O Método de Newton é utilizado para resolver numericamente equações, isto é, para, dada uma equação, encontrar uma solução aproximada com um número razoavelmente grande de casas decimais corretas. A ideia é a seguinte: suponhamos que temos uma função f (com boas propriedades analíticas; de classe C^2, digamos), e queremos aproximar uma solução de $f(x) = 0$. Começamos com uma aproximação a olho, um valor inicial x_0 que pareça estar razoavelmente próximo de uma solução. Então consideramos a reta tangente ao gráfico de f no ponto $(x_0, f(x_0))$. Esta reta interseta o eixo das abcissas num ponto, digamos de abcissa x_1. Repetimos o processo com x_1; intersetamos a reta tangente ao gráfico de f no ponto de abcissa x_1 com o eixo das abcissas, num ponto de abcissa x_2. E assim sucessivamente. Obtemos uma sucessão $x_0, x_1, x_2, x_3, \ldots$ que, em condições apropriadas, converge para uma solução da equação $f(x) = 0$. Existem outros métodos numéricos deste tipo para aproximar soluções de equações, mas o Método de Newton é conhecido por ser particularmente rápido; a sucessão $x_0, x_1, x_2, x_3 \ldots$ converge particularmente depressa para uma solução da equação.

Observemos que a reta tangente ao gráfico de f no ponto de abcissa x_i tem equação

$$y = (x - x_i)f'(x_i) + f(x_i)$$

que interseta o eixo das abcissas no ponto

$$\left(x_i - \frac{f(x_i)}{f'(x_i)}, 0\right).$$

Portanto a sucessão mencionada atrás é definida por

$$x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}.$$

Sendo $\mathbb{Q}_p$ um "universo paralelo" a $\mathbb{R}$, é natural perguntarmo-nos se o Método de Newton pode ser adaptado para produzir soluções de equações polinomiais nos p-ádicos. De facto pode, e é assim que vamos obter a seguinte generalização do Lema 2.2.4.

Lema 2.3.1 (Lema de Hensel, versão 3)**.** *Seja $f \in \mathbb{Z}_p[X]$ um polinómio. Suponha-se que existe $a \in \mathbb{Z}_p$ tal que*

$$v_p(f(a)) > 2v_p(f'(a)).$$

Então existe $b \in \mathbb{Z}_p$ tal que $f(b) = 0$, e além disso $v_p(b - a) \geq v_p(f(a)) - v_p(f'(a))$.

Isto generaliza o Lema 2.2.4 porque, como vimos atrás, a hipótese deste último pode escrever-se na forma: existe $a \in \mathbb{Z}_p$ tal que $f(a) \equiv 0 \pmod{p}$ e $f'(a) \not\equiv 0 \pmod{p}$. Isto é o mesmo que ter-se $v_p(f(a)) \geq 1$ e $v_p(f'(a)) = 0$. O que esta nova versão do Lema de Hensel nos diz é que podemos relaxar a condição de $f'(a)$ não ser divisível por p, *desde que $f(a)$ seja divisível por uma potência particularmente grande de p*: se $M > 2N$ e tivermos $f(a) \equiv 0 \pmod{p^M}$ e $v_p(f'(a)) = N$, obtemos um b tal que $f(b) = 0$. Mas note-se que o preço a pagar por permitir divisibilidade por p em $f'(a)$ é que a solução b obtida não é necessariamente congruente com a módulo p^M; parte desse expoente M é "desperdiçado", e a condição final do Lema só nos garante que temos $b \equiv a \pmod{p^{M-N}}$.

Demonstração. Observe-se que a condição sobre a do Lema se pode reescrever na forma

$$|f(a)|_p < |f'(a)|_p^2.$$

Definimos a sucessão $(a_n)_{n\geq 1}$ por

$$a_1 = a \text{ e } a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)} \text{ para todo o inteiro positivo } n.$$

Vamos provar, por indução em n, que se verificam as seguintes condições:

(i) $a_n \in \mathbb{Z}_p$;

(ii) $|f'(a_n)|_p = |f'(a)|_p$;

(iii) $|f(a_n)|_p \leq |f(a)|_p r^{2^{n-1}-1}$, onde $r = \frac{|f(a)|_p}{|f'(a)|_p^2} < 1$.

Em particular, daqui seguirá que $f'(a_n) \neq 0$ para todo o n (pois $|f'(a_n)|_p^2 = |f'(a)|_p^2 > |f(a)|_p \geq 0$), e portanto a_{n+1} está bem definido.

Para $n = 1$ todas as condições se verificam trivialmente. Suponha-se agora que todas as condições se verificam para n. Pela hipótese de indução, temos

$$|f(a_n)|_p \leq |f(a)|_p < |f'(a)|_p^2 = |f'(a_n)|_p^2.$$

Como $f'(a_n) \in \mathbb{Z}_p$, temos $|f'(a_n)|_p \leq 1$ e portanto daqui resulta que $|f(a_n)|_p < |f'(a_n)|_p$, ou seja, $\left|\frac{f(a_n)}{f'(a_n)}\right|_p < 1$. Assim $\frac{f(a_n)}{f'(a_n)} \in \mathbb{Z}_p$. Logo,

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)} \in \mathbb{Z}_p.$$

Está assim mostrado (i) para $n+1$. Passemos a (ii). Podemos escrever

$$f(x) = f(a_n) + f'(a_n)(x - a_n) + g(x)(x - a_n)^2 \tag{2.4}$$

onde g é um polinómio com coeficientes em $\mathbb{Z}_p$ (estamos a separar os dois primeiros termos da expansão em série de Taylor de f com centro em a_n, e os termos que sobram são divisíveis por $(x - a_n)^2$; isto é válido em qualquer anel). Derivando, vem

$$f'(x) = f'(a_n) + 2g(x)(x - a_n) + g'(x)(x - a_n)^2.$$

Substituindo $x = a_{n+1}$ nesta identidade, obtemos

$$f'(a_{n+1}) = f'(a_n) - 2\frac{f(a_n)}{f'(a_n)}g(a_{n+1}) + \frac{f(a_n)^2}{f'(a_n)^2}g'(a_{n+1}).$$

Da desigualdade triangular ultramétrica resulta que

$$|f'(a_{n+1})|_p \leq \max\left\{|f'(a_n)|_p, \left|2\frac{f(a_n)}{f'(a_n)}g(a_{n+1}) - \frac{f(a_n)^2}{f'(a_n)^2}g'(a_{n+1})\right|_p\right\} \tag{2.5}$$

e além disso tem-se igualdade se os dois valores absolutos forem distintos. Vamos estimar o segundo termo: temos

$$\begin{aligned}\left|2\frac{f(a_n)}{f'(a_n)}g(a_{n+1}) - \frac{f(a_n)^2}{f'(a_n)^2}g'(a_{n+1})\right|_p &= \frac{|f(a_n)|_p}{|f'(a_n)|_p} \cdot \left|2g(a_{n+1}) - \frac{f(a_n)}{f'(a_n)}g'(a_{n+1})\right|_p \\ &\leq \frac{|f(a_n)|_p}{|f'(a_n)|_p} = \frac{|f(a_n)|_p}{|f'(a)|_p} \\ &\leq \frac{|f(a)|_p}{|f'(a)|_p} < |f'(a)|_p = |f'(a_n)|_p.\end{aligned}$$

(A primeira desigualdade decorre de que $2g(a_{n+1}) - \frac{f(a_n)}{f'(a_n)}g'(a_{n+1}) \in \mathbb{Z}_p$, e portanto o seu valor absoluto é menor ou igual a 1.) Conclui-se, usando 2.5 e a observação que se lhe segue, que

$$|f'(a_{n+1})|_p = |f'(a_n)|_p = |f'(a)|_p,$$

estando assim provado (ii) para $n+1$. Finalmente, vamos a (iii): substituindo $x = a_{n+1}$ em 2.4, obtemos

$$f(a_{n+1}) = \frac{f(a_n)^2}{f'(a_n)^2}g(a_{n+1}).$$

Assim,

$$\begin{aligned} |f(a_{n+1})|_p &= \frac{|f(a_n)|_p^2}{|f'(a_n)|_p^2} \cdot |g(a_{n+1})|_p \\ &\leq \frac{|f(a_n)|_p^2}{|f'(a_n)|_p^2} \leq \frac{\left(|f(a)|_p r^{2^{n-1}-1}\right)^2}{|f'(a)|_p^2} \\ &= |f(a)|_p \cdot \frac{|f(a)|_p}{|f'(a)|_p^2} r^{2^n-2} = |f(a)|_p r^{2^n-1} \end{aligned}$$

e obtivemos (iii), como pretendido.

Vamos agora provar que $(a_n)_{n\geq 1}$ converge em $\mathbb{Z}_p$; como

$$a_n = a_1 - \frac{f(a_1)}{f'(a_1)} - \cdots - \frac{f(a_{n-1})}{f'(a_{n-1})}$$

a convergência de $(a_n)_n$ é equivalente à convergência da série

$$\sum_{n=1}^{\infty} \frac{f(a_n)}{f'(a_n)}.$$

Pela Proposição 1.4.2, essa série converge se e só se o termo geral tende para 0; ora,

$$\left|\frac{f(a_n)}{f'(a_n)}\right|_p = \frac{|f(a_n)|_p}{|f'(a_n)|_p} \leq \frac{|f(a)|_p}{|f'(a)|_p} r^{2^{n-1}-1}$$

e isto tende para 0 uma vez que $r < 1$. Seja $b = \lim_{n\to\infty} a_n$. Então temos

$$b = \lim_{n\to\infty} a_{n+1} = \lim_{n\to\infty} \left(a_n - \frac{f(a_n)}{f'(a_n)}\right) = b - \frac{f(b)}{f'(b)},$$

de onde resulta que $f(b) = 0$. Falta provar a conclusão final do Lema, que se pode reescrever na forma

$$|b - a|_p \leq \frac{|f(a)|_p}{|f'(a)|_p}. \tag{2.6}$$

Para cada n, temos

$$|a_n - a|_p = |a_n - a_1|_p = |(a_n - a_{n-1}) + \cdots + (a_2 - a_1)|_p \leq \max\{|a_n - a_{n-1}|_p, \ldots, |a_2 - a_1|_p\}.$$

Para cada k, temos $a_{k+1} - a_k = -\frac{f(a_k)}{f'(a_k)}$, e portanto

$$|a_{k+1} - a_k|_p = \frac{|f(a_k)|_p}{|f'(a_k)|_p} \leq \frac{|f(a)|_p}{|f'(a)|_p},$$

usando (ii) e (iii), de onde decorre que $|a_n - a|_p \leq \frac{|f(a)|_p}{|f'(a)|_p}$. Tomando o limite quando n tende para ∞ obtemos 2.6, como pretendido. □

Exemplo 2.3.2. Vamos utilizar o Lema 2.3.1 para dar uma prova alternativa de que, se $u \equiv 1 \pmod 8$, então u é um quadrado em $\mathbb{Q}_2$. Seja $f(x) = x^2 - u$. Vamos usar o Lema 2.3.1 com $a = 1$: temos

$$v_2(f(1)) = v_2(1 - u) \geq 3$$

e

$$v_2(f'(1)) = v_2(2) = 1.$$

Como $3 > 2 \cdot 1$, pelo Lema 2.3.1 existe $b \in \mathbb{Q}_2$ tal que $f(b) = 0$.

§2.4. Séries de Potências

Vamos agora mergulhar mais profundamente na Análise p-ádica. Naturalmente, começamos por transportar a definição de derivada para o contexto p-ádico.

Definição 2.4.1. Seja $U \subseteq \mathbb{Q}_p$ um aberto e seja $f : U \to \mathbb{Q}_p$ uma função. A *derivada de f em $a \in U$* é (caso exista) o limite

$$f'(a) = \lim_{x \to a} \frac{f(x) - f(a)}{x - a}.$$

A função f diz-se *diferenciável em a* se o limite anterior existir, e diz-se *diferenciável* se for diferenciável em a para todo o $a \in U$.

Não deverá ser surpreendente que a derivada p-ádica tem as mesmas propriedades básicas que a derivada em $\mathbb{R}$ ou $\mathbb{C}$; de facto, todas essas propriedades são provadas exatamente da mesma maneira que as propriedades análogas em $\mathbb{R}$.

Proposição 2.4.2 (Propriedades da derivada)**.** *Tem-se o seguinte:*

(i) Se f e g são diferenciáveis em a, então $f + g$ é diferenciável em a e $(f + g)'(a) = f'(a) + g'(a)$;

(ii) Se f e g são diferenciáveis em a, então fg é diferenciável em a e $(fg)' = f'(a)g(a) + f(a)g'(a)$;

(iii) Se f é diferenciável em $g(a)$ e g é diferenciável em a, então $f \circ g$ é diferenciável em a e $(f \circ g)'(a) = f'(g(a))g'(a)$.

Demonstração. Análoga à do caso real. □

Acontece que, tendo em conta todo o respeito que a derivada recebe em $\mathbb{R}$, em $\mathbb{Q}_p$ esta acaba por se revelar um pouco dececionante. Isto é essencialmente culpa da topologia dos p-ádicos: $\mathbb{Q}_p$ é *totalmente desconexo*, ou seja, não contém nenhum subespaço conexo com mais do que um ponto. Ora, as propriedades mais úteis da derivada em $\mathbb{R}$ (o Teorema de Lagrange, por exemplo) aplicam-se precisamente a funções definidas em *abertos conexos*.

Por esta razão, trabalhar com funções diferenciáveis genéricas em $\mathbb{Q}_p$ é um pouco delicado, e portanto vamos restringir a nossa atenção a funções mais "bem comportadas": funções definidas por séries de potências. Para tal, vamos precisar de alguns resultados preliminares sobre séries numéricas em $\mathbb{Q}_p$. Um deles é, como seria de esperar, a Proposição 1.4.2, e vamos juntar-lhe mais dois resultados úteis, que provaremos abaixo. O primeiro é sobre séries duplas; dá-nos um critério para podermos "trocar os sinais de somatório" em séries desse tipo.

Proposição 2.4.3. *Sejam $a_{ij} \in \mathbb{Q}_p$, onde i e j percorrem os inteiros não negativos. Suponha-se que, para todo o $\varepsilon > 0$, existe N tal que*

$$|a_{ij}|_p < \varepsilon \text{ sempre que } \max\{i, j\} \geq N.$$

Então as séries

$$\sum_{i=0}^{\infty} \left(\sum_{j=0}^{\infty} a_{ij} \right) \quad e \quad \sum_{j=0}^{\infty} \left(\sum_{i=0}^{\infty} a_{ij} \right)$$

convergem para o mesmo valor.

Demonstração. Começamos por provar que ambas as séries convergem. As séries "interiores" convergem pela Proposição 1.4.2. Fixemos $\varepsilon > 0$, e considere-se um N como na hipótese da proposição. Então, para $i \geq N$, temos $|a_{ij}|_p < \varepsilon$ para todo o j, e portanto, pela desigualdade ultramétrica,

$$\left| \sum_{j=0}^{\infty} a_{ij} \right|_p < \varepsilon.$$

Daqui decorre que

$$\lim_{i \to \infty} \sum_{j=0}^{\infty} a_{ij} = 0$$

e portanto, pela Proposição 1.4.2, a primeira série converge. A convergência da segunda série é análoga.

Resta provar que ambas as séries convergem para o mesmo valor. Para isso basta provar que, para todo o $\varepsilon > 0$, existe N tal que a diferença entre as somas parciais de ordem n é menor que ε para todo o $n \geq N$. Escolhemos novamente N como dado pela hipótese da proposição, e definimos

$$s_n = \sum_{i=0}^{n} \left(\sum_{j=0}^{\infty} a_{ij} \right) \text{ e } s'_n = \sum_{j=0}^{n} \left(\sum_{i=0}^{\infty} a_{ij} \right).$$

Temos então, para $n \geq N$

$$\left| s_n - s'_n \right|_p = \left| \sum_{i=n+1}^{\infty} \left(\sum_{j=0}^{\infty} a_{ij} \right) - \sum_{j=n+1}^{\infty} \left(\sum_{i=0}^{\infty} a_{ij} \right) \right|_p$$

e como todos os a_{ij} que aparecem acima são, em valor absoluto, menores que ε (temos sempre $i > N$ ou $j > N$, portanto $\max\{i, j\} > N$), decorre da desigualdade ultramétrica que o valor absoluto anterior também o é. Ou seja, provámos que $|s_n - s'_n|_p < \varepsilon$ para todo o $n \geq N$, e isto mostra que s_n e s'_n convergem para o mesmo valor. □

A próxima proposição afirma que podemos multiplicar séries numéricas da maneira esperada.

Proposição 2.4.4. *Sejam $(a_n)_n$ e $(b_n)_n$ duas sucessões de números p-ádicos, tais que as séries*

$$\sum_{n=0}^{\infty} a_n \text{ e } \sum_{n=0}^{\infty} b_n$$

convergem para a e b, respetivamente. Então a série

$$\sum_{n=0}^{\infty} c_n$$

converge para ab, onde

$$c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

Demonstração. Sejam $A_n = \sum_{j=0}^{n} a_j$ e $B_n = \sum_{j=0}^{n} b_j$. Como as sucessões $(a_n)_n$ e $(b_n)_n$ convergem (para 0), em particular são limitadas, e existe $M > 0$ tal que $|a_n|_p \leq M$ e $|b_n|_p \leq M$ para todo o n. Fixemos $\varepsilon > 0$, e fixemos $N > 0$ tal que, para $n \geq N$, ambas as seguintes condições se verificam:

- $|ab - A_nB_n|_p < \varepsilon$;
- $|a_n|_p < \frac{\varepsilon}{M}$;
- $|b_n|_p < \frac{\varepsilon}{M}$.

Então, para $n \geq 2N$,

$$\left|ab - \sum_{k=0}^{n} c_k\right|_p = \left|ab - \sum_{k=0}^{N} a_k \sum_{k=0}^{N} b_k - \sum_{\substack{i+j\leq 2n \\ i>N \text{ ou } j>N}} a_i b_j\right|_p$$
$$\leq \max\left\{|ab - A_NB_N|_p, \left|\sum_{\substack{i+j\leq 2n \\ i>N \text{ ou } j>N}} a_i b_j\right|_p\right\}.$$

Mas temos $|ab - A_NB_N|_p < \varepsilon$ por hipótese, e além disso qualquer $|a_ib_j|_p$ na soma acima é menor do que ε; de facto, supondo sem perda de generalidade que $i > N$, temos

$$|a_ib_j|_p = |a_i|_p|b_j|_p < \frac{\varepsilon}{M} \cdot M = \varepsilon.$$

Assim o máximo anterior é menor do que ε, e isto prova que a série $\sum c_k$ converge para ab. □

Estamos prontos para passar às séries de potências. Estas permitem-nos definir funções da forma

$$f(x) = \sum_{n=0}^{\infty} a_n(x-a)^n$$

em pontos x onde a série anterior converge. Mas as séries de potências podem ser tratadas de um modo puramente formal, e é isso que faremos brevemente primeiro. Vamos então fazer uma convenção útil: utilizaremos a letra maiúscula X quando estivermos a trabalhar com uma série de potências formal, e a letra minúscula x quando estivermos a trabalhar com uma série de potências como uma função.

Uma *série de potências* (centrada em 0) com coeficientes num anel comutativo R é uma expressão da forma

$$f(X) = \sum_{n\geq 0} a_n X^n$$

onde $a_n \in R$. As seguintes operações com séries de potências fazem sentido em qualquer anel R, e as primeiras duas fazem do conjunto das séries de potências com coeficientes em R um anel comutativo, que denotamos por $R[[X]]$:

- Soma: Dadas séries de potências $f(X) = \sum_{n\geq 0} a_nX^n$ e $g(X) = \sum_{n\geq 0} b_nX^n$, definimos

$$(f+g)(X) = \sum_{n\geq 0}(a_n + b_n)X^n.$$

- Produto: Definimos

$$(fg)(X) = \sum_{n\geq 0} c_nX^n,$$

onde

$$c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

- Derivação: Definimos a *derivada* de $f(X)$ como sendo

$$f'(X) = \sum_{n\geq 0}(n+1)a_{n+1}X^n.$$

- Composição: Não vamos dar aqui uma fórmula explícita, mas quando $b_0 = 0$ podemos definir a *série composta* $f(g(X))$: a ideia é que a série $g(X)^n$ só tem coeficientes não nulos de ordem $\geq n$, portanto a soma

$$\sum_{n\geq 0} a_n g(X)^n$$

está bem definida; para cada $m \geq 0$ a soma correspondente ao coeficiente de X^m é uma soma finita.

Obviamente, a nós interessa-nos particularmente o caso $R = \mathbb{Q}_p$. Mas quando passamos a trabalhar com séries em $\mathbb{Q}_p[[X]]$ como *funções*, ou seja, quando deixamos de olhar para as séries apenas como expressões formais e consideramos a hipótese de substituir X numa série em $\mathbb{Q}_p[[X]]$ por um elemento de $\mathbb{Q}_p$ e ver o que acontece, algumas questões inconvenientes levantam-se. Por exemplo:

- Será que podemos somar e multiplicar funções definidas por séries de potências da maneira natural? Ou seja, será que a soma das *funções* definidas pelas séries de potências $f(X)$ e $g(X)$ em $\mathbb{Q}_p[X]$ é a função definida pela série de potências $(f+g)(X)$ (e analogamente para o produto)?

- Será que podemos "derivar termo-a-termo" funções definidas por séries de potências? Ou seja, será que a derivada da *função* definida pela série $f(X)$ é a função definida pela série $f'(X)$?

- Será que podemos compor funções definidas por séries de potências da maneira natural? Ou seja, será que a composta das funções definidas pelas séries de potências $f(X)$ e $g(X)$ é definida pela série de potências $f(g(X))$?

Vamos responder a estas questões ao longo das próximas páginas. Começamos pela primeira:

Proposição 2.4.5. *Sejam $f(X)$ e $g(X)$ duas séries de potências em $\mathbb{Q}_p[[X]]$. Se x é um número p-ádico tal que as séries $f(x)$ e $g(x)$ convergem, então a série $(f+g)(x)$ converge para $f(x)+g(x)$ e a série $(fg)(x)$ converge para $f(x)g(x)$.*

Demonstração. A primeira é óbvia; a segunda é uma consequência da Proposição 2.4.4. □

Chegados a este ponto, vamos ver o que podemos dizer, dada uma série de potências $f(X)$, sobre o conjunto dos $x \in \mathbb{Q}_p$ tais que a série $f(x)$ converge. O resultado é igual ao resultado análogo em $\mathbb{R}$ ou $\mathbb{C}$ (mas a prova é mais simples!).

Proposição 2.4.6 (Raio de convergência)**.** *Seja $f(X) = \sum_{n\geq 0} a_n X^n$ uma série de potências em $\mathbb{Q}_p[[X]]$. Então existe $\rho \geq 0$ tal que a série $f(x)$ converge para $|x|_p < \rho$ e diverge para $|x|_p > \rho$. Este ρ designa-se o* raio de convergência *de f, e é dado explicitamente por*

$$\rho = \frac{1}{\limsup_{n\to\infty} \sqrt[n]{|a_n|_p}}.$$

Demonstração. Definimos ρ pela expressão acima, e vamos mostrar que se $|x|_p < \rho$ então $f(x)$ converge e que se $|x|_p > \rho$ então $f(x)$ diverge.

- Se $|x|_p < \rho$, então $\frac{1}{|x|_p} > \limsup_{n\to\infty} \sqrt[n]{|a_n|_p}$, e portanto existe $\varepsilon > 0$ tal que, para n suficientemente grande, se tem

$$\frac{1}{|x|_p} \geq (1+\varepsilon)\sqrt[n]{|a_n|_p}$$

(por definição de lim sup). Para n suficientemente grande tem-se então $|a_n x^n|_p \leq \frac{1}{(1+\varepsilon)^n}$. Isto implica que $a_n x^n$ tende para 0, e portanto a série $f(x)$ converge.

- Se $|x|_p > \rho$, então $\frac{1}{|x|_p} < \limsup_{n\to\infty} \sqrt[n]{|a_n|_p}$, logo existem infinitos inteiros não negativos n para os quais $\frac{1}{|x|_p} \leq \sqrt[n]{|a_n|_p}$. Para esses inteiros n tem-se $|a_n x^n|_p \geq 1$, e portanto $a_n x^n$ não tende para 0 e a série $f(x)$ não converge.

□

Até aqui nada de novo em relação ao caso real; a grande diferença está no que acontece no caso $|x| = \rho$, que é deixado em aberto pela proposição anterior. De facto, no caso real/complexo, podemos ter todo o tipo de comportamentos quando $|x| = \rho$: a série $f(x)$ pode convergir para alguns desses valores e não convergir para outros de maneira bastante errática. No caso p-ádico, não: a série $f(x)$ converge para *todos* os x com $|x|_p = \rho$ ou para *nenhum* tal x, conforme $|a_n|_p \rho^n$ tende para 0 ou não (porquê?).

Sendo ρ o raio de convergência de uma série de potências $f(X) = \sum_{n\geq 0} a_n X^n$, esta série define uma função f na bola aberta definida por $|x|_p < \rho$. O que acontece se fizermos uma mudança de variável substituindo x por $x - \alpha$, para algum α dentro dessa mesma bola? Obtemos uma função definida pela série de potências centrada em α

$$\sum_{n\geq 0} a_n (X-\alpha)^n. \tag{2.7}$$

Esta série converge na bola aberta de centro α e raio ρ. Claro que podemos expandir os termos $(X-\alpha)^n$ e reagrupar novamente os termos obtidos em potências de X, obtendo assim uma série de potências centrada em 0. Formalmente, tudo isto é "legal". Mas à primeira vista parece que há problemas de convergência com esta reorganização dos termos; afinal, a nova série de potências converge numa bola aberta centrada em 0, portanto não pode convergir no mesmo conjunto que (2.7), pois não?

De facto, no caso real/complexo não pode; uma bola centrada em 0 e uma bola centrada em $\alpha \neq 0$ são necessariamente diferentes. Mas em $\mathbb{Q}_p$ isso não acontece; recordemos que pela Proposição 1.4.1 a bola aberta de centro α e raio ρ coincide com a bola aberta de centro 0 e raio ρ! E portanto é concebível que a função definida por (2.7) *coincida* com a função definida pela série que obtemos agrupando os termos de (2.7) em potências de x! É esse o conteúdo da próxima proposição.

Proposição 2.4.7. *Seja $f(X) = \sum_{n\geq 0} a_n X^n$ uma série de potências com raio de convergência $\rho > 0$. Seja $\alpha \in \mathbb{Q}_p$ tal que $|\alpha|_p < \rho$, e defina-se, para cada inteiro não negativo k,*

$$b_k = \sum_{n\geq k} (-1)^{n-k} \binom{n}{k} \alpha^{n-k} a_n.$$

Então a função $x \mapsto f(x-\alpha)$, definida na bola aberta de centro 0 e raio ρ, é dada nessa bola pela série de potências

$$g(X) = \sum_{k\geq 0} b_k X^k.$$

Demonstração. Temos, para x na bola aberta de centro 0 e raio ρ,

$$\begin{aligned} f(x) &= \sum_{n\geq 0} a_n (x-\alpha)^n \\ &= \sum_{n\geq 0} a_n \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} \alpha^{n-k} x^k \\ &= \sum_{n\geq 0}\sum_{k\geq 0} (-1)^{n-k} \binom{n}{k} a_n \alpha^{n-k} x^k, \end{aligned}$$

onde usamos a convenção de que $\binom{n}{k} = 0$ para $k > n$. A proposição fica assim provada se mostrarmos que podemos trocar a ordem das somas acima. Isso é trabalho para a Proposição 2.4.3: definindo

$$x_{n,k} = (-1)^{n-k} \binom{n}{k} a_n \alpha^{n-k} x^k,$$

basta provar que, para todo o $\varepsilon > 0$, existe N tal que $|x_{n,k}|_p < \varepsilon$ sempre que $\max\{n,k\} \geq N$.

Para isso, escolhemos $r > 0$ tal que $r < \rho$ mas $r > |\alpha|_p$ e $r > |x|_p$ (que existe uma vez que por hipótese $|x|_p$ e $|\alpha|_p$ são menores do que $|\rho|$). Então temos $\lim_{n\to\infty} |a_n|_p r^n = 0$, uma vez que a série $f(y)$ converge para $|y|_p = r$. Escolhemos assim N tal que $|a_n|_p r^n < \varepsilon$ para $n > N$. Vamos provar que $|x_{n,k}|_p < \varepsilon$ sempre que $\max\{n,k\} > N$.

De facto, isto é trivial se $k > n$, pois nesse caso $x_{n,k} = 0$. Podemos assim supor $n \geq k$ e portanto $n > N$. Mas então

$$|x_{n,k}|_p = \left|\binom{n}{k}\right|_p \cdot |a_n|_p |\alpha|_p^{n-k} |x|_p^k \leq |a_n|_p r^n < \varepsilon,$$

onde usámos que $|\alpha|_p < r$, $|x|_p < r$ e ainda $\left|\binom{n}{k}\right|_p \leq 1$, sendo que a última desigualdade decorre simplesmente de $\binom{n}{k}$ ser um inteiro. □

Vamos agora provar versões da Proposição 2.4.5 para derivadas e compostas de séries de potências. Começamos com o caso da derivada, que é mais simples.

Proposição 2.4.8. *Seja $f(X) = \sum_{n\geq 0} a_n X^n$ uma série de potências em $\mathbb{Q}_p[[X]]$ com raio de convergência $\rho > 0$. Seja $x \in \mathbb{Q}_p$ um elemento da região de convergência de $f(x)$. Então (sendo $f'(X)$ a derivada formal de $f(X)$) a série $f'(x)$ converge para a derivada em x da função definida por $f(X)$; ou seja,*

$$f'(x) = \lim_{h\to 0} \frac{f(x+h) - f(x)}{h}.$$

Demonstração. Começamos por observar que $f'(x)$ converge. Isto é óbvio se $x = 0$. Caso contrário, temos

$$f'(x) = \sum_{n\geq 0} n a_n x^{n-1} \tag{2.8}$$

e $|n a_n x^{n-1}|_p \leq \frac{1}{|x|_p} |a_n x^n|_p$; como $a_n x^n$ tende para 0, conclui-se que $n a_n x^{n-1}$ também tende para 0, e a série (2.8) converge.

Vejamos agora que

$$\begin{aligned}\frac{f(x+h)-f(x)}{h} &= \frac{1}{h}\left(\sum_{n\geq 0} a_n(x+h)^n - \sum_{n\geq 0} a_n x^n\right)\\ &= \sum_{n\geq 0} a_n \frac{(x+h)^n - x^n}{h}\\ &= \sum_{n\geq 0} a_n \sum_{k=1}^{n} \binom{n}{k} x^{n-k}h^{k-1}\\ &= \sum_{n\geq 0} n a^n x^{n-1} + \sum_{n\geq 0}\sum_{k=2}^{n} a_n \binom{n}{k} x^{n-k}h^{k-1},\end{aligned}$$

onde a última igualdade resulta de isolar a parcela correspondente a $k = 1$ em cada uma das somas interiores. A primeira parcela é precisamente a derivada formal $f'(X)$ avaliada em x, logo resta provar que a segunda parcela tende para 0 quando h tende para 0.

Para isso, fixemos $\varepsilon > 0$, e observemos que, como $a_n x^n$ tende para 0 com x, existe N tal que $|a_n x^n|_p < \varepsilon |x|_p$ para todo o $n > N$. Escrevemos assim

$$\sum_{n\geq 0}\sum_{k=2}^{n} a_n \binom{n}{k} x^{n-k}h^{k-1} = \sum_{n=0}^{N}\sum_{k=2}^{n} a_n \binom{n}{k} x^{n-k}h^{k-1} + \sum_{n>N}\sum_{k=2}^{n} a_n \binom{n}{k} x^{n-k}h^{k-1}.$$

Cada uma das parcelas da primeira soma finita tende para 0 com h, logo a primeira parcela acima tende para 0 quando h tende para 0, e em particular tem valor absoluto menor do que ε se $|h|_p$ for suficientemente pequeno. Pela Desigualdade Ultramétrica, resta apenas provar que existe $\delta > 0$ tal que, se $|h|_p < \delta$, então

$$\left|\sum_{n>N}\sum_{k=2}^{n} a_n \binom{n}{k} x^{n-k}h^{k-1}\right|_p < \varepsilon. \tag{2.9}$$

Para isso, tomamos $\delta = |x|_p$: desta forma, temos

$$\left|a_n \binom{n}{k} x^{n-k}h^{k-1}\right|_p \leq |a_n x^{n-1}|_p < \varepsilon$$

sempre que $|h|_p < \delta$. Pela Desigualdade Ultramétrica, o valor absoluto em (2.9) também é menor do que ε, e isto conclui a prova. □

Vamos agora olhar para o caso da *composta* de duas séries de potências, que é mais delicado. Sejam $f(X) = \sum_{n\geq 0} a_n X^n$ e $g(X) = \sum_{n\geq 0} b_n X^n$ séries de potências formais em $\mathbb{Q}_p[[X]]$, com $b_0 = 0$. Então a série composta $h(X) = f(g(X))$ está bem definida. No entanto, *não* é necessariamente verdade que a *função* definida por h seja a composta das funções definidas por f e g. Por outras palavras, não é necessariamente verdade que se tomarmos um número p-ádico x e o substituirmos em $g(X)$, e substituirmos o resultado por sua vez em $f(X)$, obtemos o mesmo resultado que se substituirmos x diretamente em $h(X)$ (mesmo quando todas as séries numéricas envolvidas convergem!).[1]

No entanto, a seguinte proposição dá-nos uma condição suficiente para não termos problemas de compatibilidade ao compor séries de potências.

[1]Para satisfazer o leitor curioso, um exemplo concreto de um caso onde isto falha é o seguinte: sejam $f(X) = \sum_{n\geq 0} \frac{X^n}{n!}$, $g(X) = -2X + 2X^2$ e $h(X) = f(g(X))$. Então $h(1) \neq f(g(1))$ em $\mathbb{Q}_2$.

Proposição 2.4.9. *Sejam $f(X) = \sum_{n\geq 0} a_n X^n$ e $g(X) = \sum_{n\geq 0} b_n X^n$ séries de potências formais em $\mathbb{Q}_p[[X]]$ com $b_0 = 0$, e seja $h(X) = f(g(X))$ a composta formal. Seja $x \in \mathbb{Q}_p$ tal que:*

- *A série numérica $g(x)$ converge;*
- *Sendo $y = g(x)$, a série numérica $f(y)$ converge;*
- *Para todo o inteiro positivo n, tem-se $|b_n x^n|_p \leq |g(x)|_p$.*

Então $h(x)$ converge, e $h(x) = f(g(x))$.

Demonstração. Seja

$$g(X)^m = \sum_{n\geq 0} d_{m,n} X^n,$$

para cada m, onde obviamente $d_{m,n} = 0$ para $n < m$. A composta formal de $f(X)$ e $g(X)$ é dada por

$$h(X) = a_0 + \sum_{n=1}^{\infty} \left(\sum_{m=1}^{\infty} a_m d_{m,n} \right) X^n$$

e em particular

$$h(x) = a_0 + \sum_{n=1}^{\infty} \left(\sum_{m=1}^{\infty} a_m d_{m,n} x^n \right).$$

Por outro lado, temos

$$\begin{aligned} f(g(x)) &= a_0 + \sum_{m=1}^{\infty} a_m g(x)^m \\ &= a_0 + \sum_{m=1}^{\infty} a_m \sum_{n=1}^{\infty} d_{m,n} x^n \\ &= a_0 + \sum_{m=1}^{\infty} \left(\sum_{n=1}^{\infty} a_m d_{m,n} x^n \right). \end{aligned}$$

Comparando as expressões para $h(x)$ e $f(g(x))$ vemos que a questão da igualdade $h(x) = f(g(x))$ é essencialmente uma questão de trocar a ordem dos somatórios numa série dupla. Isso, claro, é trabalho para a Proposição 2.4.3. Fixemos $\varepsilon > 0$. Basta-nos provar que existe N tal que, se $\max\{m, n\} \geq N$, então

$$|a_m d_{m,n} x^n|_p < \varepsilon. \tag{2.10}$$

Observemos que isto é trivial se $m > n$, pois nesse caso $d_{m,n} = 0$. Podemos assim supor que $m \leq n$, e a condição $\max\{m, n\} \geq N$ fica simplesmente $n \geq N$.

Temos

$$d_{m,n} = \sum_{i_1 + \cdots + i_m = n} b_{i_1} \cdots b_{i_m}$$

e portanto

$$\begin{aligned}|d_{m,n}x^n|_p &\leq \left|\sum_{i_1+\cdots+i_m=n} b_{i_1}\cdots b_{i_m}x^n\right|_p \\ &= \left|\sum_{i_1+\cdots+i_=n} b_{i_1}x^{i_1}\cdots b_{i_m}x^{i_m}\right|_p \\ &\leq \max_{i_1+\cdots+i_m=n} |b_{i_1}x^{i_1}|_p\cdots|b_{i_m}x^{i_m}|_p. \end{aligned} \tag{2.11}$$

Como, por hipótese, a série $\sum_{m\geq 0} a_m g(x)^m$ converge, o termo geral $a_m g(x)^m$ tende para 0, e existe m_0 tal que, se $m > m_0$, então $|a_m g(x)^m|_p < \varepsilon$. Suponha-se que $n \geq m > m_0$. Pela terceira hipótese da proposição, todos os termos $|b_{i_k}x^{i_k}|_p$ em (2.11) são majorados por $|g(x)|_p$, e portanto decorre de (2.11) que

$$|d_{m,n}x^n|_p \leq |g(x)|^m.$$

Conclui-se que

$$|a_m d_{m,n}x^n|_p \leq |a_m g(x)^m|_p < \varepsilon.$$

Portanto (2.10) é *automático* se $m > m_0$. Podemos, assim, supor que $m \in \{1,\ldots,m_0\}$. Sejam

$$M = \max_{m=1,\ldots,m_0} |a_m|_p \quad \text{e} \quad L = \max\{1, \max_{k\geq 1} |b_k x^k|_p\}.$$

Consideramos agora T tal que $|b_k x^k|_p \leq \frac{\varepsilon}{ML^{m_0-1}}$ para $k \geq T$, que existe uma vez que $b_k x^k$ tende para 0 (pois a série $g(x)$ converge). Finalmente, seja $N = m_0 T$; vamos provar que com esta escolha de n se tem (2.10).

Para isso, estimamos $|d_{m,n}x^n|_p$ usando (2.11): se $i_1 + \cdots + i_m = n \geq N \geq mT$ então existe k tal que $i_k \geq T$. Sem perda de generalidade, $k = 1$. Deste modo $|b_{i_1}x^{i_1}|_p < \frac{\varepsilon}{ML^{m_0-1}}$, e temos automaticamente $|b_{i_j}x^{i_j}|_p \leq L$ para $j = 2,\ldots,m$ pela definição de L. Resulta portanto que

$$|d_{m,n}x^n|_p < \frac{\varepsilon}{ML^{m_0-1}}\cdot L^{m-1} \leq \frac{\varepsilon}{ML^{m_0-1}}\cdot L^{m_0-1} = \frac{\varepsilon}{M}.$$

Por fim,

$$|a_m d_{m,n}x^n|_p \leq M|d_{m,n}x^n|_p < M\cdot\frac{\varepsilon}{M} = \varepsilon$$

pela definição de M, acabando a prova. □

Para terminar esta secção, vamos ver que, se restringirmos a nossa atenção a funções p-ádicas *definidas por séries de potências*, então podemos essencialmente reconstituir uma função a partir da sua derivada, a menos de uma constante. Isto não é verdade para funções diferenciáveis genéricas: por exemplo, a função $f : \mathbb{Q}_p \to \mathbb{Q}_p$ definida por

$$f(x) = \begin{cases} 0 & \text{se } x \in \mathbb{Z}_p \\ 1 & \text{caso contrário} \end{cases}$$

é diferenciável em $\mathbb{Q}_p$ e tem derivada nula, mas não é constante! Vamos ver agora que este tipo de patologias não ocorre com funções definidas por séries de potências. Para isso, precisamos de um resultado prévio.

Proposição 2.4.10. *Sejam $f(X)$ e $g(X)$ duas séries de potências em $\mathbb{Q}_p[[X]]$. Suponha-se que $f(X)$ e $g(X)$ definem a mesma função na bola aberta de centro 0 e raio r, para algum $r > 0$. Então $f(X) = g(X)$ (i.e. as duas séries de potências têm os mesmos coeficientes).*

Demonstração. Seja

$$h(X) = f(X) - g(X) = \sum_{n\geq 0} c_n X^n.$$

Então por hipótese $h(X)$ define a função nula na bola aberta de centro 0 e raio r. Suponha-se que nem todos os c_n são iguais a 0 e seja m o menor inteiro tal que $c_m \neq 0$. Então, para todo o x com $|x|_p < r$,

$$0 = h(x) = x^m(c_m + c_{m+1}x + c_{m+2}x^2 + \cdots).$$

Em particular, se $|x|_p < r$ e $x \neq 0$, então

$$c_m + c_{m+1}x + c_{m+2}x^2 + \cdots = 0.$$

Seja $u(x) = c_m + c_{m+1}x + c_{m+2}x^2 + \cdots$. Então u é uma função contínua (vimos na Proposição 2.4.8 que uma função definida por uma série de potências é até *diferenciável*) e, como $u(x) = 0$ para valores de x arbitrariamente próximos de 0, isto implica $u(0) = 0$. Mas isso significa que $c_m = 0$, que contradiz a escolha de m.

Então $c_n = 0$ para todo o n. Isto diz-nos que $h(X)$ é a série nula. Como $h(X) = f(X) - g(X)$, resulta que $f(X) = g(X)$, como pretendido. □

Corolário 2.4.11. *Sejam $f, g : U \to \mathbb{Q}_p$ funções definidas por séries de potências num aberto $U \subseteq \mathbb{Q}_p$ contendo 0. Se $f'(x) = g'(x)$ para todo o $x \in U$, então existe uma constante c tal que $f(x) = g(x) + c$ para todo o $x \in U$.*

Demonstração. Vamos utilizar também as letras f e g para designar as séries de potências

$$f(X) = \sum_{n\geq 0} a_n X^n \quad \text{e} \quad \sum_{n\geq 0} b_n X^n$$

que definem as *funções* f e g. Pela Proposição 2.4.8, temos, para $x \in U$,

$$f'(x) = \sum_{n\geq 1} n a_n x^{n-1} \quad g'(x) = \sum_{n\geq 1} n b_n x^{n-1}.$$

A hipótese de que $f'(x) = g'(x)$ para todo o $x \in U$ implica, pela Proposição 2.4.10, que $na_n = nb_n$ para todo o $n \geq 1$, ou seja, $a_n = b_n$ para todo o $n \geq 1$. Isto implica que as séries $f(X)$ e $g(X)$ diferem por uma constante, completando a prova. □

§2.5. Exponencial e Logaritmo

Nesta secção vamos definir, utilizando séries de potências, duas funções p-ádicas fundamentais que são úteis tanto para o nosso entendimento de $\mathbb{Q}_p$ como para as aplicações da Análise p-ádica que veremos posteriormente. A ideia é "imitar" a construção (uma possível construção) da função exponencial e da função logaritmo em $\mathbb{R}$; potencialmente vamos obter funções p-ádicas com propriedades semelhantes. Começamos pelo logaritmo.

Seja

$$f(X) = X - \frac{X^2}{2} + \frac{X^3}{3} - \cdots = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} X^n.$$

Vamos determinar o raio de convergência de $f(X)$. Pela Proposição 2.4.6, basta-nos calcular

$$\lim_{n\to\infty} \sqrt[n]{|n|_p} = \lim_{n\to\infty} p^{\frac{v_p(n)}{n}}.$$

Como $p^{v_p(n)}$ divide n temos $p^{v_p(n)} \leq n$ e portanto $v_p(n) \leq \frac{\log(n)}{\log(p)}$. Portanto

$$\frac{v_p(n)}{n} \leq \frac{\log(n)}{n\log(p)}$$

e o lado direito tende para 0 quando n tende para infinito. Como $\frac{v_p(n)}{n} \geq 0$ para todo o n conclui-se que o limite quando n tende para infinito de $\frac{v_p(n)}{n}$ é igual a 0. Resulta que

$$\lim_{n\to\infty} \sqrt[n]{|n|_p} = 1$$

e portanto o raio de convergência de $f(X)$ é igual a 1.

Assim temos duas possibilidades: ou $f(x)$ converge precisamente quando x pertence à bola *aberta* de centro 0 e raio 1, ou quando x pertence à bola *fechada* de centro 0 e raio 1. Mas $f(x)$ não converge quando $|x|_p = 1$; de facto, não temos

$$\lim_{n\to\infty} \frac{(-1)^{n+1}}{n} = 0$$

em $\mathbb{Q}_p$ (porquê?). Conclui-se que $f(x)$ converge precisamente para $|x|_p < 1$, ou seja, para $x \in p\mathbb{Z}_p$. Deste modo, a seguinte definição faz sentido.

Definição 2.5.1. Definimos o *logaritmo p-ádico* $\log_p : 1 + p\mathbb{Z}_p \to \mathbb{Q}_p$ por

$$\log_p(x) = f(x-1) \quad \text{para } x \in 1 + p\mathbb{Z}_p.$$

Podemos determinar facilmente a derivada do logaritmo p-ádico. De facto, a derivada formal de $f(X)$ é

$$f'(X) = 1 - X + X^2 - X^3 + \cdots$$

e portanto, pela Proposição 2.4.8

$$f'(x) = \sum_{n=0}^{\infty} (-x)^n = \frac{1}{1+x}$$

para $x \in p\mathbb{Z}_p$. Obtemos o seguinte:

Proposição 2.5.2 (Derivada do logaritmo)**.** *Para $x \in p\mathbb{Z}_p$ tem-se $\log_p'(x) = \frac{1}{x}$.*

Nada muito diferente, até agora, do logaritmo real!

As semelhanças não ficam por aqui. Vamos agora provar uma propriedade que é essencial para uma função, seja em que contexto for, que queira ser digna do nome de logaritmo.

Proposição 2.5.3. *Para quaisquer $a, b \in 1 + p\mathbb{Z}_p$ tem-se*

$$\log_p(ab) = \log_p(a) + \log_p(b).$$

Demonstração. Escrevemos $a = 1 + x$ e $b = 1 + y$ com $x, y \in p\mathbb{Z}_p$. Então $ab = 1 + (x + y + xy)$, e a propriedade a provar fica

$$f(x + y + xy) = f(x) + f(y). \tag{2.12}$$

Para provar isto, fixamos $y \in p\mathbb{Z}_p$, e definimos a função $g : p\mathbb{Z}_p \to \mathbb{Q}_p$ por

$$g(x) = f(x + y + xy) = f((1 + y)x + y) \text{ para todo o } x \in p\mathbb{Z}_p.$$

Vamos calcular a derivada de g. Usando a regra da cadeia, temos

$$g'(x) = (1 + y)f'(x + y + xy) = (1 + y) \cdot \frac{1}{1 + x + y + xy} = (1 + y) \cdot \frac{1}{(1 + x)(1 + y)} = \frac{1}{1 + x}.$$

Então $g'(x) = f'(x)$ para todo o $x \in p\mathbb{Z}_p$. Mas pela Proposição 2.4.7 a função $x \mapsto f((1+y)x+y)$ é dada em $p\mathbb{Z}_p$ por uma série de potências centrada em 0, tal como f! Então pelo Corolário 2.4.11 resulta que existe uma constante c tal que

$$g(x) = f(x) + c$$

para todo o $x \in p\mathbb{Z}_p$. Tomando $x = 0$ obtemos que

$$c = g(0) = f(y)$$

e portanto

$$g(x) = f(x) + f(y)$$

para todo o $x \in p\mathbb{Z}_p$, que equivale precisamente a (2.12), como pretendido. □

Vamos ver uma consequência curiosa. Suponha-se agora que $p = 2$. Então $-1 \in 1 + p\mathbb{Z}_p$, e portanto $\log_2(-1)$ está bem definido. Além disso, temos

$$2\log_2(-1) = \log_2((-1)^2) = \log_2(1) = 0.$$

Portanto $\log_2(-1) = 0$. Mas, usando diretamente a definição de $\log_2$ em termos de f, isso diz-nos que

$$\sum_{n=1}^{\infty} \frac{2^n}{n} = 0 \text{ em } \mathbb{Q}_2!$$

O que é que isto significa? Significa que, sendo

$$x_n = \frac{2^1}{1} + \frac{2^2}{2} + \cdots + \frac{2^n}{n},$$

o valor absoluto p-ádico $|x_n|_2$ tende para 0, ou, por outras palavras, $v_2(x_n)$ tende para infinito. Mas isso não é nada trivial a partir da definição de x_n! Nem sequer é óbvio, por exemplo, que conseguimos encontrar n tal que o numerador de x_n é divisível por 2^{1000}. Vejamos o comportamento de $v_2(x_n)$ na seguinte tabela:

n	x_n	$v_2(x_n)$
1	2	1
2	4	2
3	$\frac{20}{3}$	2
4	$\frac{32}{3}$	5
5	$\frac{256}{15}$	8
6	$\frac{416}{15}$	5
7	$\frac{4832}{105}$	5
8	$\frac{8192}{105}$	13
9	$\frac{42496}{315}$	9
10	$\frac{74752}{315}$	10

É caso para celebrar: é a nossa primeira aplicação de métodos p-ádicos a um resultado elementar!

Para terminar a nossa discussão sobre o logaritmo p-ádico, vamos provar um resultado sobre o contradomínio do mesmo.

Proposição 2.5.4. *Para todo o $a \in 1 + p\mathbb{Z}_p$ tem-se $\log_p(a) \in p\mathbb{Z}_p$, e portanto $\log_p$ pode ser vista como uma função $1 + p\mathbb{Z}_p \to p\mathbb{Z}_p$.*

Demonstração. Seja $a = 1 + x$. Para a primeira parte, basta provar que para todo o inteiro positivo n se tem $\frac{x^n}{n} \in p\mathbb{Z}_p$. Isto equivale a ter-se

$$v_p\left(\frac{x^n}{n}\right) > 0, \text{ ou seja, } nv_p(x) > v_p(n).$$

Isto, por sua vez, é equivalente a $p^{v_p(n)} < p^{nv_p(x)}$; como $p^{v_p(n)}$ divide n tem-se $p^{v_p(n)} \leq n$. Como $a \in 1 + p\mathbb{Z}_p$ tem-se $v_p(x) \geq 1$, e portanto

$$p^{v_p(n)} \leq n < p^n \leq p^{nv_p(x)}$$

como pretendido. □

Passemos à função exponencial. Para a definir, utilizamos a série de potências

$$\exp_p(X) = 1 + X + \frac{X^2}{2} + \frac{X^3}{6} + \cdots = \sum_{n=0}^{\infty} \frac{X^n}{n!}.$$

Denotamos também a função que esta série de potências define (numa bola apropriada de centro em 0) por $\exp_p$. Ao contrário do que acontece em $\mathbb{R}$, a série que define a exponencial p-ádica não tem raio de convergência infinito. Em vez disso, temos o seguinte:

Proposição 2.5.5. *A série $\exp_p(x)$ converge se e só se $|x|_p < p^{\frac{-1}{p-1}}$.*

Demonstração. Começamos por notar que, para qualquer inteiro positivo n,

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \tag{2.13}$$

e em particular

$$v_p(n!) < \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \cdots = \frac{n}{p-1}.$$

Suponha-se que $|x|_p < p^{\frac{-1}{p-1}}$. Então

$$\left|\frac{x^n}{n!}\right|_p = \frac{|x|_p^n}{p^{-v_p(n!)}} < \frac{|x|_p^n}{p^{-\frac{n}{p-1}}} = \left(|x|_p p^{\frac{1}{p-1}}\right)^n$$

e isto tende para 0 quando n tende para infinito, logo $\frac{x^n}{n!}$ tende para 0 em $\mathbb{Q}_p$ e a série $\exp_p(x)$ converge pela Proposição 1.4.2.

Suponha-se agora que $|x|_p \geq p^{\frac{-1}{p-1}}$. Se $n = p^m$ é uma potência de p, então por (2.13) temos

$$v_p(n!) = p^{m-1} + p^{m-2} + \cdots + p + 1 = \frac{p^m - 1}{p-1} = \frac{n-1}{p-1}.$$

Então, quando n é uma potência de p, temos

$$\left|\frac{x^n}{n!}\right|_p = \frac{|x|_p^n}{p^{-v_p(n!)}} = \frac{|x|_p^n}{p^{-\frac{n-1}{p-1}}} \geq \frac{p^{\frac{-n}{p-1}}}{p^{-\frac{n-1}{p-1}}} = p^{\frac{-1}{p-1}}.$$

Portanto $\frac{x^n}{n!}$ não tende para 0 em $\mathbb{Q}_p$, e a série $\exp_p(x)$ não converge. □

O domínio de convergência de $\exp_p(x)$ pode ser reescrito de outro modo: a condição $|x|_p < p^{\frac{-1}{p-1}}$ equivale em $\mathbb{Q}_p$ a $x \in p\mathbb{Z}_p$ se $p \neq 2$ e a $x \in 4\mathbb{Z}_2$ se $p = 2$. Vamos agora ver que, como esperado, assim como o logaritmo transforma produtos em somas, a exponencial transforma somas em produtos.

Proposição 2.5.6. *Sejam $x, y \in p\mathbb{Z}_p$ (ou $4\mathbb{Z}_2$ se $p = 2$). Então*

$$\exp_p(x+y) = \exp_p(x)\exp_p(y).$$

Demonstração. Pela Proposição 2.4.4, temos

$$\exp_p(x)\exp_p(y) = \sum_{n=0}^{\infty} c_n,$$

onde

$$c_n = \sum_{k=0}^{n} \frac{x^k}{k!} \cdot \frac{y^{n-k}}{(n-k)!} = \frac{1}{n!}\sum_{k=0}^{n} \frac{n!}{k!(n-k)!} x^k y^{n-k} = \frac{1}{n!}\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = \frac{1}{n!}(x+y)^n.$$

Portanto

$$\exp_p(x)\exp_p(y) = \sum_{n=0}^{\infty} \frac{1}{n!}(x+y)^n = \exp_p(x+y),$$

como pretendido. □

Claro que estamos à espera de que as funções exponencial e logaritmo sejam, de alguma forma, inversas. É isso que a próxima proposição afirma. Vamos tratar apenas o caso $p \neq 2$ (o caso $p = 2$, não sendo mais difícil, é ligeiramente diferente). Suponha-se portanto que $p \neq 2$ ao longo do resto desta secção, a menos que seja afirmado o contrário explicitamente.

Lema 2.5.7. *Se $a \in 1 + p\mathbb{Z}_p$, então $\log_p(a) \in p\mathbb{Z}_p$, de modo que $\exp_p(\log_p(a))$ está bem definido, e*

$$\exp_p(\log_p(a)) = a.$$

Do mesmo modo, se $a \in p\mathbb{Z}_p$, então $\exp_p(a) \in 1 + p\mathbb{Z}_p$, de modo que $\log_p(\exp_p(a))$ está bem definido, e

$$\log_p(\exp_p(a)) = a.$$

Para provar isto, começamos por verificar que as igualdades apresentadas se verificam ao nível das séries de potências formais, e depois verificamos que estamos em condições de aplicar a Proposição 2.4.9.

Proposição 2.5.8. *Têm-se as igualdades de séries de potências formais*

$$\exp_p(f(X)) = 1 + X \quad e \quad f(\exp_p(X) - 1) = X.$$

Demonstração. Para a primeira igualdade, seja

$$\exp_p(f(X)) = h(X) = \sum_{n\geq 0} c_n X^n.$$

Pela Regra da Cadeia, temos

$$h'(X) = \exp_p'(f(X))f'(X) = \exp_p(f(X))f'(X) = h(X)f'(X)$$

onde usámos que a série $\exp_p(X)$ é igual à sua própria derivada, como uma conta direta mostra. Multiplicando por $1 + X$ e usando que $f'(X)(1 + X) = 1$, vem

$$h'(X)(1 + X) = h(X).$$

Mas

$$h'(X)(1 + X) = c_1 + \sum_{n\geq 1}(nc_n + (n + 1)c_{n+1})X^n$$

e portanto, como isto é igual à própria série $h(X)$, obtemos $c_1 = c_0$ e $nc_n + (n + 1)c_{n+1} = c_n$ para todo o $n \geq 1$, ou seja

$$(n + 1)c_{n+1} = (1 - n)c_n.$$

Como $c_0 = 1$ por uma conta direta, obtemos $c_1 = 1$, e a igualdade anterior com $n = 1$ dá-nos $c_2 = 0$. A igualdade acima dá-nos ainda que se $c_n = 0$ com $n > 1$ então $c_{n+1} = 0$. Conclui-se que $c_n = 0$ para todo o $n > 1$. Portanto $h(X) = 1 + X$.

Para a segunda igualdade, seja $j(X) = f(\exp_p(X) - 1)$. Derivando, obtemos

$$j'(X) = f'(\exp_p(X) - 1)\exp_p(X) = \frac{1}{1 + \exp_p(X) - 1} \cdot \exp_p(X) = 1.$$

Logo $j(X) = c + X$ para alguma constante c. Mas claramente $j(X)$ tem termo constante igual a 0, e portanto $j(X) = X$, como pretendido. □

Prova do Lema 2.5.7. Já vimos na Proposição 2.5.4 que $\log_p(a) \in p\mathbb{Z}_p$. Verifica-se de maneira semelhante que se $a \in p\mathbb{Z}_p$ então $\frac{a^n}{n!} \in p\mathbb{Z}_p$ para todo o $n \geq 1$, e portanto $\exp_p(a) \in 1 + p\mathbb{Z}_p$.

De modo a concluir as igualdades que faltam, basta provar que as composições na Proposição satisfazem as condições da Proposição 2.4.9. As duas primeiras condições resultam do que já fizemos.

Comecemos pela composta $f(\exp_p(x) - 1)$. Observe-se que para $n \geq 2$ se tem

$$v_p(n!) < n - 1$$

(vimos antes que se tem $v_p(n!) < \frac{n}{p-1}$), e portanto, se $x \in p\mathbb{Z}_p$, tem-se

$$v_p\left(\frac{x^{n-1}}{n!}\right) = (n - 1)v_p(x) - v_p(n!) > 0.$$

Portanto $\left|\frac{x^{n-1}}{n!}\right|_p < 1$ para $x \in p\mathbb{Z}_p$ e $n \geq 2$, logo

$$\left|\frac{x^n}{n!}\right|_p < |x|_p \text{ para } n \geq 2.$$

Conclui-se que todas as somas parciais da série

$$\sum_{n=1}^{\infty} \frac{x^n}{n!}$$

têm valor absoluto p-ádico igual a $|x|_p$, e portanto $|\exp_p(x) - 1|_p = |x|_p$ para $x \in p\mathbb{Z}_p$. Logo

$$\left|\frac{x^n}{n!}\right|_p \leq |\exp_p(x) - 1|_p$$

para todo o $n \geq 1$, e isto é precisamente a terceira condição da Proposição 2.4.9.

No caso da composta $\exp_p(f(x))$, o mesmo argumento funciona: como $|n!|_p \leq |n|_p$, as majorações encontradas para $\left|\frac{x^n}{n!}\right|_p$ também valem para $\left|\frac{x^n}{n}\right|_p$, portanto um argumento inteiramente análogo mostra que

$$\left|\frac{x^n}{n}\right|_p \leq |f(x)|_p$$

para $x \in p\mathbb{Z}_p$, que é a terceira condição da Proposição 2.4.9 aplicada à série $f(x)$. □

Este resultado permite-nos tirar algumas conclusões sobre a estrutura do grupo multiplicativo de $\mathbb{Q}_p$. De facto, resulta imediatamente o seguinte:

Corolário 2.5.9. *As funções* $\exp_p$ *e* $\log_p$ *definem isomorfismos inversos de grupos entre* $(1 + p\mathbb{Z}_p, \cdot)$ *e* $(p\mathbb{Z}_p, +)$*. Portanto,*

$$(1 + p\mathbb{Z}_p, \cdot) \cong (\mathbb{Z}_p, +).$$

Note-se que resulta daqui, por exemplo, que o grupo multiplicativo $1 + p\mathbb{Z}_p$ é livre de torção, o que não é particularmente óbvio! Mas nós gostaríamos de ficar com uma ideia da estrutura do grupo multiplicativo $\mathbb{Q}_p^\times$ *inteiro*, e não apenas do subgrupo $1 + p\mathbb{Z}_p$. Para isso precisamos do seguinte resultado.

Lema 2.5.10. *Seja* $U = 1 + p\mathbb{Z}_p$*, visto como um grupo com multiplicação. Então*

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times U.$$

Demonstração. Como qualquer número p-ádico diferente de 0 se pode escrever de maneira única na forma $p^n u$, com $n \in \mathbb{Z}$ e $u \in \mathbb{Z}_p^*$, a aplicação $\varphi : \mathbb{Z} \times \mathbb{Z}_p^\times \to \mathbb{Q}_p^\times$ definida por $\varphi(p, u) = p^n u$ define um isomorfismo entre $\mathbb{Z} \times \mathbb{Z}_p^\times$ e $\mathbb{Q}_p^\times$. Basta assim provar que

$$\mathbb{Z}_p^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \times U. \tag{2.14}$$

Consideremos o polinómio $f(X) = X^{p-1} - 1 \in \mathbb{Z}_p[X]$. Como é facto conhecido, o grupo multiplicativo $\mathbb{F}_p^\times$ (com $p-1$ elementos) é cíclico, e um gerador g desse grupo anula o polinómio $f(X)$ módulo p. Pelo Lema de Hensel (Lema 2.2.4) existe uma raiz $\zeta \in \mathbb{Z}_p$ de $f(X)$ tal que $\zeta \equiv g \pmod{p}$. Note-se que $\zeta \in \mathbb{Z}_p^\times$, uma vez que $|\zeta|_p^{p-1} = |\zeta^{p-1}|_p = 1$, logo $|\zeta|_p = 1$.

Definimos um homomorfismo $\psi : \mathbb{Z}/(p-1)\mathbb{Z} \times U \to \mathbb{Z}_p^\times$ por

$$\psi(a, u) = \zeta^a u.$$

Isto está bem definido, uma vez que ζ é um elemento de ordem $p-1$ em $\mathbb{Z}_p^\times$. Vamos mostrar que ψ é um isomorfismo:

- ψ é injetivo: suponha-se que $\zeta^a u = \zeta^b v$, com $a, b \in \mathbb{Z}/(p-1)\mathbb{Z}$ e $u, v \in U$. Avaliando a igualdade módulo p, como u e v são $1 \pmod p$ por definição de U conclui-se que $\zeta^a \equiv \zeta^b \pmod p$, e portanto $g^a = g^b$ em $\mathbb{F}_p^\times$ (uma vez que a projeção de ζ em $\mathbb{F}_p$ é igual a g por construção). Como g tem ordem $p-1$ (é um gerador de um grupo cíclico com $p-1$ elementos) resulta que $a \equiv b \mod p-1$, ou seja, a e b são iguais como elementos de $\mathbb{Z}/(p-1)\mathbb{Z}$. Mas então $\zeta^a = \zeta^b$, pelo que $u = v$. Logo ψ é injetivo.

- ψ é sobrejetivo: seja x um elemento arbitrário de $\mathbb{Z}_p^\times$. A projeção de x em $\mathbb{F}_p$ é não nula e portanto, como g gera $\mathbb{F}_p^\times$, existe $a \in \mathbb{Z}/(p-1)\mathbb{Z}$ tal que essa projeção é g^a. Deste modo tem-se $x \equiv \zeta^a \pmod p$, e portanto se $u = x\zeta^{-a}$ tem-se $u \equiv 1 \pmod p$, ou seja, $u \in U$. Desta forma $x = \zeta^a u$. Logo ψ é sobrejtivo.

E assim obtemos (2.14), como pretendido. □

Corolário 2.5.11. *Para todo o primo $p > 2$ tem-se*

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p.$$

O corolário anterior é falso para $p = 2$. De facto, nesse caso tem-se

$$\mathbb{Q}_2^\times \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2.$$

A diferença de estrutura entre o caso $p > 2$ e o caso $p = 2$ está relacionada com o facto de existirem *raízes primitivas* módulo todas as potências de p quando $p > 2$, mas não quando $p = 2$ (ou seja, os grupos $(\mathbb{Z}/p^n\mathbb{Z})^\times$ são todos cíclicos quando $p > 2$, mas não quando $p = 2$).

§2.6. O Teorema de Strassman

Nesta secção vamos apresentar um resultado muito útil sobre zeros de funções definidas por séries de potências. Pela primeira vez, vamos ver um resultado de Análise p-ádica que não tem nenhum resultado minimamente análogo em Análise Real ou Complexa. O resultado diz-nos que uma função definida por uma série de potências não nula na "bola unitária" $\mathbb{Z}_p$ tem um número finito de zeros em $\mathbb{Z}_p$. Isto, só por si, talvez não seja muito surpreendente, mas o Teorema de Strassman diz-nos mais: dá-nos um majorante explícito para o número de zeros em $\mathbb{Z}_p$ de uma função deste tipo.

Seja

$$f(X) = \sum_{n=0}^{\infty} a_n X^n$$

uma série de potências em $\mathbb{Q}_p[[X]]$, e suponha-se que $f(x)$ converge para $x \in \mathbb{Z}_p$. Então $\lim_{n\to\infty} a_n = 0$, e portanto a sucessão dos valores absolutos dos coeficientes $|a_n|_p$ tem um máximo. Esse máximo é atingido num número finito de valores de n; o maior desses valores é o nosso majorante para o número de zeros da função definida por $f(X)$ em $\mathbb{Z}_p$.

Teorema 2.6.1 (Teorema de Strassman)**.** *Seja*

$$f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Q}_p[[X]]$$

com $\lim_{n\to\infty} a_n = 0$ *(i.e. tal que* $f(x)$ *converge para* $x \in \mathbb{Z}_p$*). Suponha-se que nem todos os coeficientes* a_n *são iguais a* 0*, e seja* N *o maior inteiro tal que*

$$|a_N|_p = \max_{n\geq 0} |a_n|_p.$$

Então a função definida por $f(X)$ *em* $\mathbb{Z}_p$ *tem no máximo* N *zeros.*

Demonstração. Vamos chamar ao valor de N determinado pela condição do teorema o "número mágico" da série $f(X)$. Vamos provar o teorema por indução no número mágico de $f(X)$.

Se $f(X)$ tem número mágico 0, então $|a_0|_p > |a_n|_p$ para $n > 0$, e queremos provar que $f(x) \neq 0$ para todo o $x \in \mathbb{Z}_p$. De facto, se $f(x) = 0$, então

$$a_0 = -a_1 x - a_2 x^2 - \cdots$$

e em particular

$$|a_0|_p = |a_1 x + a_2 x^2 + \cdots|_p.$$

Mas como $x \in \mathbb{Z}_p$ tem-se

$$|a_1 x + a_2 x^2 + \cdots|_p \leq \max\{|a_1|_p |x|_p, |a_2|_p |x|_p^2, \cdots\} \leq \max\{|a_1|_p, |a_2|_p, \cdots\} < |a_0|_p.$$

Isto é uma contradição, e conclui o caso base.

Suponha-se agora que $f(X)$ tem número mágico $N > 0$, e que já provámos o teorema para séries de potências com número mágico $N - 1$. Queremos provar que $f(x) = 0$ para no máximo

N valores de $x \in \mathbb{Z}_p$. Se $f(x) \neq 0$ para todo o $x \in \mathbb{Z}_p$ não há nada a provar. Caso contrário, existe $\alpha \in \mathbb{Z}_p$ tal que $f(\alpha) = 0$. Então, para $x \in \mathbb{Z}_p$, temos

$$\begin{aligned} f(x) &= f(x) - f(\alpha) \\ &= \sum_{n\geq 0} a_n(x^n - \alpha^n) \\ &= \sum_{n\geq 0} a_n(x-\alpha)\sum_{k=0}^{n-1} \alpha^{n-1-k}x^k \\ &= (x-\alpha)\sum_{n\geq 0}\sum_{k=0}^{n-1} a_n\alpha^{n-1-k}x^k. \end{aligned}$$

Gostaríamos de reescrever o segundo fator como uma série de potências em x. Isso corresponde essencialmente a trocar a ordem dos somatórios acima, ou seja, é trabalho para a Proposição 2.4.3: definindo

$$x_{n,k} = \begin{cases} a_n\alpha^{n-1-k}x^k & \text{se } n \geq k+1 \\ 0 & \text{caso contrário} \end{cases}$$

queremos provar que, para todo o $\varepsilon > 0$, existe T tal que $|x_{n,k}|_p < \varepsilon$ sempre que $\max\{n,k\} \geq T$. Podemos supor $n \geq k+1$, e assim o máximo anterior é n. Mas existe T tal que se $n \geq T$ então $|a_n|_p < \varepsilon$, e como $\alpha, x \in \mathbb{Z}_p$ temos

$$|x_{n,k}|_p \leq |a_n|_p < \varepsilon$$

para $n \geq T$, como pretendido.

Portanto podemos mesmo trocar a ordem dos somatórios, e obtemos

$$\begin{aligned} f(x) &= (x-\alpha)\sum_{k\geq 0}\left(\sum_{n=k+1}^{\infty} a_n\alpha^{n-1-k}\right)x^k \\ &= (x-\alpha)g(x) \end{aligned}$$

onde

$$g(X) = \sum_{k\geq 0} b_k X^k$$

e por sua vez

$$b_k = \sum_{n=k+1}^{\infty} a_n\alpha^{n-1-k}.$$

Basta então provar que $g(x) = 0$ para no máximo $N-1$ valores de $x \in \mathbb{Z}_p$. Para isso, pela hipótese de indução, basta provar que $g(X)$ tem número mágico $N-1$.

Como

$$b_{N-1} = a_N + a_{N+1}\alpha + a_{N+2}\alpha^2 + \cdots$$

e

$$|a_{N+1}\alpha + a_{N+2}\alpha^2 + \cdots|_p \leq \max\{|a_{N+1}|_p, |a_{N+2}|_p, \ldots\} < |a_N|_p,$$

tem-se $|b_{N-1}|_p = |a_N|_p$. Além disso, para todo o k, diretamente pela definição de b_k e usando que $|\alpha|_p \leq 1$ tem-se

$$|b_k|_p \leq \max_{n\geq 0}\{|a_n|_p\} = |a_N|_p.$$

Portanto $|b_k|_p$ é máximo para $k = N-1$, e resta verificar que $|b_k|_p < |a_N|_p$ para $k > N-1$. Mas para $k \geq N$ a Desigualdade Ultramétrica e a definição de b_k dão-nos

$$|b_k|_p \leq \max_{n \geq k+1} |a_n|_p \leq \max_{n>N} |a_n|_p < |a_N|_p$$

como pretendido. Portanto o número mágico de $g(X)$ é de facto $N-1$, e então a equação $g(x) = 0$ tem no máximo $N-1$ soluções em $\mathbb{Z}_p$, e a equação $f(x) = 0$ tem no máximo N soluções, concluindo a prova do Teorema de Strassman. □

§2.7. Aplicações

Nesta secção vamos aplicar os conceitos que desenvolvemos nas secções anteriores para estudar uma classe de problemas para os quais os números p-ádicos, e em particular a Análise p-ádica, se revelam essenciais. Esses problemas estão relacionados com *sucessões definidas por recorrências lineares* (que vamos abreviar por SRLs).

Definição 2.7.1 (SRL)**.** Seja R um anel. Uma *sucessão definida por recorrência linear (SRL)* é uma sucessão $(a_n)_{n\geq 0}$ de elementos de R para a qual existe um inteiro positivo d e constantes $c_1, \ldots, c_d \in R$ tais que, para todo o inteiro positivo $n \geq d$,

$$a_n = c_1 a_{n-1} + \cdots + c_d a_{n-d}.$$

Exemplo 2.7.2. Alguns exemplos de SRLs:

(i) O exemplo canónico é a *sucessão de Fibonacci* $(f_n)_{n\geq 0}$ em $\mathbb{Z}$, definida por $f_0 = 0$, $f_1 = 1$ e

$$f_n = f_{n-1} + f_{n-2} \text{ para } n \geq 2.$$

Os primeiros termos são: $0, 1, 1, 2, 3, 5, 8, 13, 21 \ldots$.

(ii) A sucessão $(a_n)_{n\geq 0}$ em $\mathbb{Z}$ definida por $a_n = n$ é uma SRL: de facto, temos

$$a_n = 2a_{n-1} - a_{n-2} \text{ para } n \geq 2.$$

Um problema natural sobre SRLs é o seguinte: dada uma SRL $(a_n)_{n\geq 0}$ num anel R, o que podemos dizer sobre o conjunto dos inteiros n para os quais a_n toma um determinado valor fixo? Isto não é difícil para a sucessão de Fibonacci, que é claramente estritamente crescente, portanto cada valor inteiro é tomado pela sucessão de Fibonacci no máximo uma vez. Mas o mesmo pode não ser tão trivial para sucessões com um comportamento mais oscilatório.

O célebre Teorema de Skolem-Mahler-Lech responde a esta pergunta, e é um dos grandes triunfos da Análise p-ádica. Vamos dizer que uma *progressão aritmética completa de razão m* é o conjunto dos inteiros não negativos n com $n \equiv a \pmod{m}$, para algum a fixo.

Teorema 2.7.3 (Skolem-Mahler-Lech)**.** *Seja $(a_n)_{n\geq 0}$ uma SRL sobre um corpo K de característica 0, e seja c um elemento de K. Então o conjunto dos inteiros não negativos n tais que $a_n = c$ é a união de um conjunto finito com um número finito de progressões aritméticas completas da mesma razão.*

Este resultado foi provado em toda a generalidade por Lech em 1953, poucos anos depois de Skolem e Mahler terem provado alguns casos particulares, nomeadamente o caso em que $K = \mathbb{Q}$. Todas estas provas (do caso geral e dos casos particulares) utilizam Análise p-ádica, e até hoje não se conhece nenhuma prova que não a utilize.

Em vez de passarmos diretamente para uma prova geral deste resultado, vamos analisar um caso particular simples que já ilustra essencialmente uma boa parte das ideias envolvidas.

Considere-se a SRL $(u_n)_{n\geq 0}$ de números racionais que satisfaz $u_0 = 0$, $u_1 = 1$ e

$$u_n = u_{n-1} - 2u_{n-2}$$

para todo o $n \geq 2$. Vamos tentar determinar os valores de n para os quais $u_n = -1$. Os primeiros termos são:

n	u_n
0	0
1	1
2	1
3	-1
4	-3
5	-1
6	5
7	7
8	-3
9	-17
10	-11
11	23
12	45
13	-1
14	-91
15	-89

Olhando para a tabela vemos que $u_n = -1$ para $n \in \{3, 5, 13\}$, e é natural perguntarmo-nos se existem outros valores de n com essa propriedade. Pode ser surpreendente saber que este é um problema difícil, e precisamos de Análise p-ádica para o resolver.

Lema 2.7.4. *Se para a SRL definida acima se tem $u_n = -1$, então n é 3, 5 ou 13.*

Demonstração. Vamos começar por determinar uma fórmula explícita para u_n. Esta ideia funciona para determinar uma fórmula explícita para o termo geral de uma SRL em condições bastante gerais. A ideia é "trocar índice por expoente": procuramos u tal que $u_n = u^n$ satisfaz a relação de recorrência dada. Queremos portanto que

$$u^n = u^{n-1} - 2u^{n-2}$$

e cancelando u^{n-2} de ambos os lados da equação, chegamos a

$$u^2 - u + 2 = 0.$$

Existem duas soluções complexas desta equação, nomeadamente $u = \frac{1\pm\sqrt{-7}}{2}$; sejam α e β estas duas raízes. Conclui-se que as sucessões $(\alpha^n)_{n\geq 0}$ e $(\beta^n)_{n\geq 0}$ satisfazem a relação de recorrência que define u, mas infelizmente nenhuma delas satisfaz as condições iniciais para os termos de ordem 0 e 1. Mas notemos que qualquer *combinação linear* de duas sucessões que satisfazem a relação de recorrência dada também a satisfaz: ou seja, para quaisquer c, d a sucessão $(c_n)_{n\geq 0}$ definida por

$$c_n = c\alpha^n + d\beta^n$$

satisfaz a relação de recorrência $c_n = c_{n-1} - 2c_{n-2}$. Se encontrarmos c e d de tal modo que $c_0 = 0$ e $c_1 = 1$, obtemos portanto $c_n = u_n$ para todo o n. Resolvendo o sistema

$$\begin{cases} c + d = 0 \\ c\alpha + d\beta = 1 \end{cases}$$

obtemos a solução $c = \frac{1}{\alpha-\beta}$, $d = \frac{-1}{\alpha-\beta}$, e conclui-se que

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

para todo o inteiro $n \geq 0$.

Agora que temos uma fórmula explícita para u_n, poderíamos pensar que reduzimos o problema a uma equação simples. Infelizmente, a equação

$$\alpha^n - \beta^n = \beta - \alpha$$

não é nada simples. Estamos à procura dos valores de n para os quais $\alpha^n - \beta^n$ toma um determinado valor fixo. Não há nenhuma razão óbvia à partida que garanta que $\alpha^n - \beta^n$ não pode tomar um mesmo valor muitas vezes: como α e β têm o mesmo módulo em $\mathbb{C}$, não temos nenhuma maneira imediata de garantir que o módulo de $\alpha^n - \beta^n$ se afasta rapidamente de 0.

Mas não temos de trabalhar em $\mathbb{C}$! Os números

$$\alpha = \frac{1 + \sqrt{-7}}{2}, \quad \beta = \frac{1 - \sqrt{-7}}{2}$$

fazem sentido em qualquer corpo de característica diferente de 2 onde -7 é um quadrado. Em particular, fazem sentido em $\mathbb{Q}_p$ para muitos primos p: especificamente todos os primos diferentes de 7 tais que -7 é um quadrado em $\mathbb{F}_p$, pelo Lema de Hensel (especificamente pelo Exemplo 2.2.5(i)). Excluindo o primo $p = 2$ por razões patológicas, o menor tal primo que encontramos é $p = 11$. Vamos então trabalhar em $\mathbb{Q}_{11}$.

Temos

$$X^2 - X + 2 \equiv (X - 5)(X - 7) \pmod{11}.$$

O Lema de Hensel garante-nos assim duas raízes α e β de $X^2 - X + 2$ em $\mathbb{Z}_{11}$ que são congruentes com 5 e 7 módulo 11, respetivamente[2]. Para o que se segue será importante conhecermos α e β módulo 11^2. Seja assim $\alpha = 5 + 11k$, de tal modo que

$$(5 + 11k)^2 - (5 + 11k) + 2 = 0.$$

Desenvolvendo e olhando para a igualdade módulo 11^2, ficamos com

$$25 + 110k - 5 - 11k + 2 \equiv 0 \pmod{11^2} \quad \text{ou seja,} \quad 99k \equiv -22 \pmod{11^2}.$$

Dividindo por 11 ficamos com $9k \equiv -2 \pmod{11}$, que nos dá $k \equiv 1 \pmod{11}$, e portanto $\alpha \equiv 5 + 1 \cdot 11 = 16 \pmod{11^2}$. Como $\alpha + \beta = 1$ pelas fórmulas de Viète (ou repetindo o cálculo para β) conclui-se que $\beta \equiv 106 \pmod{11^2}$.

Naturalmente, ainda temos

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

[2]Estes α e β são "os mesmos" que tínahmos atrás, pois são elementos de $\mathbb{Q}(\sqrt{-7})$ que está contido simultaneamente em $\mathbb{C}$ e $\mathbb{Q}_{11}$.

(só utilizámos o facto de α e β serem raízes de $X^2 - X + 2$ para chegar a esta conclusão) e portanto queremos determinar os valores de n para os quais $\alpha^n - \beta^n = -\alpha + \beta$. A ideia é desenvolver $\alpha^n - \beta^n$ como uma série de potências em n. Ficamos assim com uma equação do tipo

$$(\text{série de potências}) = 0$$

e podemos tentar utilizar o Teorema de Strassman (Teorema 2.6.1) para majorar o número de soluções desta equação (em $\mathbb{Z}_{11}$, e portanto em $\mathbb{Z}$). Infelizmente, desenvolver α^n (e/ou β^n) como uma série de potências em n não é assim tão simples. A ideia seria escrever

$$\alpha^n = \exp(n \log(\alpha)) = \sum_{k \geq 0} \frac{\log(\alpha)^k}{k!} n^k$$

mas $\log(\alpha)$ não está bem definido: não temos $\alpha \equiv 1 \pmod{11}$. A solução para isto é escrever $n = 10s + r$, com $r \in \{0, \ldots, 9\}$. Sendo $A = \alpha^{10}$, temos

$$\alpha^n = \alpha^{10s+r} = A^s \alpha^r.$$

Para um valor de r fixo, podemos desenvolver isto como série de potências em s: como $A = \alpha^{10} \equiv 1 \pmod{11}$ (pelo Pequeno Teorema de Fermat), desta vez $\log(A)$ está bem definido! E portanto A^s pode ser escrito como uma série de potências em s. Claro que obtemos uma equação diferente para cada valor de $r \in \{0, \ldots, 9\}$, mas só temos um número finito de valores de r, por isso esse não é um problema muito sério.

De facto podemos excluir logo a maioria dos valores de r: como

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{A^s \alpha^r - B^s \beta^r}{\alpha - \beta} \equiv \frac{\alpha^r - \beta^r}{\alpha - \beta} = u_r \pmod{11},$$

se $u_n = -1$ devemos ter $u_r \equiv -1 \pmod{11}$. Olhando por exemplo para a tabela dos valores iniciais de u_n vemos que, para $r \in \{0, \ldots, 9\}$, só temos $u_r \equiv -1 \pmod{11}$ para $r = 3$ e $r = 5$. Podemos portanto supor que $r = 3$ ou $r = 5$.

Comecemos pelo caso $r = 5$, que é mais simples. Queremos determinar todos os inteiros $s \geq 0$ para os quais

$$A^s \alpha^5 - B^s \beta^5 = -\alpha + \beta.$$

Sejam $a = A - 1$ e $b = B - 1$, de modo que $a, b \in 11\mathbb{Z}_{11}$. Para $s \in \mathbb{Z}$ tem-se então

$$A^s = \exp(s \log_{11}(1 + a)) = \sum_{k \geq 0} \frac{\log(1 + a)^k}{k!} s^k$$

e analogamente

$$B^s = \exp(s \log_{11}(1 + a)) = \sum_{k \geq 0} \frac{\log(1 + a)^k}{k!} s^k$$

pelo que

$$A^s \alpha^5 - B^s \beta^5 + \alpha - \beta = (\alpha^5 - \beta^5 + \alpha - \beta) + \sum_{k \geq 1} \frac{\log(1 + a)^k \alpha^5 - \log(1 + b)^k \beta^5}{k!} s^k.$$

Seja

$$f(s) = \sum_{k \geq 0} c_k s^k$$

o lado direito da igualdade anterior; queremos resolver a equação $f(s) = 0$. Notemos que $c_0 = \alpha^5 - \beta^5 + \alpha - \beta = 0$ uma vez que $u_5 = -1$, logo $|c_0|_{11} = 0$. Além disso, uma conta simples usando $\alpha \equiv 16 \pmod{11^2}$ dá-nos $\alpha^5 \equiv 111 \pmod{11^2}$ e $a = \alpha^{10} - 1 \equiv 99 \pmod{11^2}$; do mesmo modo, $\beta^5 \equiv 21 \pmod{11^2}$ e $b \equiv 77 \pmod{11^2}$. Tudo isto é suficiente para calcular

$$c_1 = \log(1+a)\alpha^5 - \log(1+b)\beta^5$$

módulo 11^2. De facto, como

$$\log(1+a) = a - \frac{a^2}{2} + \frac{a^3}{3} - \cdots$$

e todas as parcelas $\frac{a^j}{j}$ estão em $11^2\mathbb{Z}_{11}$ para $j \geq 2$, pelo que $\log(1+a) \equiv a \equiv 99 \pmod{11^2}$ e $\log(1+b) \equiv b \equiv 77 \pmod{11^2}$. Finalmente,

$$c_1 \equiv 99 \times 111 - 77 \times 21 \equiv 11 \times 5 \pmod{11^2}.$$

Logo c_1 é divisível por 11 mas não por 11^2 e portanto $v_{11}(c_1) = 1$, ou seja, $|c_1|_{11} = \frac{1}{11}$. E para $k \geq 2$ tem-se

$$v_{11}(\log(1+a)^k\alpha^5 - \log(1+b)^k\beta^5) \geq k$$

uma vez que 11 divide $\log(1+a)$ e $\log(1+b)$. Isto é suficiente para concluir que $v_{11}(c_k) \geq 2$, e $|c_k|_{11} \leq \frac{1}{11^2}$. Portanto o "número mágico" do Teorema 2.6.1 aplicado a $f(s)$ é 1. Logo a equação $f(s) = 0$ tem no máximo uma solução. Mas já sabemos que $s = 0$ é uma solução, correspondente a $n = 5$, portanto é a única. Ou seja, o caso $r = 5$ só nos dá a solução $n = 5$ da equação $u_n = -1$.

Resta ver o caso $r = 3$. Queremos agora determinar os inteiros $s \geq 0$ para os quais

$$A^s\alpha^3 - B^s\beta^3 = -\alpha + \beta. \tag{2.15}$$

Novamente escrevemos

$$A^s\alpha^3 - B^s\beta^3 + \alpha - \beta = (\alpha^3 - \beta^3 + \alpha - \beta) + \sum_{k\geq 1} \frac{\log(1+a)^k\alpha^3 - \log(1+b)^k\beta^3}{k!} s^k = \sum_{k\geq 0} c_k s^k$$

e notamos que $c_0 = 0$, pois $u_3 = -1$. Usar que

$$v_{11}(\log(1+a)^k\alpha^3 - \log(1+b)^k\beta^3) \geq k$$

é suficiente para concluir que $v_{11}(c_k) \geq 3$ para $k \geq 3$, e portanto $|c_k|_3 \leq \frac{1}{11^3}$. Vamos agora determinar c_1 e c_2 módulo 11^2. Temos $c_1 = \log(1+a)\alpha^3 - \log(1+b)\beta^3$ e $\log(1+a) \equiv a - \frac{a^2}{2} \pmod{11^3}$; determinando α módulo 11^3 da mesma forma que o determinámos módulo 11^2 podemos determinar $a = \alpha^{10} - 1 \pmod{11^3}$, e assim sabemos $\log(1+a)$ módulo 11^3. Do mesmo modo determinamos $\log(1+b)$. A conclusão é que

$$c_1 \equiv 8 \times 11^2 \pmod{11^3} \quad \text{e} \quad c_2 \equiv 3 \times 11^2 \pmod{11^3}.$$

Portanto $|c_1|_{11} = |c_2|_{11} = \frac{1}{11^2}$, e o número mágico do Teorema de Strassman é, desta vez, igual a 2. Conclui-se que a equação (2.15) tem no máximo duas soluções em $\mathbb{Z}_{11}$. Mas já sabemos duas soluções, nomeadamente $s = 0$ e $s = 1$, correspondentes a $n = 3$ e $n = 13$. Estas são, portanto, as *únicas* soluções, o que conclui a prova do Lema. □

Exatamente a mesma ideia permite determinar os valores de n para os quais $u_n = 1$.

Lema 2.7.5. *Se para a mesma SRL se tem $u_n = 1$, então n é 1 ou 2.*

Sermos capazes de provar estes resultados já é uma excelente utilidade da Análise p-ádica. Mas para o caso de o leitor estar a pensar "Mas para que é que determinar os valores de n tais que $u_n = c$ serve?", deixamos aqui uma explicação: este tipo de problemas aparece muito naturalmente em tentativas de resolver equações diofantinas. Vamos ver um exemplo.

Lema 2.7.6. *As soluções inteiras da equação*

$$x^2 + 7 = 2^m$$

são $(x, m) = (\pm 1, 3), (\pm 3, 4), (\pm 5, 5), (\pm 11, 7)$ e $(\pm 181, 15)$.

Demonstração. Precisamos de um pouco de Teoria Algébrica dos Números básica. Vamos utilizar os seguintes factos sobre o anel $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$:

(i) $\mathcal{O}$ é um domínio de fatorização única;

(ii) As únicas unidades em $\mathcal{O}$ são 1 e -1.

A propriedade (i) decorre de que R é um domínio Euclideano, com valorização dada pela *norma*, que se obtém restringindo a norma complexa a R:

$$\mathrm{N}(z) = z \cdot \overline{z}.$$

A propriedade (ii) decorre de que se $a \in R$ é uma unidade então $\mathrm{N}(a) = 1$. É fácil concluir daqui que $a = -1$ ou $a = 1$.

Passemos à equação. Obviamente x é ímpar, e podemos escrevê-lo como $2y - 1$ para algum inteiro y. A equação fica

$$(2y-1)^2 + 7 = 2^m, \quad \text{ou seja,} \quad y^2 - y + 2 = 2^{m-2}.$$

Em R, temos a fatorização $y^2 - y + 2 = (y - \alpha)(y - \beta)$, onde $\alpha = \frac{1+\sqrt{-7}}{2}$ e $\beta = \frac{1-\sqrt{-7}}{2}$. Notemos que $\alpha\beta = 2$, portanto obtemos

$$(y - \alpha)(y - \beta) = \alpha^{m-2}\beta^{m-2}. \tag{2.16}$$

Como $\mathrm{N}(\alpha) = 2$, α é primo em R; caso contrário poderíamos escrever $\alpha = pq$ onde p e q não são unidades em R, mas então

$$2 = \mathrm{N}(\alpha) = \mathrm{N}(p)\mathrm{N}(q)$$

o que implica que um dos números $\mathrm{N}(p)$ e $\mathrm{N}(q)$ seja igual a 1, o que implica que p seja uma unidade ou q seja uma unidade, contradição. Do mesmo modo vemos que β é primo em R. Portanto por (2.16) conclui-se que $y - \alpha = \pm\alpha^i\beta^j$ para alguns i e j. Por outro lado,

$$y - \beta = \overline{y - \alpha} = \pm\beta^i\alpha^j$$

uma vez que α e β são conjugados, e portanto $(y-\alpha)(y-\beta) = \alpha^{i+j}\beta^{i+j}$. Resulta que $j = m-2-i$, $y - \alpha = \pm\alpha^i\beta^{m-2-i}$ e $y - \beta = \pm\alpha^{m-2-i}\beta^i$.

Mas temos $\alpha - \beta = \sqrt{-7}$ e portanto $\mathrm{N}(\alpha - \beta) = 7$; como $\mathrm{N}(\alpha - \beta)$ é primo com $\mathrm{N}(2) = 4$ conclui-se, pela multiplicatividade da norma, que $\alpha - \beta$ e 2 são coprimos em R. Como $\alpha\beta$ é a fatorização em primos de 2 em R conclui-se que $\alpha - \beta$ não é divisível por α nem β; mas

$$\alpha - \beta = (y - \beta) - (y - \alpha) = \pm\alpha^{m-2-i}\beta^i - \pm\alpha^i\beta^{m-2-i}.$$

Para isto não ser divisível por α nem β devemos ter $\min(i, m-2-i) = 0$, ou seja, $i = 0$ ou $i = m-2$. Obtemos uma igualdade

$$\alpha - \beta = \pm(\alpha^{m-2} - \beta^{m-2}).$$

Mas isto implica $u_{m-2} = \pm 1$! Pelos Lemas 2.7.4 e 2.7.5 conclui-se que $m - 2 \in \{1, 2, 3, 5, 13\}$, logo $m \in \{3, 4, 5, 7, 15\}$, e a partir daqui é trivial concluir a prova. □

Agora que vimos que resolver equações do tipo $u_n = c$ não é totalmente inútil, vamos avançar no sentido de uma prova geral do Teorema de Skolem-Mahler-Lech (Teorema 2.7.3). Vamos pensar em como podemos adaptar as provas dos Lemas 2.7.4 e 2.7.5. Para simplificar, suponhamos primeiro que $K = \mathbb{Q}$, e que a nossa SRL satisfaz a relação de recorrência

$$a_n = c_1 a_{n-1} + \cdots + c_d a_{n-d}.$$

Usando um raciocínio semelhante ao ilustrado no início da prova do Lema 2.7.4, podemos exprimir o termo geral a_n como combinação linear das raízes do polinómio

$$X^d - c_1 X^{d-1} - \cdots - c_d,$$

pelo menos se essas raízes $\theta_1, \cdots, \theta_d$ forem todas distintas. Uma vez mais podemos aplicar o raciocínio utilizado na prova do Lema 2.7.4, desde que consigamos visualizar $\theta_1, \cdots, \theta_d$ como elementos de $\mathbb{Q}_p$ para algum primo p.

Queremos então em particular encontrar um primo p tal que o polinómio anterior tenha uma raiz em $\mathbb{F}_p$ (que em condições bastante gerais podemos levantar para uma raiz em $\mathbb{Z}_p$ pelo Lema de Hensel). Para isso podemos utilizar o seguinte resultado clássico de Teoria dos Números.

Proposição 2.7.7. *Seja $P(X)$ um polinómio não constante com coeficientes inteiros. Então existem infinitos primos p tais que p divide $P(n)$, para algum inteiro n.*

Demonstração. A ideia é imitar a prova clássica de Euclides da existência de uma infinidade de primos (que é precisamente este resultado para $P(X) = X$). Seja

$$P(X) = c_m X^m + \cdots + c_0$$

com $c_m \neq 0$. Se $c_0 = 0$ o resultado é trivial pois $P(p)$ é divisível por p. Caso contrário, considere-se a igualdade

$$P(c_0 t) = c_m c_0^m t^m + \cdots + c_1 c_0 t + c_0 = c_0(c_m c_0^{m-1} t^m + \cdots + c_1 t + 1) = c_0 Q(t), \tag{2.17}$$

onde $Q(X)$ é um polinómio de grau m com coeficiente constante 1. Suponha-se que existe apenas um número finito de primos $p_1, \ldots, p_k$ que dividem $P(n)$ para algum n, e seja a um inteiro tal que $Q(ap_1 \cdots p_k) \neq \pm 1$, que existe pois o polinómio $Q(X)$ não é constante. Então como

$$Q(ap_1 \cdots p_k) \equiv 1 \pmod{p_i}$$

para $i = 1, \cdots, k$, o número $Q(ap_1 \cdots p_k)$ não é divisível por nenhum dos primos $p_1, \ldots, p_k$, e tem um divisor primo p diferente desses primos. Mas então, por (2.17), p divide $P(c_0 a p_1 \cdots p_k)$. Conclui-se que $p_1, \ldots, p_k$ não são os únicos primos que dividem $P(n)$ para algum n, e esta contradição prova a proposição. □

Voltando ao contexto anterior à proposição, isto garante-nos que podemos encontrar infinitos primos p tais que o polinómio $X^d - c_1 X^{d-1} - \cdots - c_d$ tem uma raiz em $\mathbb{F}_p$, e portanto, se estivermos em condições de aplicar o Lema de Hensel, podemos mergulhar um dos θ_i em $\mathbb{Q}_p$. Infelizmente, isso não chega: queremos encontrar um primo p tal que o polinómio anterior tem *todas* as raízes em $\mathbb{F}_p$, e não apenas uma.

Curiosamente, existe uma maneira elegante de dar a volta a esse obstáculo usando a Proposição 2.7.7, juntamente com um resultado de Teoria de Galois. A ideia é a seguinte: consideramos a extensão

$$\mathbb{Q}(\theta_1, \ldots, \theta_d)$$

de $\mathbb{Q}$, e observamos que, pelo *Teorema do Elemento Primitivo* (aplicável a quaisquer extensões separáveis, em particular a extensões de corpos de característica 0), esta extensão é uma *extensão simples*, ou seja, existe θ tal que

$$\mathbb{Q}(\theta) = \mathbb{Q}(\theta_1, \ldots, \theta_d).$$

Seja agora $P(X)$ o polinómio mínimo de θ sobre $\mathbb{Q}$. Pela Proposição 2.7.7 existem infinitos primos p para os quais a equação $P(x) = 0$ tem uma solução em $\mathbb{F}_p$, e pode-se verificar facilmente que a condição do Lema de Hensel só pode falhar para um número finito de primos p, portanto para infinitos primos p a equação $P(x) = 0$ tem uma solução em $\mathbb{Q}_p$. Obtemos assim um *mergulho*

$$\mathbb{Q}(\theta) \hookrightarrow \mathbb{Q}_p$$

e como $\mathbb{Q}(\theta)$ contém todas as raízes $\theta_1, \ldots, \theta_d$, conclui-se que estas também são mergulhadas em $\mathbb{Q}_p$!

Isto esboça a ideia da prova do Teorema de Skolem-Mahler-Lech sobre $\mathbb{Q}$. Vamos agora formalizar isto no contexto mais geral de corpos arbitrários de característica 0. Para isso precisamos da noção de *grau de transcendência* de uma extensão de corpos. Se L/K é uma extensão de corpos, dizemos que elementos $\alpha_1, \ldots, \alpha_n$ de L são *algebricamente independentes* sobre K se sempre que $P(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ é um polinómio e $P(\alpha_1, \ldots, \alpha_n) = 0$, então $P = 0$. Dizemos que a extensão L/K é *puramente transcendente* se L é gerado sobre K por elementos de L algebricamente independentes sobre K. Pode-se provar que, embora esse conjunto gerador formado por elementos algebricamente independentes sobre K não seja único, quaisquer dois tais conjuntos têm o mesmo cardinal. Esse cardinal designa-se o *grau de transcendência* de L/K. Podemos estender o conceito de grau de transcendência para extensões não necessariamente puramente transcendentes do seguinte modo: se M/K é uma extensão arbitrária, então podemos decompô-la usando uma extensão intermédia L/K tal que L/K é uma extensão puramente transcendente e M/L é uma extensão algébrica. O grau de transcendência de L/K é determinado por M, e chamamos-lhe o *grau de transcendência* de M/K.

Qualquer corpo de característica 0 é automaticamente uma extensão de $\mathbb{Q}$. No caso particular de $\mathbb{Q}_p$, temos o seguinte resultado:

Proposição 2.7.8. *O grau de transcendência de $\mathbb{Q}_p$ sobre $\mathbb{Q}$ é infinito.*

Demonstração. Só precisamos de utilizar o facto de que $\mathbb{Q}_p$ é não numerável. Uma maneira de provar isso é utilizar a Proposição 2.1.8, que nos dá que existe uma bijeção entre $\mathbb{Z}_p$ e o conjunto das sucessões $(a_n)_{n\geq 0}$ de elementos de $\{0,\ldots,p-1\}$. Como este conjunto não é numerável conclui-se que $\mathbb{Z}_p$ não é numerável, e, por maioria de razão, $\mathbb{Q}_p$ também não é.

Por outro lado, qualquer extensão de $\mathbb{Q}$ com grau de transcendência finito é automaticamente numerável. De facto, dada uma tal extensão M, existe uma extensão intermédia $L/\mathbb{Q}$ tal que $L=\mathbb{Q}(\alpha_1,\ldots,\alpha_n)$, para alguns α_i, e M é uma extensão algébrica de L. Ora, L é numerável pois qualquer elemento de L se pode escrever como uma fração racional com coeficientes racionais nos α_i e o conjunto dessas frações racionais é numerável. Por fim, uma extensão algébrica de um corpo numerável também é numerável: qualquer elemento de M é raiz de um polinómio não nulo com coeficientes em L, o conjunto desses polinómios é numerável e cada polinómio tem um número finito de raízes. □

Usando este resultado podemos provar o seguinte lema, que nos dá, em condições bastante gerais, o tão desejado mergulho de um corpo de característica 0 em algum $\mathbb{Q}_p$.

Lema 2.7.9 (Lema do Mergulho)**.** *Seja K um corpo de característica 0 tal que K é finitamente gerado sobre $\mathbb{Q}$, e seja S um conjunto finito de elementos não nulos de K. Então, para infinitos primos p, existe um mergulho, i.e., um homomorfismo injetivo*

$$\alpha : K \hookrightarrow \mathbb{Q}_p$$

tal que $|\alpha(c)|_p = 1$ (ou seja, $\alpha(c)\in\mathbb{Z}_p^\times$) para todo o $c\in S$.

Demonstração. Estendendo S se necessário, podemos supor que se $c\in S$ então $c^{-1}\in S$. Deste modo, basta garantir que $|\alpha(c)|_p\leq 1$ (ou seja, $\alpha(c)\in\mathbb{Z}_p$) para todo o $c\in S$ (porquê?).

A condição de K ser finitamente gerado sobre $\mathbb{Q}$ garante que existem $x_1,\ldots,x_m$ algebricamente independentes sobre $\mathbb{Q}$ tais que $K/\mathbb{Q}(x_1,\ldots,x_m)$ é uma extensão finita. Sendo uma extensão finita de corpos de característica 0, o Teorema do Elemento Primitivo garante-nos que é uma extensão simples, e em particular existe $y\in K$, algébrico sobre $\mathbb{Q}(x_1,\ldots,x_m)$, tal que

$$K=\mathbb{Q}(y,x_1,\ldots,x_m).$$

Para cada $c\in S$, podemos escrever

$$c=\frac{U_c(y,x_1,\ldots,x_m)}{V_c(x_1,\ldots,x_m)}$$

onde U_c, V_c são polinómios com coeficientes racionais em $m+1$ e m variáveis, respetivamente, e $V_c\neq 0$. Como y é algébrico sobre $\mathbb{Q}(x_1,\ldots,x_m)$ existe um polinómio $H\in\mathbb{Q}[Y,X_1,\ldots,X_m]$ tal que $H(y,x_1,\ldots,x_m)=0$. Seja $G(Y)=H(Y,x_1,\ldots,x_m)$ o polinómio mínimo de y sobre $\mathbb{Q}(x_1,\ldots,x_n)$, e seja $H_0(X_1,\ldots,X_m)$ o coeficiente líder (ou seja, o coeficiente da maior potência de Y que aparece em $G(Y)$).

Seja ainda $\Delta(X_1,\ldots,X_m)$ o *discriminante*[3] do polinómio $G(Y)$. Podemos supor sem perda de generalidade que todos os polinómios introduzidos até agora têm coeficientes inteiros.

Escolhemos inteiros $a_1,\ldots,a_m$ tais que todos os números

$$\Delta(a_1,\ldots,a_m), H_0(a_1,\ldots,a_m), V_c(a_1,\ldots,a_m)$$

[3] O discriminante de um polinómio $P(Y)\in L[Y]$, sendo L um corpo, é o produto $\prod_{i<j}(\beta_i-\beta_j)^2$ onde $\beta_1,\ldots,\beta_s$ são as raízes de $P(Y)$; sendo uma expressão polinomial simétrica nas raízes, o discriminante é um elemento do corpo base L.

são diferentes de 0 (para todo o $c \in S$); observe-se para isto que Δ (como um polinómio em m variáveis) é diferente de 0 (é o discriminante de um polinómio irredutível sobre um corpo de característica 0). Pela Proposição 2.7.7, existem infinitos primos p tais que a congruência

$$H(b, a_1, \ldots, a_m) \equiv 0 \pmod{p} \tag{2.18}$$

tem solução em $\mathbb{Z}$. Por outro lado, só há um número finito de primos que dividem $\Delta(a_1, \ldots, a_m)$ ou $V_c(a_1, \ldots, a_m)$ para algum $c \in S$; assim, podemos escolher infinitos primos p tais que a congruência anterior tem solução e tal que

$$p \nmid \Delta(a_1, \ldots, a_m).$$

Vamos provar que existe um mergulho de K em $\mathbb{Q}_p$ para esses primos p. Pelo Lema 2.7.8, existem $t_1, \ldots, t_m \in \mathbb{Q}_p$ algebricamente independentes sobre $\mathbb{Q}$. Multiplicando os t_i por potências de p apropriadas podemos supor que $t_i \in p\mathbb{Z}_p$ para cada i. Definimos agora

$$\xi_i = a_i + t_i$$

para $i = 1, \ldots, m$. Como os a_i são inteiros, $t_1, \ldots, t_m$ são algebricamente independentes sobre $\mathbb{Q}$ e tem-se $\xi_i \equiv a_i \pmod{p}$ para cada i. Portanto a congruência

$$H(b, \xi_1, \ldots, \xi_m) \equiv 0 \pmod{p}$$

tem solução, por (2.18). Além disso, as raízes em $\mathbb{F}_p$ do polinómio $H(X, \xi_1, \ldots, \xi_m)$ são *simples*: isso decorre da definição de discriminante e do facto de que $\Delta(\xi_1, \ldots, \xi_m) \neq 0$ em $\mathbb{F}_p$! Portanto, pelo Lema de Hensel, existe $\eta \in \mathbb{Z}_p$ tal que

$$H(\eta, \xi_1, \ldots, \xi_m) = 0.$$

E agora temos tudo o que precisamos para definir α: definimo-lo por

$$\alpha(x_i) = \xi_i \text{ para } i = 1, \ldots, m \text{ e } \alpha(y) = \eta.$$

Isto está bem definido e é injetivo: $\xi_1, \ldots, \xi_m$ são algebricamente independentes sobre $\mathbb{Q}$ e η, por construção, satisfaz a mesma relação algébrica sobre $\mathbb{Q}(\xi_1, \ldots, \xi_m)$ que y satisfaz sobre $\mathbb{Q}(x_1, \ldots, x_m)$. Além disso, para $c \in S$,

$$\alpha(c) = \frac{U_c(\eta, \xi_1, \ldots, \xi_n)}{V_c(\xi_1, \ldots, \xi_n)}$$

e isto pertence a $\mathbb{Z}_p$, uma vez que $\eta, \xi_1, \ldots, \xi_n$ pertencem a $\mathbb{Z}_p$ e o denominador não é divisível por p por hipótese. □

Com isto, estamos prontos para adaptar a ideia da prova do Lema 2.7.4 para dar uma prova completa do Teorema de Skolem-Mahler-Lech.

Prova do Teorema 2.7.3. Suponha-se que K tem característica 0 e a SRL $(a_n)_{n\geq 0}$ de elementos de K satisfaz

$$a_n = c_1 a_{n-1} + \cdots + c_d a_{n-d}$$

para todo o $n \geq d$, para algumas constantes $c_1, \ldots, c_d \in K$. Pela teoria geral das SRLs, existem $\theta_1, \ldots, \theta_e$ numa extensão algébrica de K e polinómios $P_1, \ldots, P_e$ tais que

$$a_n = P_1(n)\theta_1^n + \cdots + P_e(n)\theta_e^n \text{ para todo o } n \geq 0.$$

Não podemos usar diretamente o Lema 2.7.9 porque não temos a garantia de que K é finitamente gerado sobre $\mathbb{Q}$. Mas isso é fácil de rodear; todos os elementos da sucessão $(a_n)_{n\geq 0}$ estão no subcorpo de K gerado sobre $\mathbb{Q}$ pelos coeficientes dos polinómios P_i e por $\theta_1, \ldots, \theta_e$. Podemos então supor sem perda de generalidade que K é esse corpo, que já é finitamente gerado, e agora já podemos aplicar o Lema 2.7.9; este permite-nos supor que $K \subseteq \mathbb{Q}_p$ para algum primo $p > 2$, e ainda que $\theta_1, \ldots, \theta_e \in \mathbb{Z}_p^\times$.

Para $i = 1, \ldots, e$, seja $\Theta_i = \theta_i^{p-1}$, e observe-se que pelo Pequeno Teorema de Fermat se tem $\Theta_i \equiv 1 \pmod{p}$. Deste modo $\log(\Theta_i)$ está bem definido. Agora fixamos $c \in K$ e procuramos soluções de $a_n = c$ com n em cada classe de congruência módulo $p-1$. Fixamos $r \in \{0, \ldots, p-2\}$ e escrevemos $n = (p-1)s + r$, com s inteiro não negativo. Em $\mathbb{Q}_p$, tem-se

$$\begin{aligned} a_n - c &= P_1(n)\theta_1^n + \cdots + P_e(n)\theta_e^n - c \\ &= P_1((p-1)s+r)\theta_1^{(p-1)s+r} + \cdots + P_e((p-1)s+r)\theta_e^{(p-1)s+r} - c \\ &= P_1((p-1)s+r)\Theta_1^s\theta_1^r + \cdots + P_e((p-1)s+r)\Theta_e^s\theta_e^r - c \\ &= \theta_1^r P_1((p-1)s+r)\exp(s\log(\Theta_1)) + \cdots + \theta_e^r P_e((p-1)s+r)\exp(s\log(\Theta_r)) - c. \end{aligned}$$

Isto pode ser escrito como uma série de potências em s, que converge em $\mathbb{Z}_p$. Agora,

- Se essa série não for a série nula, então pelo Teorema de Strassman (Teorema 2.6.1) só tem um número finito de zeros, e a equação $a_n = c$ tem um número finito de soluções com $n \equiv r \pmod{p-1}$.
- Se essa série for a série nula, então $a_n = c$ para todo o $n \equiv r \pmod{p-1}$, e obtemos uma progressão aritmética completa de razão $p-1$ formada por soluções da equação $a_n = c$.

E com isto provámos o teorema. □

3. Corpos locais

§3.1. Corpos valorados discretos completos

O objetivo deste capítulo é generalizar o estudo dos números p-ádicos para outros corpos valorados com propriedades semelhantes, os chamados *corpos locais*. Dos corpos interessantes de um ponto de vista aritmético, estes são os corpos mais agradáveis a seguir aos corpos finitos, e o seu estudo é em grande parte facilitado pelo nosso conhecimento sobre corpos finitos através do Lema de Hensel. Uma introdução detalhada aos corpos finitos é feita no Apêndice A.

O estudo de cada um destes corpos individualmente é muito semelhante ao estudo dos p-ádicos, e de facto alguns dos resultados que vamos encontrar a seguir são completamente análogos a resultados provados no capítulo anterior, pelo que não os provaremos de novo aqui com detalhe. Começamos com uma maneira alternativa útil de pensar num valor absoluto não arquimediano.

Definição 3.1.1. Seja K um corpo. Uma *valoração* em K é uma função $\nu : K \to \mathbb{R} \cup \{\infty\}$ que satisfaz:

- Dado $x \in K$, tem-se $\nu(x) = \infty$ se e só se $x = 0$;
- $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ para quaisquer $x, y \in K$;
- $\nu(xy) = \nu(x) + \nu(y)$ para quaisquer $x, y \in K$.

Exemplo 3.1.2. A função $v_p : \mathbb{Q} \to \mathbb{R}$ (ou $\mathbb{Q}_p \to \mathbb{R}$) é uma valoração.

A definição anterior é muito semelhante à definição de valor absoluto não arquimediano. De facto, se $|\cdot|$ é um valor absolouto não arquimediano em K, então

$$\nu(x) = -\log(|x|)$$

define uma valoração em K. Reciprocamente, se ν é uma valoração em K, então

$$|x| = e^{-\nu(x)}$$

define um valor absoluto em K. No entanto, pensar em termos de valorações pode ser mais intuitivo do que pensar em termos de valores absolutos, dependendo do contexto.

Decorre da definição de valoração que, se $\nu : K \to \mathbb{R} \cup \{\infty\}$ é uma valoração, então a imagem $v(K^\times)$ é um subgrupo do grupo aditivo de $\mathbb{R}$ (pois ν define um homomorfismo de $K^\times$ em $(\mathbb{R}, +)$). Existem dois tipos de subgrupos de $\mathbb{R}$:

- Os subgrupos discretos, da forma $\alpha\mathbb{Z}$, com $\alpha \in \mathbb{R}_{\geq 0}$;
- Subgrupos densos em $\mathbb{R}$.

Estamos interessados em valorações cuja imagem é do primeiro tipo, e, portanto, vamos dar-lhes um nome.

Definição 3.1.3. Uma valoração $\nu : K \to \mathbb{R} \cup \{\infty\}$ diz-se *discreta* se $\nu(K^\times)$ é um subgrupo discreto de $\mathbb{R}$. A mesma valoração diz-se *normalizada* se $\nu(K^\times) = \mathbb{Z}$.

Definição 3.1.4. Um corpo valorado não arquimediano $(K, |\cdot|)$ diz-se *discreto* se $|\cdot|$ é não trivial e a valoração definida por $\nu(x) = -\log(|x|)$ é discreta.

Todos os corpos valorados a que nos vamos referir a partir de agora são não arquimedianos, portanto vamos omitir o termo "não arquimediano" nas referências a corpos valorados; supõe-se a partir de agora que qualquer corpo valorado é não arquimediano a não ser que seja explicitamente dito o contrário.

Dada uma valoração discreta ν, a sua imagem é $\alpha\mathbb{Z}$ para algum $\alpha \geq 0$; se $\alpha \neq 0$ definindo $\nu'(x) = \frac{1}{\alpha}\nu(x)$ obtemos uma nova valoração no mesmo corpo, que é normalizada. Assim, dado um corpo valorado discreto $(K, |\cdot|)$, podemos associar-lhe canonicamente uma valoração normalizada.

Exemplo 3.1.5. O corpo valorado $(\mathbb{Q}_p, |\cdot|_p)$ é discreto, e a valoração normalizada associada é v_p.

Definição 3.1.6. Seja $(K, |\cdot|)$ um corpo valorado discreto, com valoração normalizada correspondente ν. Um elemento $\pi \in K$ diz-se um *uniformizador* se $\nu(\pi) = 1$.

Exemplo 3.1.7. Em $\mathbb{Q}_p$, p é um uniformizador.

Definição 3.1.8. Seja $(K, |\cdot|)$ um corpo valorado discreto. O seu *anel de inteiros* $\mathcal{O}_K$ é definido por

$$\mathcal{O}_K = \{x \in K : |x| \leq 1\}.$$

Proposição 3.1.9. *Seja $(K, |\cdot|)$ um corpo valorado discreto com anel de inteiros $\mathcal{O}_K$. Então,*

(i) As unidades de $\mathcal{O}_K$ são os $x \in \mathcal{O}_K$ com $|x| = 1$;

(ii) Se π é um uniformizador de K, então os ideais de $\mathcal{O}_K$ são $\{0\}$ e os conjuntos da forma $\pi^n\mathcal{O}_K$, com n inteiro não negativo.

Demonstração. Este é um dos resultados que generalizam resultados que já conhecemos do caso p-ádico, mas em que a prova se mantém totalmente análoga. A prova fica, assim, como exercício para o leitor; é só repetir os argumentos utilizados para provar as Proposições 2.1.5 e 2.1.6, substituindo $\mathbb{Q}_p$ por K, $\mathbb{Z}_p$ por $\mathcal{O}_K$ e p por π. □

Corolário 3.1.10. *O anel $\mathcal{O}_K$ contém um único ideal maximal, $\mathfrak{m}_K = \pi\mathcal{O}_K$.*

Definição 3.1.11. Dado um corpo valorado discreto $(K, |\cdot|)$ com anel de inteiros $\mathcal{O}_K$ e ideal maximal $\mathfrak{m}_K$ de $\mathcal{O}_K$, definimos o *corpo residual*

$$k_K = \mathcal{O}_K/\mathfrak{m}_K.$$

Exemplo 3.1.12. O corpo residual de $\mathbb{Q}_p$ é $\mathbb{F}_p$.

Naturalmente, dizemos que um corpo valorado é *completo* se for completo em relação à topologia induzida pelo valor absoluto. Para corpos valorados discretos, a completude é uma propriedade muito agradável, entre outras razões porque é esta que nos permite deduzir o Lema de Hensel.

Lema 3.1.13 (Lema de Hensel, versão 1)**.** *Seja K um corpo valorado discreto completo e seja $f \in \mathcal{O}_K[X]$ um polinómio. Seja $\overline{f}$ o polinómio em $k_K[X]$ obtido reduzindo f módulo $\mathfrak{m}_K$ coeficiente a coeficiente. Suponha-se que existem polinómios ϕ_1 e ϕ_2 em $k_K[X]$, primos entre si, tais que*

$$\overline{f} = \phi_1\phi_2.$$

Então existem polinómios $f_1, f_2 \in \mathcal{O}_K[X]$ tais que $f_1 \equiv \phi_1 \pmod{p}$, $f_2 \equiv \phi_2 \pmod{p}$, $\deg(f_1) = \deg(\phi_1)$, e

$$f = f_1 f_2.$$

Lema 3.1.14 (Lema de Hensel, versão 2)**.** *Seja $f(X) \in \mathcal{O}_K[X]$ um polinómio. Suponha-se que o polinómio $\overline{f}(X) \in k_K[X]$ obtido reduzindo os coeficientes de f módulo $\mathfrak{m}_K$ tem uma raiz $a \in k_K$ que é uma* raiz simples*, ou seja, com multiplicidade* 1*. Então existe $\alpha \in \mathcal{O}_K$, com $\alpha \equiv a \pmod{\mathfrak{m}_K}$, tal que $f(\alpha) = 0$.*

Demonstração. Novamente, a prova destas duas versões do Lema de Hensel é inteiramente análoga às que demos no contexto de $\mathbb{Q}_p$, e essas podem ser adaptadas usando a mesma receita de sempre: substituir $\mathbb{Q}_p$ por K, $\mathbb{Z}_p$ por $\mathcal{O}_K$ e p por π (onde π é um uniformizador de K, de tal modo que $\mathfrak{m}_K = \pi\mathcal{O}_K$). □

Vamos também registar aqui uma consequência do Lema de Hensel que já vimos no contexto de $\mathbb{Q}_p$, e que nos vai ser útil.

Proposição 3.1.15. *Seja K um corpo valorado discreto completo, e seja $f(X) = a_n X^n + \cdots + a_0$ um polinómio em $K[X]$. Se f é irredutível, então o coeficiente de f com maior valor absoluto é a_n ou a_0.*

Demonstração. É análoga à da Proposição 2.2.3. □

§3.2. Extensões de valores absolutos

Se tudo o que vimos sobre $\mathbb{Q}_p$ se generaliza de maneira análoga para qualquer corpo valorado discreto completo, qual é o interesse de estudarmos esses corpos? A verdade é que, embora cada um desses corpos individualmente seja "parecido" com $\mathbb{Q}_p$, a maneira como esses corpos encaixam uns nos outros traz-nos algo de novo. De facto, é principalmente nesse encaixe que vamos estar interessados ao longo deste capítulo. O começo desta longa história está no resultado que se segue, que nos garante que qualquer extensão finita de um corpo valorado discreto completo é também um corpo valorado discreto completo.

Teorema 3.2.1. *Seja $(K, |\cdot|)$ um corpo valorado discreto completo, e seja $L : K$ uma extensão finita, de grau n (ver Definição A.0.1). Então o valor absoluto $|\cdot|$ pode ser estendido a L de maneira única, e L é completo em relação ao valor absoluto estendido. Essa única extensão é dada através da fórmula*

$$|x| = \sqrt[n]{|\mathrm{N}_{L/K}(x)|} \quad \textit{para todo o } x \in L$$

onde $\mathrm{N}_{L/K}$ designa a norma *associada à extensão $L : K$.*

Antes de avançarmos no sentido de uma prova deste teorema, vamos registar um corolário imediato.

Corolário 3.2.2. *Seja $(K, |\cdot|)$ um corpo valorado discreto completo, e seja $L : K$ uma extensão algébrica. Então o valor absoluto $|\cdot|$ pode ser estendido a L de maneira única.*

Demonstração. É uma consequência imediata do Teorema 3.2.1, juntamente com o facto de que

$$L = \bigcup_{\substack{L' \subseteq L \\ [L':K] < \infty}} L'.$$

□

Para provar o Teorema 3.2.1, precisamos de algum conhecimento sobre normas em espaços vetoriais sobre corpos como os que estamos a estudar.

Definição 3.2.3. Seja K um corpo valorado e seja V um espaço vetorial sobre K. Uma *norma* em V é uma função $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ com as seguintes propriedades:

- Dado $x \in V$, tem-se $\|x\| = 0$ se e só se $x = 0$;
- $\|\lambda x\| = |\lambda|\|x\|$ para qualquer $\lambda \in K$ e qualquer $x \in V$;
- $\|x + y\| \leq \|x\| + \|y\|$ para quaisquer $x, y \in V$.

Dada uma norma $\|\cdot\|$ em V, podemos definir uma métrica em V por $d(v, w) = \|v - w\|$.

Exemplo 3.2.4. Suponha-se que V tem dimensão finita sobre K, e seja $(e_1, \ldots, e_n)$ uma base. Então

$$\left\| \sum_{i=1}^{n} a_i e_i \right\| = \max\{|a_1|, \ldots, |a_n|\}$$

define uma norma em V. É fácil verificar que, se K é completo, então V é completo em relação a esta norma.

Definição 3.2.5. Duas normas $\|\cdot\|_1$ e $\|\cdot\|_2$ em V dizem-se *equivalentes* se existem constantes $C, D > 0$ tais que

$$\|x\|_2 \leq C\|x\|_1 \quad \text{e} \quad \|x\|_1 \leq D\|x\|_2$$

para qualquer $x \in V$.

É claro que duas normas equivalentes em V induzem a mesma topologia, e que V é completo em relação a uma norma se e só se for completo em relação à outra. O resultado principal para nós sobre equivalência de normas é o seguinte.

Proposição 3.2.6. *Suponha-se que o corpo valorado K é completo, e que V é um espaço vetorial de dimensão finita sobre K. Então quaisquer duas normas em V são equivalentes.*

Demonstração. □

Com isto estamos prontos para provar o Teorema 3.2.1.

Prova do Teorema 3.2.1. Seja $L : K$ uma extensão finita de grau n.

Comecemos por provar a unicidade da extensão do valor absoluto. Notemos que L é um espaço vetorial de dimensão finita sobre K, e qualquer extensão do valor absoluto $|\cdot|$ a L define uma norma em L. Sejam $|\cdot|_1$ e $|\cdot|_2$ duas extensões do valor absoluto $|\cdot|$ a L. Pela Proposição 3.3 esses dois valores absolutos induzem a mesma topologia em L. Então, pelo Lema 1.2.9, existe uma constante real $\alpha > 0$ tal que $|x|_2 = |x|_1^\alpha$ para todo o $x \in L$. Em particular isto é verdade para $x \in K$, caso em que $|x|_2 = |x|_1 = |x|$, e portanto $|x| = |x|^\alpha$. Como $|\cdot|$ é por hipótese não trivial existe $x \in K^\times$ tal que $|x| \neq 1$, e portanto $\alpha = 1$. Logo $|\cdot|_2 = |\cdot|_1$, e está provada a unicidade.

Passemos à existência. Observemos que para $x \in K$ se tem

$$\sqrt[n]{|\mathrm{N}_{L/K}(x)|} = \sqrt[n]{|x^n|} = |x|.$$

Portanto a fórmula

$$|x| = \sqrt[n]{|\mathrm{N}_{L/K}(x)|}$$

define uma extensão da função $|\cdot|$ a L. Falta verificar que esta extensão define um valor absoluto (não arquimediano).

Que $|x| = 0$ se e só se $x = 0$ é imediato, tendo em conta que $\mathrm{N}_{L/K}(x) = 0$ se e só se $x = 0$. A multiplicatividade do valor absoluto decorre da multiplicatividade da norma. Resta provar a desigualdade ultramétrica. Queremos provar que $|x+y| \leq \max\{|x|, |y|\}$ para quaisquer $x, y \in L$; se $x = 0$ ou $y = 0$ isto é imediato, logo suponhamos que tal não acontece, e suponhamos ainda sem perda de generalidade que $|x| \leq |y|$. Dividindo por $|y|$, a desigualdade a provar fica

$$\left|\frac{x}{y} + 1\right| \leq 1.$$

Basta assim provar que, se $|\alpha| \leq 1$, então $|\alpha + 1| \leq 1$; ou seja, que

$$|\mathrm{N}_{L/K}(\alpha)| \leq 1 \Rightarrow |\mathrm{N}_{L/K}(\alpha + 1)| \leq 1.$$

Isto resulta do lema que se segue, notando que se $P(X)$ é o polinómio mínimo (mónico) de α sobre K então o polinómio mínimo de $\alpha + 1$ é $P(X - 1)$. A completude de L resulta de que, vendo a extensão de $|\cdot|$ como uma norma em L, essa norma é equivalente à norma do Exemplo 3.2.4 pela Proposição 3.3, e L é completo em relação a essa norma. □

Lema 3.2.7. *Seja K um corpo valorado discreto completo e seja $L : K$ uma extensão finita. Seja $\alpha \in L$. Então as seguintes condições são equivalentes:*

(i) $|\mathrm{N}_{L/K}(\alpha)| \leq 1$*;*

(ii) O polinómio mínimo (mónico) de α sobre K tem coeficientes em $\mathcal{O}_K$.

Demonstração. Seja $n = [L : K]$. Provamos as duas implicações em separado:

- (i)⇒(ii): Seja
$$P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$$
o polinómio mínimo de α sobre K. Sendo um polinómio mínimo, $P(X)$ é irredutível. Além disso, resultados básicos sobre a norma associada a uma extensão finita dão-nos
$$\mathrm{N}_{L/K}(\alpha) = \pm a_0^{\frac{n}{d}}.$$
A hipótese de que $|\mathrm{N}_{L/K}(\alpha)| \leq 1$ dá-nos assim que $|a_0| \leq 1$. Mas a Proposição 3.1.15 diz-nos que o coeficiente de $P(X)$ com maior valor absoluto é 1 ou a_0. Decorre assim que $|a_k| \leq 1$ para todo o k, ou seja, $a_k \in \mathcal{O}_K$.

- (ii)⇒(i): Novamente utilizamos que
$$\mathrm{N}_{L/K}(\alpha) = \pm a_0^{\frac{n}{d}},$$
e a hipótese de que todos os coeficientes de $P(X)$ (em particular, a_0) pertencem a $\mathcal{O}_K$ implica $|a_0| \leq 1$, logo $|\mathrm{N}_{L/K}(\alpha)| \leq 1$, como pretendido.

□

§3.3. Ramificação e inércia

Vamos restringir um pouco a classe de corpos com que estamos a trabalhar, passando a aceitar apenas aqueles que têm corpo residual finito.

Definição 3.3.1 (Corpo local)**.** Um *corpo local* é um corpo valorado discreto completo com corpo residual finito.

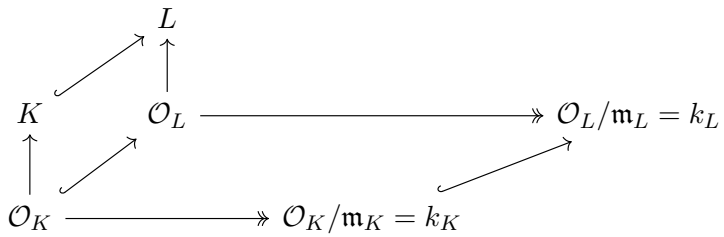
Observação 3.3.2. Existem outras definições na literatura (que produzem classes de corpos ligeiramente diferentes). Por exemplo, é comum exigir apenas que o corpo residual seja *perfeito* de característica finita, não necessariamente finito. Uma outra definição comum é a seguinte: um corpo local é um corpo localmente compacto em relação a uma topologia não discreta. A única diferença em relação à nossa definição é que esta abrange os corpos $\mathbb{R}$ e $\mathbb{C}$, enquanto a nossa não.

Exemplo 3.3.3. O exemplo prototípico de um corpo local é, naturalmente, $\mathbb{Q}_p$.

Seja $(K, |\cdot|)$ um corpo local, e seja $L : K$ uma extensão finita, que é, como sabemos, um corpo valorado discreto completo (Teorema 3.2.1). Tendo em conta a definição do anel de inteiros, é claro que $\mathcal{O}_K \subseteq \mathcal{O}_L$, e ainda que $\mathfrak{m}_K \subseteq \mathfrak{m}_L$. De facto, temos algo mais forte:

$$\mathfrak{m}_K = \mathcal{O}_K \cap \mathfrak{m}_L.$$

(É uma consequência do facto de que $\mathfrak{m}_K = \{x \in \mathcal{O}_K : |x| < 1\}$ e $\mathfrak{m}_L = \{x \in \mathcal{O}_L : |x| < 1\}$.) Isto diz-nos que a inclusão $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ induz um homomorfismo injetivo $\mathcal{O}_K/\mathfrak{m}_K \hookrightarrow \mathcal{O}_L/\mathfrak{m}_L$, ou seja, $k_K \hookrightarrow k_L$. Portanto o corpo residual k_L é uma extensão do corpo residual k_K.



Podemos ver que a extensão $k_L : k_K$ é uma extensão *finita*, e até que $[k_L : k_K] \leq [L : K]$. Para isso, seja $n = [L : K]$, e sejam $\overline{x_0}, \ldots, \overline{x_n}$ quaisquer $n + 1$ elementos de k_L. Queremos ver que são linearmente dependentes sobre k_K. Considerem-se $x_0, \ldots, x_n \in \mathcal{O}_L$ cujas projeções em k_K sejam iguais a $\overline{x_0}, \ldots, \overline{x_n}$. Como L tem dimensão n enquanto espaço vetorial sobre K, existem $a_0, \ldots, a_n \in K$, nem todos iguais a 0, tais que

$$a_0 x_0 + \cdots + a_n x_n = 0. \tag{3.1}$$

A ideia natural agora é reduzir esta igualdade módulo $\mathfrak{m}_L$ de modo a obter uma dependência linear entre $\overline{x_0}, \ldots, \overline{x_n}$ em k_L. No entanto, nada nos garante que $a_0, \ldots, a_n$ estão todos em $\mathcal{O}_L$ (ou $\mathcal{O}_K$), e, mesmo que estejam, não temos a garantia de que as projeções em k_K não são todas iguais a 0. Para remediar isso, seja π um uniformizador de K e escrevemos $a_i = \pi^{\nu_i} u_i$ para cada i, onde $u_0, \ldots, u_n$ são unidades e $\nu_0, \ldots, \nu_n$ são inteiros. Sem perda de generalidade, suponha-se que ν_i é mínimo quando $i = 0$. Dividindo a igualdade (3.1) por π^{ν_0}, obtemos

$$b_0 x_0 + \cdots + b_n x_n = 0$$

onde $b_i = \pi^{\nu_i - \nu_0} u_i$ para cada i. Desta forma, todos os b_i pertencem a $\mathcal{O}_K$ e b_0 não pertence a $\mathfrak{m}_K$, de modo que a projeção de b_0 módulo $\mathfrak{m}_K$ é diferente de 0. Denotando por $\overline{b_0}, \ldots, \overline{b_n}$ as projeções de $b_0, \ldots, b_n$ em k_K, obtemos

$$\overline{b_0}\overline{x_0} + \cdots + \overline{b_n}\overline{x_n} = 0.$$

Como $\overline{b_0} \neq 0$, conclui-se que $\overline{x_0}, \ldots, \overline{x_n}$ são linearmente dependentes. Portanto $[k_L : k_K] \leq n$.

Como k_K é um corpo finito, conclui-se que k_L também é um corpo finito, e portanto qualquer extensão finita de um corpo local é também um corpo local. Vamos dar um nome ao grau (finito) desta extensão de corpos finitos que estudámos atrás.

Definição 3.3.4 (Número de inércia)**.** Seja $L : K$ uma extensão finita de corpos locais. O *número de inércia* da extensão é

$$f(L/K) = [k_L : k_K].$$

Do Facto A.0.3 resulta imediatamente o seguinte:

Proposição 3.3.5. *Sejam $L : K$ e $M : L$ extensões finitas de corpos locais. Então*

$$f(M/K) = f(L/K)f(M/L).$$

Existe (pelo menos) um outro invariante importante associado a uma extensão finita $L : K$ de corpos locais, o chamado *índice de ramificação*. Este essencialmente mede quão maior é a imagem do valor absoluto $|\cdot|$ a partir de L do que a mesma imagem a partir de K. Considere-se uma valoração ν em L associada ao valor absoluto $|\cdot|$. Então $\nu(K^\times) = \alpha\mathbb{Z}$ para algum $\alpha > 0$. O índice de ramificação e é o único inteiro positivo e tal que $\nu(L^\times) = \frac{\alpha}{e}\mathbb{Z}$. Uma maneira equivalente de o definir é a seguinte.

Definição 3.3.6 (Índice de ramificação)**.** Seja $L : K$ uma extensão finita de corpos locais, seja π_K um uniformizador de K e seja ν a valoração normalizada em L. O *índice de ramificação* da extensão é

$$e(L/K) = \nu(\pi_K).$$

(É fácil ver que isto não depende da escolha de π_K.)

Tal como o número de inércia, o índice de ramificação é multiplicativo em torres:

Proposição 3.3.7. *Sejam $L : K$ e $M : L$ extensões finitas de corpos locais. Então*

$$e(M/K) = e(L/K)e(M/L).$$

Demonstração. Sejam π_K, π_L, π_M uniformizadores de K, L e M respetivamente. Então $\pi_K = u\pi_L^{e(L/K)}$ para alguma unidade u, e $\pi_L = u'\pi_M^{e(M/L)}$, de modo que

$$\pi_K = uu'^{e(M/L)}\pi_M^{e(L/K)e(M/L)}.$$

Portanto se ν é a valoração normalizada em M tem-se $\nu(\pi_K) = e(L/K)e(M/L)$, que equivale ao pretendido. □

Resulta da Proposição 3.3.5 e da Proposição 3.3.7 que o número $e(L/K)f(L/K)$ também é multiplicativo em torres. Curiosamente, este produto não é nada mais nada menos do que o grau da extensão! É este o resultado fundamental que relaciona os números $e(L/K)$ e $f(L/K)$, o famoso "Teorema $n = ef$".

Teorema 3.3.8. *Seja $L : K$ uma extensão finita de corpos locais. Então*

$$[L : K] = e(L/K)f(L/K).$$

Demonstração. Vamos abreviar $e(L/K)$ e $f(L/K)$ por e e f, de tal modo que queremos provar que $[L : K] = ef$. Seja π um uniformizador de L, de tal modo que, para alguma unidade u, $\pi^e u = \pi_K$ é um uniformizador de K. Note-se ainda que, sendo $\overline{\alpha}$ um gerador do grupo multiplicativo $k_L^\times$, se tem $k_L = k_K(\overline{\alpha})$. Observe-se que então o polinómio mínimo de $\overline{\alpha}$ sobre k_K tem grau f, e $(1, \overline{\alpha}, \ldots, \overline{\alpha}^{f-1})$ é uma base de k_L sobre k_K. Escolhemos $\alpha \in \mathcal{O}_L$ de tal modo que a projeção de α em k_L é igual a α. Afirmamos que os elementos

$$\alpha^i \pi^j, \quad 0 \leq i \leq f-1,\, 0 \leq j \leq e-1$$

de L formam uma base de L sobre K. Como são ef elementos, isto prova o resultado.

Começamos por provar que são linearmente independentes. Para isso sejam $(c_{i,j})_{i=0,\ldots,f-1}^{j=0,\ldots,e-1}$ elementos de K, não todos nulos, tais que

$$\sum_{i,j} c_{i,j} \alpha^i \pi^j = 0.$$

Multiplicando todos os $c_{i,j}$ por uma potência apropriada de π_K, podemos supor que $c_{i,j} \in \mathcal{O}_K$ para quaisquer i e j, e ainda que nem todos os coeficientes $c_{i,j}$ são divisíveis por π_K. Seja j_0 o menor índice tal que, para algum índice i_0, se tem $\pi_K \nmid c_{i_0,j_0}$. Para cada j, seja $s_j = \sum_{i=0}^{f-1} c_{i,j}\alpha^i$ Então,

- Para $j < j_0$, a soma s_j é divisível por $\pi_K = \pi^e u$ (já que, pela minimalidade de j_0, todos os coeficientes $c_{i,j}$ com $j < j_0$ o são), e em particular por π^{j_0+1};
- Para $j > j_0$, tem-se $\pi^{j_0+1} \mid s_j \pi^j$.

Mas temos

$$\sum_{j=0}^{e-1} s_j \pi^j = 0$$

e todas as parcelas da soma acima com $j \neq j_0$ são portanto divisíveis por π^{j_0+1}. Resulta que

$$\pi^{j_0+1} \mid s_{j_0} \pi^{j_0}, \quad \text{ou seja,} \quad \pi \mid s_{j_0}.$$

Isso significa que a soma $s_{j,0} = c_{0,j_0} + c_{1,j_0}\alpha + \cdots + c_{f-1,j_0}\alpha^{f-1}$ pertence a $\mathfrak{m}_L$, e a sua projeção em k_L é igual a 0. Utilizando a barra superior para denotar redução módulo $\mathfrak{m}_L$,

$$\overline{c_{0,j_0}} + \overline{c_{1,j_0}}\,\overline{\alpha} + \cdots + \overline{c_{f-1,j_0}}\,\overline{\alpha}^{f-1} = 0.$$

Como $(1, \overline{\alpha}, \ldots, \overline{\alpha}^{f-1})$ é uma base de k_L sobre k_K, conclui-se que

$$\overline{c_{0,j_0}} = \overline{c_{1,j_0}} = \cdots = \overline{c_{f-1,j_0}} = 0.$$

Portanto todos os coeficientes c_{i,j_0} são divisíveis por π_K, o que contradiz a escolha de j_0.

Resta provar que os $\alpha^i \pi^j$ considerados atrás geram L. Seja

$$M = \bigoplus_{i,j} \mathcal{O}_K \cdot \alpha^i \pi^j = \left\{ \sum c_{i,j} \alpha^i \pi^j : c_{i,j} \in \mathcal{O}_K \right\}.$$

Basta provar que $M = \mathcal{O}_L$. De facto, dado $x \in L$, temos $x\pi_K^m \in \mathcal{O}_L$ para m suficientemente grande, de onde decorrerá que $x\pi_K^m$ se pode escrever como combinação linear dos $\alpha^i\pi^j$ com coeficientes em K, pelo que x também pode.

Afirmamos inicialmente que M é fechado em L. Para isso, consideramos uma base $(v_1, \ldots, v_n)$ de L como espaço vetorial sobre K, tal que $v_1, \ldots, v_{ef}$ são os $\alpha^i\pi^j$ por alguma ordem. (Isto é possível porque já vimos que os $\alpha^i\pi^j$ são linearmente independentes.) Considere-se a norma $\|\cdot\|$ do Exemplo 3.2.4 associada a esta base de L, e note-se que esta norma define a topologia que estamos a considerar em L, pois pela Proposição essa norma é equivalente em L ao valor absoluto $|\cdot|$. A topologia induzida por $\|\cdot\|$ em L é obtida por transporte da topologia produto em K^n para L através da bijeção

$$(a_1, \ldots, a_n) \mapsto a_1v_1 + \cdots + a_nv_n.$$

A imagem recíproca de M através desta bijeção é

$$\underbrace{\mathcal{O}_K \times \cdots \times \mathcal{O}_K}_{ef \text{ vezes}} \times \underbrace{\{0\} \times \cdots \times \{0\}}_{n-ef \text{ vezes}}$$

e portanto é um produto de fechados, sendo também fechado. Logo M é fechado em L.

Seja agora

$$N = \bigoplus_{i=0}^{f-1} \mathcal{O}_K \cdot \alpha^i.$$

É imediato a partir da definição de M que

$$M = N + \pi N + \cdots + \pi^{e-1}N. \tag{3.2}$$

Por outro lado, também se tem $\mathcal{O}_L = N + \pi\mathcal{O}_L$: de facto, se $x \in \mathcal{O}_L$, então a redução de x módulo π_K é uma combinação linear dos α^i com coeficientes em k_K, ou seja, temos

$$x \equiv c_0 + c_1\alpha + \cdots + c_{f-1}\alpha^{f-1} \pmod{\pi}$$

para alguns $c_0, \ldots, c_{f-1} \in \mathcal{O}_K$, o que significa precisamente que x é a soma de um elemento de N com um elemento de $\pi\mathcal{O}_L$. Usando a igualdade $\mathcal{O}_L = N + \pi\mathcal{O}_L$ iterativamente, obtemos

$$\begin{aligned}
\mathcal{O}_L &= N + \pi\mathcal{O}_L \\
&= N + \pi(N + \pi\mathcal{O}_L) = N + \pi N + \pi^2\mathcal{O}_L \\
&= \cdots \\
&= N + \pi N + \pi^2 N + \cdots + \pi^{e-1}N + \pi^e\mathcal{O}_L.
\end{aligned}$$

Usando (3.2) e o facto de que $\pi^e\mathcal{O}_L = \pi_K\mathcal{O}_L$, isto dá-nos

$$\mathcal{O}_L = M + \pi_K\mathcal{O}_L.$$

Repetindo o truque iterativo anterior, obtemos

$$\begin{aligned}
\mathcal{O}_L &= M + \pi_K\mathcal{O}_L \\
&= M + \pi_K(M + \pi_K\mathcal{O}_L) = M + \pi_K M + \pi_K^2\mathcal{O}_L = M + \pi_K^2\mathcal{O}_L \\
&= \cdots \\
&= M + \pi_K^m\mathcal{O}_L
\end{aligned}$$

para qualquer inteiro $m \geq 0$. Por outras palavras, para qualquer $x \in \mathcal{O}_L$, existe $a \in M$ tal que

$$|x - a| \leq |\pi|^{-m}.$$

Logo M é denso em $\mathcal{O}_L$. Como M é fechado, conclui-se que $M = \mathcal{O}_L$, como pretendido. □

Exemplo 3.3.9. Vamos determinar o índice de ramificação e o número de inércia num caso concreto. Considere-se a extensão $L = \mathbb{Q}_3(\zeta_8, \sqrt{3})$ de $\mathbb{Q}_3$, onde ζ_8 é uma raiz oitava primitiva da unidade.

Observe-se que ζ_8 é uma raiz do polinómio $X^4 + 1$, mas isto não determina o polinómio mínimo de ζ_8 sobre $\mathbb{Q}_3$ porque $X^4 + 1$ não é irredutível em $\mathbb{Q}_3[X]$. De facto, temos

$$X^4 + 1 \equiv (X^2 - 2X + 2)(X^2 + 2X + 2) \pmod 3$$

e portanto, pelo Lema de Hensel, $X^4 + 1$ fatoriza em $\mathbb{Q}_3[X]$ como produto de dois polinómios de grau 2 (que são irredutíveis, pois $X^2 - 2X + 2$ e $X^2 + 2X + 2$ são-no em $\mathbb{F}_3[X]$).

Portanto $[\mathbb{Q}_3(\zeta_8) : \mathbb{Q}_3] = 2$. Por outro lado, é evidente que $[\mathbb{Q}_3(\zeta_8, \sqrt{3}) : \mathbb{Q}_3(\zeta_8)] \leq 2$. Portanto $[L : \mathbb{Q}_3] \leq 4$.

Vamos agora olhar para o número de inércia; em L temos uma solução da equação $x^4 + 1 = 0$, que está necessariamente em $\mathcal{O}_L$ (porquê?). Portanto também existe uma solução dessa equação em k_L. Mas em $k_{\mathbb{Q}_3} = \mathbb{F}_3$ não existe uma solução dessa equação. Logo k_L é estritamente maior do que $\mathbb{F}_3$. Resulta que $f(L/\mathbb{Q}_3) \geq 2$.

Por fim, observe-se que 3 é um uniformizador em $\mathbb{Q}_3$, mas 3 é um quadrado em L, portanto o índice de ramificação $e(L/\mathbb{Q}_3)$ também é maior ou igual a 2. Juntando tudo, obtemos

$$4 \geq [L : \mathbb{Q}_3] = e(L/\mathbb{Q}_3) f(L/\mathbb{Q}_3) \geq 2 \cdot 2 = 4.$$

Portanto todas as desigualdades intermédias são igualdades. Conclui-se que $e(L/\mathbb{Q}_3) = 2$ e $f(L/\mathbb{Q}_3) = 2$ (e $[L : \mathbb{Q}_3] = 4$).

O Teorema 3.3.8 diz-nos essencialmente que, quando construimos uma extensão de um corpo local com um certo grau, podemos "distribuir" o grau pela ramificação e pela inércia, e se quisermos mais ramificação vamos obter menos inércia e vice-versa. Vamos dar um nome especial às duas situações extremas que podem aparecer.

Definição 3.3.10. Uma extensão de corpos locais $L : K$ diz-se *não ramificada* se $e(L/K) = 1$ (e portanto $f(L/K) = [L : K]$).

Definição 3.3.11. Uma extensão de corpos locais $L : K$ diz-se *totalmente ramificada* se $f(L/K) = 1$ (e portanto $e(L/K) = [L : K]$).

Vamos ver em breve que, se $L : K$ é uma extensão arbitrária de corpos locais, então existe um corpo intermédio M tal que $M : K$ é uma extensão não ramificada e $L : M$ é uma extensão totalmente ramificada. Isso, em certa medida, reduz o estudo das extensões de corpos locais ao estudo separado das extensões não ramificadas e das extensões totalmente ramificadas.

§3.4. Extensões não ramificadas

A teoria das extensões não ramificadas de um corpo local K é particularmente simples: estas estão em correspondência natural com as extensões do corpo residual k_K.

Lema 3.4.1. *Seja K um corpo local. Para qualquer extensão finita $\ell : k_K$ do corpo residual, existe uma única extensão finita não ramificada $L : K$ tal que $k_L = \ell$.*

Demonstração. Como k_K e ℓ são corpos finitos, existe $\overline{\alpha} \in \ell$ tal que $\ell = k_K(\alpha)$. Seja $\overline{f}$ o polinómio mínimo de $\overline{\alpha}$, e seja f um polinómio mónico do mesmo grau em $\mathcal{O}_K[X]$ cuja redução módulo $\mathfrak{m}_K$ é igual a $\overline{f}$. Como $\overline{f}$ é irredutível, f também o é.

Seja $L = K(\theta)$, onde θ é uma raiz de f. Observe-se que θ pertence a $\mathcal{O}_L$ (de facto, qualquer raiz em L de um polinómio mónico com coeficientes em K pertence a $\mathcal{O}_L$; porquê?). Além disso,

$$[L : K] = \deg(f) = \deg(\overline{f}) = [\ell : k_K].$$

Por outro lado, como k_L contém uma raiz de $\overline{f}$ (a redução de θ módulo $\mathfrak{m}_L$), existe um mergulho de ℓ em k_L. Logo,

$$[\ell : k_K] \leq [k_L : k_K]. \tag{3.3}$$

Conclui-se que $[L : K] = [k_L : k_K]$ e portanto, pelo Teorema 3.3.8, devemos ter $e(L/K) = 1$, ou seja, $L : K$ é uma extensão não ramificada. Além disso, isto força a que haja igualdade em (3.3), logo $k_L = \ell$.

Resta provar a unicidade de L. Seja $L : K$ uma extensão não ramificada com $k_L = \ell$. Como $\overline{f}$ é um polinómio irredutível com coeficientes num corpo finito, a raiz $\overline{\alpha} \in \ell = k_L$ é uma raiz simples, e portanto, pelo Lema de Hensel, existe uma raiz $\alpha \in \mathcal{O}_L$ de f que se reduz a $\overline{\alpha}$ módulo $\mathfrak{m}_L$. Então $K(\alpha) \in L$. Mas, pelo que vimos antes, $K(\alpha) : K$ é uma extensão não ramificada e o corpo residual de $K(\alpha)$ é ℓ. Além disso, $[K(\alpha) : K] = [\ell : k_K] = [L : K]$. Portanto $L = K(\alpha)$, e isto mostra a unicidade de L. □

Observação 3.4.2. O lema anterior permite-nos traduzir muito do nosso conhecimento sobre corpos finitos para resultados sobre extensões não ramificadas de corpos locais. Por exemplo, do Corolário A.0.17 resulta, juntamente com o Lema 3.4.1, que qualquer corpo local K tem exatamente uma extensão não ramificada de grau n, para cada n.

Exemplo 3.4.3. A prova do Lema 3.4.1 dá-nos uma "receita" para, dada uma extensão finita $\ell : k_K$ do corpo residual, construir a extensão não ramificada $L : K$ que a induz: escrevemos $\ell = k_K(\overline{\alpha})$ e acrescentamos a K uma raiz de um levantamento em $\mathcal{O}_K[X]$ do polinómio mínimo de $\overline{\alpha}$ sobre k_K. Vamos ver um exemplo: qual é a (única) extensão quadrática não ramificada de $\mathbb{Q}_2$? A única extensão quadrática de $\mathbb{F}_2$ é $\mathbb{F}_4 = \mathbb{F}_2(\beta)$ onde $\beta^2 + \beta + 1 = 0$. Um polinómio em $\mathbb{Z}_2[X]$ que se reduz a $X^2 + X + 1$ módulo 2 é $X^2 - X - 1$, cujas raízes são $\frac{1\pm\sqrt{5}}{2}$. Portanto a única extensão quadrática não ramificada de $\mathbb{Q}_2$ é $\mathbb{Q}_2(\sqrt{5})$.

Vamos agora provar que qualquer extensão finita de corpos locais se pode "decompor" numa extensão não ramificada e numa extensão totalmente ramificada.

Lema 3.4.4. *Seja $L : K$ uma extensão finita de corpos locais, com índice de ramificação e e número de inércia f. Então existe um corpo intermédio M tal que*

- *$M : K$ é uma extensão não ramificada, com $[M : K] = f$;*

- *$L : M$ é uma extensão totalmente ramificada, com $[L : M] = e$.*

Demonstração. Como vimos atrás, a única extensão não ramificada de K que induz a extensão residual $k_L : k_K$ é da forma $K(\alpha)$, onde o polinómio mínimo f de α sobre K tem coeficientes em $\mathcal{O}_K$, e a projeção $\overline{\alpha}$ de α em $\mathcal{O}_L$ (que tem $\overline{f}$ como polinómio mínimo) é tal que $k_L = k_K(\overline{\alpha})$. Como $\overline{\alpha}$ é uma raiz simples de $\overline{f}$, pelo Lema de Hensel f tem uma raiz em L. Ou seja, o corpo $K(\alpha)$ referido atrás mergulha em L; seja M a imagem desse mergulho.

Por construção, M é uma extensão não ramificada de K contida em L tal que $[M : K] = [k_L : k_K] = f$. Por outro lado, temos

$$ef = [L : K] = [L : M][M : K] = [L : M]f,$$

pelo que $[L : M] = e$. Por fim, pela Proposição 3.3.5,

$$f = f(L/K) = f(L/M)f(M/K) = f(L/M)f$$

e portanto $f(L/M) = 1$ e $L : M$ é uma extensão totalmente ramificada, como pretendido. □

Exemplo 3.4.5. A extensão $\mathbb{Q}_3(\zeta_8, \sqrt{3})$ do Exemplo 3.3.9 admite a decomposição

$$\mathbb{Q}_3(\zeta_8, \sqrt{3}) : \mathbb{Q}_3(\zeta_8) : \mathbb{Q}_3$$

onde $\mathbb{Q}_3(\zeta_8) : \mathbb{Q}_3$ é não ramificada e $\mathbb{Q}_3(\zeta_8, \sqrt{3}) : \mathbb{Q}_3(\zeta_8)$ é totalmente ramificada.

§3.5. Extensões totalmente ramificadas

A teoria das extensões totalmente ramificadas tem uma faceta inesperada, que é o papel inesperado que nela têm os *polinómios de Eisenstein*, os polinómios que satisfazem as condições do célebre critério de irredutibilidade de Eisenstein. Vamos começar por transcrever essas condições para a linguagem dos corpos locais.

Definição 3.5.1 (Polinómios de Eisenstein)**.** Seja K um corpo local com valoração normalizada ν. Um polinómio

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$$

diz-se um *polinómio de Eisenstein* se verifica as seguintes condições:

- $\nu(a_{n-1}), \ldots, \nu(a_0)$ são todos maiores do que 0 (ou seja, $a_{n-1}, \ldots, a_0 \in \mathfrak{m}_K$);
- $\nu(a_0) = 1$.

Observação 3.5.2. Se $K = \mathbb{Q}_p$, o que as condições anteriores dizem é que $a_{n-1}, \ldots, a_0$ são inteiros p-ádicos e p divide $a_{n-1}, \ldots, a_0$, mas p^2 não divide a_0. Estas são precisamente as condições que aparecem no critério de Eisenstein clássico.

Lema 3.5.3 (Critério de Eisenstein)**.** *Qualquer polinómio de Eisenstein é irredutível.*

Demonstração. Seja $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ um polinómio de Eisenstein em $K[X]$, e suponha-se por absurdo que f não é irredutível, de tal modo que $f = gh$ com g e h polinómios de grau maior do que 0. Sem perda de generalidade podemos supor que g e h são mónicos. Afirmamos inicialmente que $g, h \in \mathcal{O}_K[X]$. Se isto não acontece, podemos escrever

$$g(X) = \frac{g'(X)}{\pi^a}, \quad h(X) = \frac{h'(X)}{\pi^b}$$

onde π é um uniformizador de K e a e b são inteiros não negativos e $a + b > 0$, onde $g'(X)$ e $h'(X)$ pertencem a $\mathcal{O}_K[X]$ e não são divisíveis por π. Então

$$\frac{g'(X)h'(X)}{\pi^{a+b}} = f(X) \in \mathcal{O}_K[X].$$

Logo π divide $g'(X)h'(X)$. Reduzindo módulo π, obtemos que $f'(X)g'(X) = 0$ em $k_K[X]$. Como $k_K[X]$ é um domínio de integridade conclui-se que um dos polinómios $g'(X)$ e $h'(X)$ é 0 em $k_K[X]$. Logo π divide $g'(X)$ ou $h'(X)$, uma contradição.

Assim g e h estão em $\mathcal{O}_K[X]$. Reduzindo a igualdade $f(X) = g(X)h(X)$ módulo π, chegamos a

$$X^n = g(X)h(X) \text{ em } k_K[X].$$

Como $k_K[X]$ é um domínio de fatorização única, conclui-se que $g(X) = X^s$ e $h(X) = X^t$ em $k_K[X]$, para alguns $s, t > 0$. Sejam b_0 e c_0 os coeficientes constantes de $g(X)$ e $h(X)$, respetivamente. A conclusão anterior mostra que $\nu(b_0), \nu(c_0) \geq 1$. Mas então

$$\nu(a_0) = \nu(b_0c_0) \geq 2,$$

uma contradição. Portanto f é irredutível. □

A relação dos polinómios de Eisenstein com extensões totalmente ramificadas vem do seguinte resultado.

Lema 3.5.4. *Seja K um corpo local. Então,*

(i) Se $L : K$ é uma extensão finita totalmente ramificada e π é um uniformizador de L, então $L = K(\pi)$ e o polinómio mínimo de π sobre K é um polinómio de Eisenstein.

(ii) Se $f \in K[X]$ é um polinómio de Eisenstein e π é uma raiz de f, então $K(\pi)$ é uma extensão totalmente ramificada de K com uniformizador π.

Demonstração. Começamos por (i). Na prova do Teorema 3.3.8 vimos que todo o elemento de L se pode escrever como combinação linear de termos da forma $\alpha^i\pi^j$ (com $0 \leq i \leq f-1$ e $0 \leq j \leq e-1$), onde α é um elemento de $\mathcal{O}_L$ que se reduz a um elemento primitivo de k_L sobre k_K. Se $L : K$ é totalmente ramificada então $f = 1$ e portanto todo o elemento de L se pode escrever como combinação linear de potências de π. Logo $L = K(\pi)$.

Seja

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

o polinómio mínimo de π sobre K. Designemos por ν_K e ν_L as valorações normalizadas em K e L, respetivamente. Note-se que, como a extensão é totalmente ramificada, temos $\nu_L(x) = n\nu_K(x)$ para $x \in K$. O facto de se ter $f(\pi) = 0$ diz-nos que

$$\pi^n = -a_{n-1}\pi^{n-1} - \cdots - a_0.$$

Conclui-se que

$$n = \nu(\pi^n) \geq \min\{\nu_L(a_{n-1}\pi^{n-1}), \ldots, \nu_L(a_0)\}.$$

Além disso, há igualdade se estas valorações forem todas diferentes. Vamos ver que é o caso. Temos

$$\nu_L(a_k\pi^k) = \nu_L(a_k) + k \equiv k \pmod{n},$$

uma vez que $\nu_L(a_k) = n\nu_K(a_k)$. Como k varia entre 0 e $n-1$ conclui-se que os números $\nu(a_k\pi^k)$ são de facto todos diferentes.

Portanto,

$$n = \min_{k=0,\ldots,n-1}\{\nu_L(a_k\pi^k)\} = \min_{k=0,\ldots,n-1}\{\nu_L(a_k) + k\}. \tag{3.4}$$

Daqui resulta que:

- Por um lado, temos $\nu_L(a_k) + k \geq n$ para $k = 0, \ldots, n-1$. Isto implica que $\nu_L(a_k) > 0$ para $k = 0, \ldots, n-1$.
- Mas, como $\nu_L(a_k)$ é divisível por n, isto diz-nos que $\nu_L(a_k) + k \geq n + k > n$ para $k > 0$. Como, para se ter (3.4), devemos ter $\nu_L(a_k) + k = n$ para algum $k \in \{0, \ldots, n-1\}$, esse k tem que ser 0, e $\nu_L(a_0) = n$. Portanto $\nu_K(a_0) = 1$.

Estas duas conclusões implicam que f seja um polinómio de Eisenstein, como pretendido.

Passemos a (ii). Vamos começar por provar que, sob as condições de (ii), $L : K$ é uma extensão totalmente ramificada. Para isso, utilizamos o Lema 3.4.4, que nos dá um corpo intermédio M tal que $M : K$ é uma extensão não ramificada e $L : M$ é totalmente ramificada.

Como $M : K$ é uma extensão não ramificada, a valoração normalizada em M estende a valoração normalizada em K, e portanto o polinómio f também é um polinómio de Eisenstein em $M[X]$. Logo, pelo Critério de Eisenstein (Lema 3.5.3), f é irredutível em $M[X]$. Por outro lado, obviamente temos $K = M(\pi)$, e portanto

$$[L : M] = [M(\pi) : M] = \deg(f) = [K(\pi) : K] = [L : K] = [L : M] \cdot [M : K].$$

Resulta que $[M : K] = 1$, e portanto $M = K$. Isto implica que $L : K$ é totalmente ramificada.

Falta provar que π é um uniformizador de L. Seja $n = [L : K]$, e seja

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0.$$

Sejam novamente ν_K e ν_L as valorações normalizadas em K e L, respetivamente. Notemos inicialmente que $\nu(\pi) > 0$; caso contrário, na soma $0 = \pi^n + a_{n-1}\pi^{n-1} + \cdots + a_0$ todos os termos $a_{n-1}\pi^{n-1}, \ldots, a_0$ têm valoração positiva (recorde-se que f é de Eisenstein) mas π^n não tem, contradição. Por outro lado, temos

$$a_0 = -\pi^n - a_{n-1}\pi^{n-1} - \cdots - a_1\pi$$

e além disso $\nu_L(a_0) = n$, já que $\nu_K(a_0) = 1$; assim,

$$n \geq \min\{n\nu_L(\pi), (n-1)\nu_L(\pi) + \nu_L(a_{n-1}), \ldots, \nu_L(\pi) + \nu_L(a_1)\}. \tag{3.5}$$

Mas para $k = 1, \ldots, n-1$ tem-se

$$k\nu_L(\pi) + \nu_L(a_k) > \nu_L(a_k) = n\nu_K(a_k) \geq n.$$

Portanto, para 3.5 se verificar, devemos ter $n \geq n\nu_L(\pi)$, e $\nu_L(\pi) \leq 1$. Como já tínhamos $\nu_L(\pi) \geq 1$, obtemos $\nu_L(\pi) = 1$, e portanto π é um uniformizador de L, como pretendido. □

Observação 3.5.5. O Lema anterior diz-nos que qualquer extensão totalmente ramificada de um corpo local se pode obter acresentando uma raiz de um polinómio de Eisenstein, mas *não* implica que se $L = K(\alpha) : K$ é uma extensão totalmente ramificada então o polinómio mínimo de α sobre K é um polinómio de Eisenstein; isso só é necessariamente verdade se α for um uniformizador de L. Por exemplo, considere-se a extensão $\mathbb{Q}_2(\sqrt{3}) : \mathbb{Q}_2$: esta é uma extensão totalmente ramificada, e no entanto o polinómio mínimo de $\sqrt{3}$ sobre $\mathbb{Q}_2$, que é $X^2 - 3$, *não* é de Eisenstein. Mas também temos $\mathbb{Q}_2(\sqrt{3}) = \mathbb{Q}_2(1 + \sqrt{3})$, e o polinómio mínimo de $1 + \sqrt{3}$ sobre $\mathbb{Q}_2$ é $X^2 - 2X - 2$, que é de Eisenstein; de facto, $1 + \sqrt{3}$ é um uniformizador de $\mathbb{Q}_2(\sqrt{3})$.

Observação 3.5.6. Embora seja verdade que qualquer extensão totalmente ramificada de um corpo local K é obtida acrescentando a K uma raiz de um polinómio de Eisenstein, esse polinómio está longe de ser único; vários polinómios de Eisenstein podem dar origem à mesma extensão, e não se conhece uma maneira "canónica" de associar a uma extensão totalmente ramificada um polinómio de Eisenstein "especial" que lhe dá origem.

§3.6. Teoria de Galois de corpos locais

Talvez o leitor esteja familiarizado com o *problema inverso de Galois*: este consiste em saber se, para qualquer grupo finito G, existe uma extensão finita $F : \mathbb{Q}$ tal que $\mathrm{Gal}(F/\mathbb{Q}) = G$. Este problema está em aberto, mas até à data não existe nenhuma razão forte que sugira que algum grupo finito não pode ser realizado como o grupo de Galois de uma extensão de $\mathbb{Q}$. O que acontece se substituirmos $\mathbb{Q}$ por $\mathbb{Q}_p$? Será que continua a ser razoável esperar que qualquer grupo finito apareça como o grupo de Galois de uma extensão finita de $\mathbb{Q}_p$? O resultado principal desta secção mostra que não, e que de facto temos restrições muito fortes sobre a estrutura do grupo de Galois de uma extensão finita de corpos locais: este é sempre um *grupo solúvel*.

Vamos começar por analisar o caso das extensões não ramificadas, que é particularmente simples.

Proposição 3.6.1. *Seja $L : K$ uma extensão finita não ramificada de corpos locais. Então*

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k_K).$$

Demonstração. Seja $n = [L : K] = [k_L : k_K]$. Escrevemos $k_L = k_K(\overline{\alpha})$, e seja $\overline{f}$ o polinómio mínimo de $\overline{\alpha}$ sobre k_K. De acordo com a prova do Lema 3.4.1, temos $L = K(\alpha)$ onde α é uma raiz de um polinómio mónico f, com $\deg(f) = \deg(\overline{f})$, que se reduz a $\overline{f}$ módulo $\mathfrak{m}_K$.

Notemos que o polinómio $\overline{f}$ fatoriza em fatores lineares distintos sobre k_L; de facto, o Lema A.0.20 mostra que a extensão $k_L : k_K$ é uma extensão de Galois, pelo que existem n automorfismos de k_L que ficam k_K, mas esses automorfismos estão em correspondência bijetiva com as raízes de $\overline{f}$ em k_L, pelo que $\overline{f}$, que tem grau n, tem n raízes distintas em k_L. Pelo Lema de Hensel, conclui-se que f tem n raízes distintas em L.

Obtemos assim uma bijeção entre $\mathrm{Gal}(L/K)$ e $\mathrm{Gal}(k_L/k_K)$ do seguinte modo: associamos ao automorfismo de L que fixa K e envia α na raiz θ de f o automorfismo de k_L que fixa k_K e envia α na raiz $\overline{\theta}$ de $\overline{f}$, onde $\overline{\theta}$ é obtida reduzindo θ módulo $\mathfrak{m}_L$. Fica como exercício para o leitor mostrar que esta correspondência é um homomorfismo de grupos. □

Corolário 3.6.2. *Toda a extensão não ramificada de corpos locais é uma extensão de Galois.*

Demonstração. Se $L : K$ é não ramificada, pela Proposição 3.6.1 temos

$$|\mathrm{Gal}(L/K)| = |\mathrm{Gal}(k_L/k_K)| = [k_L : k_K] = [L : K]$$

pois $k_L : k_K$ é uma extensão de Galois. □

O grupo de Galois $\mathrm{Gal}(k_L/k_K)$ é cíclico de ordem $[L : K]$ pelo Lema A.0.20, portanto já temos tudo o que é necessário para compreender os grupos de Galois que aparecem no caso de uma extensão não ramificada. Tendo em conta o Lema 3.4.4, vamos agora concentrar-nos nos grupos de Galois associados a extensões totalmente ramificadas. Para isso, precisamos de um resultado preparatório.

Proposição 3.6.3. *Seja $L : K$ uma extensão totalmente ramificada, e seja π um uniformizador de L. Então, para todo o $x \in \mathcal{O}_L$, existem $a_0, a_1, a_2, a_3, \ldots \in \mathcal{O}_K$ tais que*

$$x = a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3 + \cdots.$$

Demonstração. A prova é análoga à da Proposição 2.1.8. Considere-se a classe de congruência de x módulo $\mathfrak{m}_L$: como $L : K$ é não ramificada, tem-se $k_L = k_K$, e portanto essa classe tem um representante em $\mathcal{O}_K$. Existe assim $a_0 \in \mathcal{O}_K$ tal que $x \equiv a_0 \pmod{\pi}$, e podemos escrever

$$x = a_0 + x_1\pi$$

com $x_1 \in \mathcal{O}_L$.

Analogamente, podemos escrever $x_1 = a_1 + x_2\pi$, e obtemos

$$x = a_0 + a_1\pi + x_2\pi^2.$$

Continuando este raciocínio, obtemos para cada k uma expressão

$$x = a_0 + a_1\pi + \cdots + a_{k-1}\pi^{k-1} + x_k\pi^k$$

com $a_0, \ldots, a_{k-1}, x_k \in \mathcal{O}_K$. É fácil concluir que a série

$$\sum_{j=0}^{\infty} a_j\pi^j$$

converge para x. □

Recorde-se que o nosso objetivo principal nesta secção é provar que o grupo de Galois de qualquer extensão finita de corpos locais é solúvel, e vamos fazê-lo agora para extensões totalmente ramificadas. Um grupo finito N diz-se *solúvel* se existe uma torre de subgrupos

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r = N$$

tal que, para $i = 1, \ldots, r$, N_{i-1} é um subgrupo normal de N_i e N_i/N_{i-1} é abeliano. Precisamos de construir uma torre de subgrupos da forma acima indicada quando $G = \mathrm{Gal}(L/K)$ é o grupo de Galois de uma extensão totalmente ramificada. Essa construção é dada pela definição seguinte.

Definição 3.6.4. Seja $L : K$ uma extensão de Galois de corpos locais. Seja ν a valoração normalizada em L. Para cada $s \geq 1$, seja

$$G_s = \{\sigma \in \mathrm{Gal}(L/K) : \nu(\sigma(x) - x) \geq s + 1 \text{ para todo o } x \in \mathcal{O}_L\}.$$

Da definição resulta de imediato que $G_{-1} = \mathrm{Gal}(L/K)$. No caso em que $L : K$ é totalmente ramificada, podemos dizer ainda mais:

Proposição 3.6.5. *Se $L : K$ é totalmente ramificada, então $G_0 = \mathrm{Gal}(L/K)$.*

Demonstração. Seja $\sigma \in \mathrm{Gal}(L/K)$, e seja $x \in \mathrm{O}_L$. Como $k_L = k_K$, a classe de congruência de x módulo m_L tem um representante $y \in \mathrm{O}_K$. Então

$$\sigma(x) - x = \sigma(y + (x - y)) - x = y + \sigma(x - y) - x = \sigma(x - y) - (x - y).$$

Como $x - y \in \mathfrak{m}_L$, também se tem $\sigma(x - y) \in \mathfrak{m}_L$, e portanto $\sigma(x) - x \in \mathfrak{m}_L$. Como isto vale para todo o $x \in \mathrm{O}_L$, isto diz-nos precisamente que $\mathrm{Gal}(L/K) = G_0$. □

É, ainda, claro que $G_s = \{1\}$ para s suficientemente grande. Para ver isto, fixemos $\sigma \in \mathrm{Gal}(L/K)$ diferente da identidade; então existe $x \in \mathcal{O}_L$ tal que $\sigma(x) \neq x$. Logo não temos $\sigma \in G_s$ para s suficientemente grande, pois para s suficientemente grande não se tem $\nu(\sigma(x) - x) \geq s+1$. Como $\mathrm{Gal}(L/K)$ é finito, aplicando este argumento a cada automorfismo individualmente conclui-se que $G_s = \{1\}$ para s suficientemente grande.

De modo a provar que o grupo de Galois de uma extensão totalmente ramificada é solúvel, basta então provar que, para cada $s \geq 0$, G_{s+1} é um subgrupo normal de G_s e G_s/G_{s+1} é abeliano. Isso resulta do lema que se segue.

Lema 3.6.6. *Seja $L : K$ uma extensão totalmente ramificada de Galois de corpos locais. Seja π um uniformizador de L, e seja ν uma valoração normalizada em L. Para cada $s \geq 0$, definimos o grupo $U^{(s)}$ da seguinte forma: $U^{(0)} = \mathcal{O}_L^\times$ e, para $s > 0$,*

$$U^{(s)} = \{x \in \mathcal{O}_L : \nu(x-1) \geq s\}.$$

(É fácil ver que $U^{(s)}$ é um grupo com a multiplicação de L.) Para cada $s \geq 0$, definimos uma aplicação $\phi : G_s \to U^{(s)}/U^{(s+1)}$ por

$$\phi(\sigma) = \frac{\sigma(\pi)}{\pi}.$$

Então ϕ não depende da escolha de π, e além disso ϕ é um homomorfismo de grupos com núcleo G_{s+1}.

Demonstração. Começamos por provar que ϕ está bem definido, ou seja, que $\frac{\sigma(\pi)}{\pi}$ é de facto um elemento de $U^{(s)}$. Como, por hipótese, $\sigma \in G_s$, temos $\nu(\sigma(\pi)-\pi) \geq s+1$, temos $\sigma(\pi) = \pi+\pi^{s+1}x$ para algum $x \in \mathcal{O}_L$, e portanto

$$\frac{\sigma(\pi)}{\pi} = \frac{\pi + \pi^{s+1}x}{\pi} = 1 + \pi^s x \equiv 1 \pmod{\pi^s},$$

pelo que $\frac{\sigma(\pi)}{\pi} \in U^{(s)}$.

Provemos agora que ϕ não depende da escolha de π. Seja então ϖ outro uniformizador de L; então $\varpi = \pi u$ para alguma unidade $u \in \mathcal{O}_L^\times$. Como $\nu(\sigma(u) - u) \geq s+1$, podemos escrever $\sigma(u) = u + \pi^{s+1}y$ para algum $y \in \mathcal{O}_L$. Temos assim

$$\frac{\sigma(\varpi)}{\varpi} = \frac{\sigma(\pi u)}{\pi u} = \frac{\sigma(\pi)}{\pi} \cdot \frac{\sigma(u)}{u} = \frac{\sigma(\pi)}{\pi} \cdot (1 + \pi^{s+1}u^{-1}y).$$

Notemos que $u^{-1} \in \mathcal{O}_L$, e portanto $1 + \pi^{s+1}u^{-1}y \in U^{(s+1)}$. Conclui-se que $\frac{\sigma(\pi)}{\pi}$ e $\frac{\sigma(\varpi)}{\varpi}$ são iguais no quociente $U^{(s)}/U^{(s+1)}$.

Vejamos agora que ϕ é um homomorfismo de grupos. Sejam $\sigma, \tau \in G_s$, e note-se que

$$\phi(\sigma\tau) = \frac{(\sigma \circ \tau)(\pi)}{\pi} = \frac{\sigma(\tau(\pi))}{\tau(\pi)} \cdot \frac{\tau(\pi)}{\pi}.$$

Por definição $\phi(\tau) = \frac{\tau(\pi)}{\pi}$. Além disso, como a definição de ϕ não depende da escolha de π e $\tau(\pi)$ também é um uniformizador de L, temos $\phi(\sigma) = \frac{\sigma(\tau(\pi))}{\tau(\pi)}$. Portanto

$$\phi(\sigma\tau) = \phi(\sigma)\phi(\tau),$$

como pretendido.

Falta determinar $\mathrm{Ker}(\phi)$. Notemos que temos $\sigma \in \mathrm{Ker}(\phi)$ se e só se $\frac{\sigma(\pi)}{\pi} \in U^{(s+1)}$. Isto é equivalente a ter-se

$$\nu\left(\frac{\sigma(\pi)}{\pi} - 1\right) \geq s, \quad \text{ou seja,} \quad \nu(\sigma(\pi) - \pi) \geq s + 1.$$

Queremos provar que isto é equivalente a ter-se $\sigma \in G_{s+1}$. Uma das implicações é óbvia: se $\sigma \in G_{s+1}$ esta desigualdade é imediata. Reciprocamente, suponha-se que $\nu(\sigma(\pi) - \pi) \geq s + 1$; queremos provar que $\nu(\sigma(x) - x) \geq s + 1$ para *todo* o $x \in \mathcal{O}_L$. Seja então $x \in \mathcal{O}_L$, e usemos a Proposição 3.6.3 para escrever

$$x = a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3 + \cdots$$

com $a_0, a_1, a_2, a_3, \ldots, \in \mathcal{O}_K$. Temos assim

$$\begin{aligned}\sigma(x) - x &= (a_0 + a_1\sigma(\pi) + a_2\sigma(\pi)^2 + a_3\sigma(\pi)^3 + \cdots) - (a_0 + a_1\pi + a_2\pi^2 + a_3\pi^3 + \cdots) \\ &= a_1(\sigma(\pi) - \pi) + a_2(\sigma(\pi)^2 - \pi^2) + a_3(\sigma(\pi)^3 - \pi^3) + \cdots.\end{aligned}$$

Usando a identidade

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}),$$

vemos que todas as diferenças $\sigma(\pi)^k - \pi^k$ são divisíveis por $\sigma(\pi) - \pi$ em $\mathcal{O}_L$, e portanto são divisíveis por π^{s+1}. Conclui-se que $\sigma(x) - x$ é divisível em $\mathcal{O}_L$ por π^{s+1}, como pretendido. Isto mostra que $\mathrm{Ker}(\phi) = G_{s+1}$ e prova o Lema. □

Corolário 3.6.7. *Seja $L : K$ uma extensão de Galois totalmente ramificada de corpos locais. Então, para todo o $s \geq 0$, $G_{s+1} \trianglelefteq G_s$ e G_s/G_{s+1} é abeliano. Em particular,* $\mathrm{Gal}(L/K)$ *é um grupo solúvel.*

Demonstração. Pelo Lema 3.6.6, G_{s+1} é o núcelo de um homomorfismo definido em G_s, logo G_{s+1} é um subgrupo normal. Além disso, o Primeiro Teorema do Homomrfismo dá-nos um homomorfismo injetivo $\tilde{\phi}$ que encaixa no diagrama seguinte:

$$\begin{array}{ccc} G_s & & \\ \downarrow & \searrow^{\phi} & \\ G_s/G_{s+1} & \overset{\tilde{\phi}}{\hookrightarrow} & U^{(s)}/U^{(s+1)} \end{array}$$

Portanto G_s/G_{s+1} é isomorfo a um subgrupo de $U^{(s)}/U^{(s+1)}$, que é abeliano, e portanto é também abeliano. Por fim, juntamente com a Proposição 3.6.5 isto implica que $\mathrm{Gal}(L/K)$ é um grupo solúvel. □

Corolário 3.6.8. *Seja $L : K$ uma extensão de Galois finita de corpos locais. Então* $\mathrm{Gal}(L/K)$ *é solúvel.*

Demonstração. Usando o Lema 3.4.4, encontramos um corpo intermédio M tal que $M : K$ é uma extensão não ramificada e $L : M$ é uma extensão totalmente ramificada. Então Gal(L/M) é um subgrupo de $\mathrm{Gal}(L/K)$, e por Teoria de Galois temos

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \cong \mathrm{Gal}(M/K).$$

Mas pela Proposição 3.6.1 temos $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(k_L/k_K)$, que é cíclico, e em particular solúvel. Por fim, acabámos de ver que $\mathrm{Gal}(L/M)$ é solúvel, pois $L : M$ é totalmente ramificada. O resultado segue usando o facto de que se G/H e H são grupos solúveis então G também é solúvel. □

O Corolário 3.6.8 tem implicações bastante profundas sobre o comportamento das extensões de um corpo local, e em particular de $\mathbb{Q}_p$. Dado um inteiro positivo n, um conhecido Teorema de Hilbert afirma, em termos informais, que, escolhido "ao acaso" um polinómio de grau n com coeficientes inteiros, com probabilidade 1 este é irredutível e o seu grupo de Galois (ou seja, o grupo de Galois do seu corpo de fatorização sobre $\mathbb{Q}$) é o maior possível, ou seja, o grupo das permutações de n símbolos, S_n. Por outras palavras, dado um polinómio "genérico" com coeficientes racionais, não é de esperar que haja relações entre as suas raízes que nos impeçam de as permutar à nossa vontade para construir um automorfismo de Galois. Por outro lado, se $n \geq 5$, então o grupo de Galois de um polinómio com coeficientes em $\mathbb{Q}_p$ *nunca* é isomorfo a S_n; de facto, S_n não é solúvel para $n \geq 5$. Portanto há sempre relações misteriosas entre as raízes de polinómios de grau grande.

§3.7. O Lema de Krasner e aplicações

Nesta secção vamos utilizar a teoria que já desenvolvemos sobre extensões de corpos locais para provar que um corpo local tem apenas um número finito de extensões de cada grau. Isto encaixa na perspetiva de que os corpos locais são "os corpos mais simples a seguir aos corpos finitos"; para corpos finitos temos um resultado ainda mais forte, que garante que existe apenas *uma* extensão de cada grau, e corpos mais "complicados" de um ponto de vista aritmético, como o corpo $\mathbb{Q}$ dos racionais, tem uma infinidade de extensões de grau n para cada n.

Uma peça chave na obtenção deste resultado é um lema elegante da teoria de corpos locais, conhecido na literatura como o *Lema de Krasner*. Este afirma essencialmente que, dados α, β num fecho algébrico $\overline{K}$ de um corpo local K, se β está suficientemente próximo de α então $K(\alpha) \subseteq K(\beta)$. (Recorde-se que o valor absoluto em K se estende de maneira única a $\overline{K}$, pelo Corolário 3.2.2.)

Lema 3.7.1 (Lema de Krasner)**.** *Seja $(K, |\cdot|)$ um corpo local de característica 0 com fecho algébrico $\overline{K}$, e seja $\alpha \in \overline{K}$. Sejam $\alpha = \alpha_1, \ldots, \alpha_n$ os conjugados de α sobre K (i.e. as raízes do polinómio mínimo de α sobre K) e seja $\beta \in K$ tal que*

$$|\beta - \alpha| < |\alpha_i - \alpha| \text{ para } i = 2, \ldots, n.$$

Então $K(\alpha) \subseteq K(\beta)$ (isto é, $\alpha \in K(\beta)$).

Demonstração. Suponhamos o contrário, e seja $L : K(\beta)$ uma extensão de Galois de $K(\beta)$ contendo α (aqui a hipótese de que K tem característica 0 é essencial, pois garante que uma tal extensão existe). Como $\alpha \notin K(\beta)$, por Teoria de Galois existe um automorfismo $\sigma \in \mathrm{Gal}(L/K(\beta))$ que *não* fixa α. Como automorfismos de Galois preservam valores absolutos[1], vem que

$$|\beta - \alpha| = |\sigma(\beta - \alpha)| = |\beta - \sigma(\alpha)|. \tag{3.6}$$

Mas, como $\sigma \in \mathrm{Gal}(L/K)$, tem-se que $\sigma(\alpha)$ é uma raiz do polinómio mínimo de α, ou seja $\sigma(\alpha) = \alpha_i$ para algum i (com i necessariamente diferente de 1). Ora, temos

$$|\alpha - \alpha_i| = |(\beta - \alpha) + (\alpha_i - \beta)| \leq \max\{|\beta - \alpha|, |\beta - \alpha_i|\}$$

e como $|\alpha - \alpha_i| > |\beta - \alpha|$, decorre que $|\alpha - \alpha_i| \leq |\beta - \alpha_i|$. Mas então $|\beta - \alpha_i| > |\beta - \alpha|$, contradizendo (3.6). □

Este pequeno lema será utilizado para garantir que polinómios irredutíveis "próximos" em $K[X]$ geram extensões "parecidas". Para tirar essa conclusão a partir do Lema de Krasner, precisamos do próximo resultado, para o qual vamos introduzir uma definição preliminar.

Definição 3.7.2 (Norma de um polinómio)**.** Seja $(K, |\cdot|)$ um corpo local. Dado um polinómio

$$f(X) = c_n X^n + \cdots + c_0 \in K[X],$$

definimos a sua *norma* por

$$\|f\| = \max\{|c_n|, \ldots, |c_0|\}.$$

É imediato verificar que, definindo a distância entre dois polinómios f e g como sendo $\|f - g\|$, obtemos uma estrutura de espaço métrico em $K[X]$.

[1] Pois... eu tenho vindo a usar isto implicitamente e devia escrever uma prova.

Lema 3.7.3 (Continuidade das raízes)**.** *Seja $(K, |\cdot|)$ um corpo local. Seja $f(X)$ um polinómio mónico em $\mathcal{O}_K[X]$, e suponha-se que $f(X)$ factoriza sobre o fecho algébrico $\overline{K}$ como*

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_n).$$

Então, para todo o $\varepsilon > 0$, existe $\delta > 0$ tal que, se g é um polinómio mónico em $\mathcal{O}_K[X]$ com $\|f - g\| < \delta$ e $\alpha \in \overline{K}$ é uma raiz de g, existe $i \in \{1, \ldots, n\}$ tal que $|\alpha - \alpha_i| < \varepsilon$.

Demonstração. Escolhemos $\delta = \varepsilon^n$. Se $g(\alpha) = 0$ e $\|f - g\| < \delta$, então $|f(\alpha) - g(\alpha)| < \delta$; de facto, é imediato a partir da definição que, se $|\alpha| \leq 1$ e h é um polinómio, então $|h(\alpha)| \leq \|h\|$ (notemos que α tem valor absoluto menor ou igual a 1 uma vez que é raiz de um polinómio mónico com coeficientes em $\mathcal{O}_K$).

Mas, como $g(\alpha) = 0$, tem-se

$$|f(\alpha) - g(\alpha)| = |f(\alpha)| = |\alpha - \alpha_1| \cdots |\alpha - \alpha_n|$$

e portanto

$$|\alpha - \alpha_1| \cdots |\alpha - \alpha_n| < \delta = \varepsilon^n,$$

de onde resulta que existe i tal que $|\alpha - \alpha_i| < \varepsilon$. □

Para aplicarmos estes lemas ao resultado pretendido, de que um corpo local tem um número finito de extensões de cada grau, vamos utilizar alguma topologia: precisamos de uma propriedade topológica crucial do anel de inteiros de um corpo local.

Lema 3.7.4. *Seja K um corpo local. Então $\mathcal{O}_K$ é compacto.*

Demonstração. Vamos utilizar um critério clássico de compacidade para espaços métricos: um espaço métrico é compacto se e só se é completo e totalmente limitado. (Um espaço métrico diz-se totalmente limitado se para todo o $\varepsilon > 0$ é possível cobri-lo com um número finito de bolas de raio ε.)

Que $\mathcal{O}_K$ é completo é imediato, tendo em conta que é um subespaço fechado do espaço completo K. Resta provar que $\mathcal{O}_K$ é totalmente limitado.

Aqui entra de forma decisiva o facto de o corpo residual associado a um corpo local ser *finito*. Seja π um uniformizador de K, e seja

$$q = |k_K| = |\mathcal{O}_K / \pi \mathcal{O}_K|.$$

Vamos ver que todos os quocientes $\mathcal{O}_K/\pi^n\mathcal{O}_K$, com $n \geq 1$, são também finitos. (Pensemos no caso $K = \mathbb{Q}_p$; sabemos que $|\mathbb{Z}_p/p^n\mathbb{Z}_p| = p^n$ para todo o n.) De facto, afirmamos que

$$|\mathcal{O}_K/\pi^n\mathcal{O}_K| = q^n \text{ para todo o } n \geq 1.$$

Provamo-lo por indução em n: para $n = 1$ é imediato. Agora considere-se o homomorfismo sobrejetivo

$$f : \mathcal{O}_K/\pi^{n+1}\mathcal{O}_K \to \mathcal{O}_K/\pi\mathcal{O}_K$$

obtido por redução módulo π. Pelo Primeiro Teorema do Isomorfismo, temos

$$(\mathcal{O}_K/\pi^{n+1}\mathcal{O}_K)/\mathrm{Ker}(f) \cong \mathcal{O}_K/\pi\mathcal{O}_K$$

e como o lado direito tem q elementos, basta provar que $|\mathrm{Ker}(f)| = q^n$. Mas, por definição, temos $f(x + \pi^{n+1}\mathcal{O}_K) = 0$ se e só se $x = \pi y$ para algum $y \in \mathcal{O}_K$. Então

$$\mathrm{Ker}(f) = \pi\mathcal{O}_K/\pi^{n+1}\mathcal{O}_K.$$

E o leitor facilmente verifica que temos um isomorfismo

$$\mathcal{O}_K/\pi^n\mathcal{O}_K \cong \pi\mathcal{O}_K/\pi^{n+1}\mathcal{O}_K$$

dado por $x + \pi^n\mathcal{O}_K \mapsto \pi x + \pi^{n+1}\mathcal{O}_K$. Portanto, por hipótese de indução, temos

$$|\mathrm{Ker}(f)| = |\mathcal{O}_K/\pi^n\mathcal{O}_K| = q^n,$$

como pretendido.

Seja agora $\varepsilon > 0$; vamos ver como cobrir $\mathcal{O}_K$ com um número finito de bolas abertas de raio ε. Para tal, seja n um inteiro positivo tal que $|\pi|^n < \varepsilon$. Pelo que vimos, o quociente $|\mathcal{O}_K/\pi^n\mathcal{O}_K|$ é finito; assim, existem $a_1, \ldots, a_r \in \mathcal{O}_K$ tais que qualquer elemento de $\mathcal{O}_K$ é congruente com um dos a_i's módulo π^n. Mas então, dado qualquer $x \in \mathcal{O}_K$, tem-se, para algum i,

$$x - a_i \in \pi^n\mathcal{O}_K, \text{ ou seja, } |x - a_i| \leq |\pi|^n < \varepsilon.$$

Portanto qualquer elemento de $\mathcal{O}_K$ está na bola de centro a_i e raio ε para algum i. Conclui-se que $\mathcal{O}_K$ é totalmente limitado, completando a prova. □

Estamos prontos para provar o resultado principal.

Teorema 3.7.5. *Seja K um corpo local, e fixemos um fecho algébrico $\overline{K}$. Então, para todo o inteiro positivo n, K tem apenas um número finito de extensões de grau n contidas em $\overline{K}$.*

Demonstração. Usando o Lema 3.4.4, reduzimos facilmente a nossa tarefa a provar que existe apenas um número finito de extensões *não ramificadas* de cada grau e um número finito de extensões *totalmente ramificadas* de cada grau. Para extensões não ramificadas, isto é uma consequência direta do Lema 3.4.1; extensões não ramificadas de grau n de K estão em correspondência com extensões de grau n do corpo residual finito k_K, e um corpo finito tem apenas *uma* extensão de grau n, para cada n.

Reduzimos então o nosso trabalho a provar que, para todo o n, K tem apenas um número finito de extensões *totalmente ramificadas* de grau n. Pelo Lema 3.5.4, qualquer tal extensão é da forma $K(\alpha)$, onde α é uma raiz de um polinómio de Eisenstein de grau n. Fixemos um polinómio de Eisenstein de grau n em $K[X]$ (necessariamente em $\mathcal{O}_K[X]$), digamos $f(X)$; suponhamos que $f(X)$ fatoriza como $f(X) = (X - \alpha_1)\cdots(X - \alpha_n)$ sobre $\overline{K}$, e seja

$$\varepsilon = \min\{|\alpha_i - \alpha_j| : 1 \leq i < j \leq n\}.$$

Pelo Lema 3.7.3, existe $\delta > 0$ tal que, se $g(X)$ é um polinómio de Eisenstein de grau n em $K[X]$ e $\|f - g\| < \delta$, então para toda a raiz α de g tem-se $|\alpha - \alpha_i| < \varepsilon$ para algum i. Isto implica, pelo Lema de Krasner (Lema 3.7.1), que $K(\alpha_i) \subseteq K(\alpha)$; mas como $[K(\alpha) : K] = [K(\alpha_i) : K] = n$ vem que $K(\alpha_i) = K(\alpha)$. Em particular, temos um número finito de possibilidades para $K(\alpha)$ quando $\|f - g\| < \delta$.

Provámos portanto que, dado qualquer polinómio de Eisenstein $f \in K[X]$, existe uma bola aberta B_f centrada em f tal que as raízes dos polinómios de Eisenstein contidos em B_f geram apenas um número *finito* de extensões (totalmente ramificadas) de K. Mas o espaço dos polinómios de Eisenstein em $K[X]$, munido da métrica dada pela Definição 3.7.2, é isomorfo a

$$\underbrace{\pi\mathcal{O}_K \times \cdots \times \pi\mathcal{O}_K}_{n-1 \text{ vezes}} \times (\pi\mathcal{O}_K \setminus \pi^2\mathcal{O}_K)$$

(onde π é um uniformizador de K). Ora, este espaço é compacto, sendo um produto de compactos: $\pi\mathcal{O}_K$ é homeomorfo a $\mathcal{O}_K$, que é compacto pelo Lema 3.7.4, e $\pi\mathcal{O}_K \setminus \pi^2\mathcal{O}_K$ é um subespaço fechado de um espaço compacto, sendo portanto também compacto. Mas então a cobertura do espaço dos polinómios de Eisenstein dada pelas bolas B_f admite uma subcobertura finita; ou seja, existem $f_1, \ldots, f_k$ tais que qualquer polinómio de Eisenstein pertence a uma das bolas $B_{f_1}, \ldots, B_{f_k}$. E as raízes de polinómios contidos em cada uma destas bolas geram um número finito de extensões, obtendo-se assim um número finito de extensões totalmente ramificadas no total, como pretendido. □

A. Corpos finitos

Neste apêndice pretende-se dar uma breve introdução à estrutura dos corpos finitos. Para isso vamos utilizar alguns resultados e conceitos sobre corpos em geral, que vamos resumir a seguir.

O primeiro é a noção de *grau* de uma extensão de corpos.

Definição A.0.1 (Grau de uma extensão)**.** Seja $L : K$ uma extensão de corpos (isto significa apenas que K é um subcorpo do corpo L). Então L é automaticamente um espaço vetorial sobre K. O *grau* $[L : K]$ da extensão é a dimensão desse espaço vetorial.

Exemplo A.0.2. O grau da extensão $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ é 2. De facto, todo o elemento de $\mathbb{Q}(\sqrt{2})$ pode ser escrito unicamente na forma

$$a + b\sqrt{2} \quad \text{com } a, b \in \mathbb{Q}.$$

Portanto $(1, \sqrt{2})$ é uma base de $\mathbb{Q}(\sqrt{2})$ como espaço vetorial sobre $\mathbb{Q}$ (precisamos de dois parâmetros racionais para descrever um elemento genérico de $\mathbb{Q}(\sqrt{2})$).

Mais geralmente, se α é uma raiz de um polinómio irredutível de grau n sobre o corpo K então a extensão $K(\alpha) : K$ tem grau n: uma base é $(1, \alpha, \ldots, \alpha^{n-1})$.

O grau de uma extensão possui a seguinte propriedade fundamental:

Facto A.0.3. Sejam $L : K$ e $M : L$ extensões de corpos. Então

$$[M : K] = [M : L][L : K].$$

Precisamos também da noção de *corpo de fatorização* (em inglês, *splitting field*) de um polinómio.

Definição A.0.4 (Corpo de fatorização)**.** Seja K um corpo e seja $f \in K[X]$ um polinómio. Um *corpo de fatorização* de f é um corpo L contendo K tal que:

(a) f fatoriza em $L[X]$ como produto de fatores de grau 1;

(b) L é gerado sobre K por raízes de f.

Facto A.0.5. Seja K um corpo e seja $f \in K[X]$ um polinómio. Então existe um corpo de fatorização de f. Além disso, esse corpo de fatorização é único a menos de isomorfismo.

Passemos aos corpos finitos. Como vamos ver, os corpos finitos são estruturas algébricas particularmente bem comportadas e compreendidas. Isto é completamente diferente do que acontece, por exemplo, com os *grupos finitos*, que após muito esforço ainda estamos longe de conseguir classificar: já no caso dos corpos finitos, sabemos exatamente quantos existem com cada cardinalidade, e como se "encaixam" uns nos outros.

O nosso primeiro resultado fundamental dá-nos esta classificação prometida dos corpos finitos.

Teorema A.0.6. *Seja $q > 1$ um inteiro. Então existe um corpo finito com q elementos se e só se q é uma potência de um primo. Além disso, se q é uma potência de um primo então existe exatamente um corpo com q elementos a menos de isomorfismo.*

Antes de provarmos este teorema, vamos pensar em como podemos construir corpos finitos. Já conhecemos alguns: os corpos $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, com um número primo de elementos. Como podemos construir um corpo finito que não seja um destes? Podemos tentar obtê-lo como uma *extensão* de um destes corpos que já conhecemos.

Pensemos na maneira como obtemos $\mathbb{C}$ a partir de $\mathbb{R}$. Essencialmente essa construção destina-se a reparar um "defeito" de $\mathbb{R}$, que é não possuir uma raiz do polinómio $X^2 + 1$. Então acrescentamos essa raiz, i, a $\mathbb{R}$. Ao fazê-lo, temos de acrescentar muitos outros elementos, como $2i + 4$ e $i^7 + 3i^3 + 2$. Mais geralmente, temos de acrescentar qualquer *polinómio* em i.

Então a aritmética deste novo corpo que vamos obter é, num certo sentido, parecida com a aritmética do anel $\mathbb{R}[X]$. Mas há uma diferença, que é que a nossa "indeterminada" i satisfaz algumas relações extra, que vêm de se ter $i^2 + 1 = 0$. Portanto podemos pensar em $\mathbb{C}$ como uma variante do anel $\mathbb{R}[X]$ em que "declaramos" que $X^2 + 1 = 0$. Ou seja, obtemos

$$\mathbb{C} = \mathbb{R}[X]/\langle X^2 + 1\rangle.$$

Podemos tentar fazer a mesma coisa com um corpo $\mathbb{F}_p$. Consideremos, por exemplo, $\mathbb{F}_2$, e vamos procurar um polinómio com coeficientes em $\mathbb{F}_2$ que ainda não tenha raízes em $\mathbb{F}_2$. Agora o polinómio $X^2 + 1$ não serve, mas podemos usar o polinómio $X^2 + X + 1$. Consideramos portanto o corpo obtido acrescentando a $\mathbb{F}_2$ um novo elemento α que satisfaz $\alpha^2 + \alpha + 1 = 0$. Os elementos desse corpo estendido vão ser então 0, 1, α e $1 + \alpha$; qualquer outro polinómio em α se pode reduzir a um destes usando a relação $\alpha^2 + \alpha + 1 = 0$. Se quisermos, por exemplo, multiplicar $1 + \alpha$ por si próprio, obtemos

$$(1 + \alpha)^2 = 1 + 2\alpha + \alpha^2 = \alpha + (1 + \alpha + \alpha^2) = \alpha.$$

Construímos o *corpo com* 4 *elementos*, $\mathbb{F}_4$. As tabelas de adição e multiplicação encontram-se abaixo.

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

De facto podemos ver que este corpo é o *único* corpo com 4 elementos, em consonância com o Teorema A.0.6: seja F um corpo com 4 elementos. A ordem de 1 no grupo aditivo de F divide 4 e portanto, como $1 \neq 0$, é 2 ou 4. Se for 4, então temos $2 \neq 0$ em F mas $4 = 0$ em F, o que é absurdo pois $4 = 2^2$. Logo a ordem aditiva de 1 é 2, ou seja, $1 + 1 = 0$. Seja agora α um elemento de F diferente de 0 e 1. O quarto elemento de F é então necessariamente $1 + \alpha$. Como o grupo multiplicativo de F tem 3 elementos, tem-se $\alpha^3 = 1$. Ou seja,

$$0 = \alpha^3 - 1 = (\alpha - 1)(\alpha^2 + \alpha + 1).$$

Mas $\alpha - 1 \neq 0$ por hipótese, logo $\alpha^2 + \alpha + 1 = 0$. Isto força a que F tenha a estrutura que descrevemos antes.

Passemos agora ao caso geral. Para isso vamos recordar a noção de *característica* de um corpo.

Definição A.0.7. Seja K um corpo. A *característica* de K é a ordem de 1 no grupo aditivo de K, ou seja, é o menor inteiro $p > 0$ tal que

$$\underbrace{1 + \cdots + 1}_{p \text{ vezes}} = 0$$

(isto é, $p = 0$ em K) ou 0 caso não exista nenhum tal inteiro.

A característica de um corpo, se for diferente de 0, é necessariamente um primo. De facto, suponha-se que K tem característica $p > 0$, mas que $p = ab$ para alguns inteiros positivos $a, b < p$. Então $ab = 0$ em K, logo $a = 0$ ou $b = 0$. Isto contradiz o facto de p ser o *menor* inteiro positivo que é igual a 0 em K.

Com isto estamos prontos para provar uma direção do Teorema A.0.6.

Lema A.0.8. *O número de elementos de qualquer corpo finito é uma potência de um primo.*

Demonstração. Seja F um corpo finito e seja p a característica de F, que, como vimos, é um primo[1]. Considere-se o subcorpo de F gerado por 1, formado pelos elementos $0, 1, 1+1, 1+1+1, \ldots$, ou seja, pelos inteiros vistos como elementos de K. Como a ordem de 1 no grupo aditivo de F é igual a p, verifica-se facilmente que este subcorpo é isomorfo a $\mathbb{F}_p$. Portanto F é uma extensão de $\mathbb{F}_p$.

Seja $n = [F : \mathbb{F}_p]$ (note-se que F, sendo finito, não pode ter dimensão infinita sobre $\mathbb{F}_p$, pois se fosse então uma sua base sobre $\mathbb{F}_p$ teria um número infinito de elementos). Seja $(e_1, \ldots, e_n)$ uma base de F sobre $\mathbb{F}_p$. Então qualquer elemento de F se pode escrever de maneira única na forma

$$a_1 e_1 + \cdots + a_n e_n$$

com $a_1, \ldots, a_n \in \mathbb{F}_p$. Temos p escolhas para cada a_i, logo temos p^n escolhas para $(a_1, \ldots, a_n)$, portanto F tem exatamente p^n elementos, terminando a prova. □

Agora falta a direção do Teorema A.0.6 em que temos de provar a *existência* (e unicidade) de corpos com certos números de elementos. O leitor pode estar à espera de que, chegado a este ponto, mostremos uma construção explícita de um corpo com p^n para cada p, n e que depois provemos laboriosamente que todo o corpo com esse número de elementos tem de ser isomorfo ao modelo que construímos. Isso é mais ou menos o que faremos, mas para o efeito de provar o Teorema A.0.6 é preferível obter o corpo com p^n elementos de uma maneira consideravelmente abstrata, que não é a maneira como se trabalha na prática com esse corpo "à mão", ou como se ensina um computador a trabalhar com ele.

Precisamos de uma proposição auxiliar[2].

Proposição A.0.9. *Seja K um corpo de característica p, e seja n um inteiro positivo. Então, para quaisquer $\alpha, \beta \in K$,*

$$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}.$$

[1] A característica de F não é 0 pois 1, sendo um elemento do grupo finito $(F, +)$, tem ordem finita nesse grupo.

[2] Este resultado é conhecido em alguns sítios como o "sonho de todo o estudante", por razões que não deve ser difícil adivinhar.

Demonstração. Utilizamos indução em n. Para $n = 1$, temos pelo Binómio de Newton

$$\begin{aligned}(\alpha+\beta)^p &= \alpha^p + \beta^p + \sum_{k=1}^{p-1} \binom{p}{k} \alpha^k \beta^{p-k} \\ &= \alpha^p + \beta^p\end{aligned}$$

onde usámos que o inteiro $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ é divisível por p, e portanto é igual a 0 em K, que tem característica p.

Suponha-se agora que $n > 1$, e que já provámos o resultado análogo para $n-1$. Então

$$\begin{aligned}(\alpha+\beta)^{p^n} &= ((\alpha+\beta)^p)^{p^{n-1}} \\ &= (\alpha^p + \beta^p)^{p^{n-1}} \\ &= (\alpha^p)^{p^{n-1}} + (\beta^p)^{p^{n-1}} \\ &= \alpha^{p^n} + \beta^{p^n},\end{aligned}$$

como pretendido. □

Com isto estamos prontos para provar a direção em falta do Teorema A.0.6.

Lema A.0.10. *Seja q uma potência de um primo p. Então existe um corpo com q elementos, nomeadamente o corpo de fatorização do polinómio $X^q - X$ sobre $\mathbb{F}_p$. Além disso, esse corpo é único a menos de isomorfismo.*

Demonstração. Seja F o corpo de fatorização de $f(X) = X^q - X$ sobre $\mathbb{F}_p$. A existência de F é garantida pelo Facto A.0.5. Notemos que

$$f'(X) = qX^{q-1} - 1 = -1$$

e portanto $f(X)$ não tem raízes múltiplas em F, pois qualquer tal raiz tem que ser também uma raiz da derivada. Portanto F tem pelo menos q elementos, que são as raízes de $f(X)$. Queremos portanto ver que são os únicos.

Mas notemos que, por definição, o corpo F é gerado sobre $\mathbb{F}_p$ por raízes de $f(X)$; basta portanto verificar que todos os elementos de $\mathbb{F}_p$ são raízes de $f(X)$ e que a soma, o produto, e o inverso de raízes de $f(X)$ também é uma raiz de $f(X)$, implicando que F não contenha nenhum elemento para além das raízes de $f(X)$. Que todos os elementos de $\mathbb{F}_p$ são raízes de $f(X)$ é, digamos, uma consequência do Pequeno Teorema de Fermat. Agora, sejam α e β raízes de $f(X)$. Então $\alpha^q = \alpha$ e $\beta^q = \beta$. Logo $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$, pelo que $\alpha\beta$ também é uma raiz de $f(X)$. Além disso,

$$(\alpha+\beta)^q = \alpha^q + \beta^q = \alpha + \beta$$

pela Proposição A.0.9, pelo que $\alpha+\beta$ é uma raiz de $f(X)$. Por fim, é evidente que o inverso de uma raiz também é uma raiz, o que mostra que F não tem elementos para além das raízes de $f(X)$, e portanto que $|F| = q$.

Falta provar a unicidade de F; para isso vamos mostrar que qualquer corpo com q elementos é isomorfo ao corpo de fatorização de $X^q - X$ sobre $\mathbb{F}_p$ (aqui é crucial a afirmação sobre unicidade no Facto A.0.5). Seja então K um corpo arbitrário com q elementos. No decurso da prova do Lema A.0.8 vimos que K contém $\mathbb{F}_{p'}$ para algum primo p' e que q é uma potência de p'. Como q é uma potência de p por hipótese, resulta que $p = p'$ e K é uma extensão de $\mathbb{F}_p$.

Seja agora α um elemento arbitrário de K. Se $\alpha \neq 0$, então α pertence ao grupo multiplicativo $K^\times$, que tem $q-1$ elementos, e portanto, pelo Teorema de Lagrange, $\alpha^{q-1} = 1$. Logo

$$\alpha^q = \alpha.$$

Por outro lado, se $\alpha = 0$ a igualdade anterior também se verifica trivialmente, e portanto verifica-se para *todo* o $\alpha \in K$. Ou seja, todos os elementos de K são raízes de $X^q - X$. Como K tem q elementos, os elementos de K são todas as raízes de $X^q - X$, no sentido de que $X^q - X$ fatoriza em fatores de grau 1 sobre K (obtemos um fator por cada uma das q raízes). Por outro lado, claramente K é gerado pelas raízes de $X^q - X$ (porque é *formado* pelas raízes de $X^q - X$!). Logo K é o corpo de fatorização de $X^q - X$ sobre $\mathbb{F}_p$, ou seja, $K = F$, como pretendido. □

Está assim provado o Teorema A.0.6! Vamos então estabelecer a seguinte convenção:

Definição A.0.11. Se $q > 1$ é uma potência de um primo, designamos o corpo com q elementos por $\mathbb{F}_q$.

Claro que, como avisámos, a caracterização de $\mathbb{F}_q$ como o corpo de fatorização de $X^q - X$ sobre $\mathbb{F}_p$ não nos diz muito sobre a aritmética de $\mathbb{F}_q$. É uma visão muito útil se o objetivo for provar a sua existência e unicidade, como fizemos acima, mas se quisermos construir as tabelas de adição e multiplicação de $\mathbb{F}_q$, como fizemos para $q = 4$, precisamos de uma perspetiva mais prática. Essencialmente gostaríamos de ver $\mathbb{F}_q$ como um corpo da forma $\mathbb{F}_p(\alpha)$ obtido acrescentando a $\mathbb{F}_p$ uma raiz de um polinómio, que foi precisamente o que fizemos para $\mathbb{F}_4$.

Para conseguirmos esse objetivo, precisamos do seguinte resultado, que é aliás um resultado muito útil sobre a estrutura do grupo multiplicativo de um corpo finito.

Lema A.0.12. *Seja F um corpo finito. Então o grupo multiplicativo $F^\times$ é cíclico.*

Para provar isto, só precisamos de uma propriedade de $F^\times$ que decorre de $F^\times$ ser o grupo multiplicativo de um corpo: o facto de, para todo o m, a equação $x^m = 1$ ter no máximo m soluções em K. Isto é simplesmente um caso particular do facto de que um polinómio de grau m tem no máximo m raízes num corpo. Portanto basta provar o seguinte resultado mais geral.

Lema A.0.13. *Seja G um grupo finito. Suponha-se que, para todo o inteiro positivo m, existem no máximo m elementos $x \in G$ tais que $x^m = 1$. Então G é cíclico.*

Demonstração. No que se segue, vamos usar a convenção clássica de que $\varphi(n)$ designa o número de inteiros entre 1 e n que são primos com n (por outras palavras, $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$). Utilizaremos a seguinte identidade clássica:

$$\sum_{d|n} \varphi(d) = n.$$

Isto resulta de que, no grupo cíclico $\mathbb{Z}/n\mathbb{Z}$, que tem n elementos, há exatamente $\varphi(d)$ elementos com ordem d para cada $d \mid n$, de onde o resultado segue somando sobre todos os $d \mid n$.

Suponha-se agora que G é um grupo que satisfaz a hipótese do Lema, com $|G| = n$. A ordem de cada elemento de G é um divisor de n, pelo Teorema de Lagrange. Para cada divisor d de n, seja N_d o número de elementos de G com ordem d.

Afirmamos que $N_d \leq \varphi(d)$ para cada divisor d de n. Se $N_d = 0$ isto é imediato. Caso contrário, existe um elemento x em G de ordem d. Para todo o inteiro não negativo k, tem-se

$$(x^k)^d = (x^d)^k = 1.$$

Como as potências $1, x, \ldots, x^{d-1}$ são todas diferentes (pois x tem ordem d), estas são d soluções da equação $y^d = 1$, e portanto, por hipótese, são as únicas. Em particular, todos os elementos de ordem d em G estão entre $1, x, \ldots, x^{d-1}$, e portanto $N_d \leq d$. Mas podemos dizer algo mais forte: suponha-se que $\mathrm{mdc}(k, d) > 1$ para algum k, e portanto que $k = me$ para algum inteiro m e algum divisor $e > 1$ de d. Então

$$(x^k)^{\frac{d}{e}} = (x^{me})^{\frac{d}{e}} = x^{md} = 1.$$

Ou seja, se $\mathrm{mdc}(k, d) > 1$ então a ordem de x^k é menor do que d. Assim, das d soluções da equação $y^d = 1$, as potências x^k com $0 \leq k < d$, as únicas que podem ter ordem d são aquelas com $\mathrm{mdc}(k, d) = 1$. E existem $\varphi(d)$ tais valores de k, portanto existem no máximo $\varphi(d)$ elementos de ordem d em G, como pretendido.

Mas então temos

$$\sum_{d|n} N_d = |G| = n = \sum_{d|n} \varphi(d).$$

Como $N_d \leq \varphi(d)$ para todo o $d \mid n$, resulta da igualdade acima que de facto se tem a *igualdade* $N_d = \varphi(d)$ para todo o d. Em particular temos $N_n = \varphi(n) > 0$. Logo G contém pelo menos um elemento de ordem n, e portanto é cíclico, como pretendido. □

Provámos assim o Lema A.0.12, que generaliza o resultado clássico de que para todo o primo p existe uma *raiz primitiva* módulo p. Mas o Lema A.0.12 também diz que podemos ver qualquer corpo finito de uma maneira semelhante à que utilizámos para descrever $\mathbb{F}_4$!

Corolário A.0.14. *Seja $q = p^n$, onde p é um primo e $n \geq 1$. Então existe $\alpha \in \mathbb{F}_q$ tal que $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Além disso, o polinómio mínimo de α sobre $\mathbb{F}_p$ tem grau n.*

Demonstração. Para a existência de α, simplesmente consideramos *qualquer* gerador α do grupo multiplicativo $\mathbb{F}_q^\times$. Como todo o elemento não nulo de $\mathbb{F}_q$ é uma potência de α, resulta que $\mathbb{F}_q$ é gerado por α sobre $\mathbb{F}_p$, como pretendido!

Por outro lado, vimos no Exemplo A.0.2 que o grau $[\mathbb{F}_q : \mathbb{F}_p]$ é o grau do polinómio mínimo de α, o argumento da prova do Lema A.0.8 mostra que o grau $[\mathbb{F}_q : \mathbb{F}_p]$ é n. □

Note-se que resulta do corolário anterior o facto, interessante por si só, de que para qualquer inteiro positivo n existe um polinómio irredutível de grau n em $\mathbb{F}_p[X]$!

Isto mostra que o corpo $\mathbb{F}_q$ pode ser obtido a partir de $\mathbb{F}_p$ acrescentando uma raiz de um polinómio irredutível de grau n sobre $\mathbb{F}_p$, como fizemos para $q = 4$! Reciprocamente, dado qualquer polinómio irredutível de grau n sobre $\mathbb{F}_p$, podemos considerar a extensão $\mathbb{F}_p(\alpha)$ obtida acrescentando uma raiz α, que tem grau n sobre $\mathbb{F}_p$ e portanto tem $p^n = q$ elementos. A beleza do Teorema A.0.6 está em que, a menos de isomorfismo, vamos obter o mesmo corpo qualquer que seja o polinómio de grau n que escolhermos!

Exemplo A.0.15. Suponha-se que queremos construir explicitamente o corpo $\mathbb{F}_8$. Pode-se verificar que existem exatamente dois polinómios irredutíveis de grau 3 sobre $\mathbb{F}_2$, nomeadamente $X^3 + X + 1$ e $X^3 + X^2 + 1$. Podemos assim realizar $\mathbb{F}_8$ como sendo $\mathbb{F}_2(\alpha)$, onde α satisfaz

$$\alpha^3 + \alpha + 1 = 0.$$

Mas, embora não pareça à primeira vista, teríamos obtido o mesmo corpo se tivéssemos utilizado uma raiz de $X^3 + X^2 + 1$! Isto diz-nos em particular que $X^3 + X^2 + 1$ tem uma raiz em $\mathbb{F}_2(\alpha)$.

Essa raiz (uma dessas raízes, na verdade) é $1+\alpha$:

$$\begin{aligned}(1+\alpha)^3+(1+\alpha)^2+1 &= (1+\alpha+\alpha^2+\alpha^3)+(1+\alpha^2)+1\\ &= 1+\alpha+\alpha^3 = 0.\end{aligned}$$

Teoria de Galois de corpos finitos

Agora que já temos alguma familiaridade com corpos finitos, vamos ver como é que esses corpos encaixam uns nos outros. O resultado principal é o que se segue.

Proposição A.0.16. *Seja p um primo e sejam m e n inteiros positivos. Então o corpo $\mathbb{F}_{p^n}$ contém $\mathbb{F}_{p^m}$ como subcorpo (isto é, contém um subcorpo isomorfo a $\mathbb{F}_{p^m}$) se e só se m divide n. Além disso, se $m \mid n$ esse subcorpo isomorfo a $\mathbb{F}_{p^m}$ é único.*

Demonstração. Suponha-se primeiro que temos uma inclusão $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$. Pelo Facto A.0.3,

$$[\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] \cdot [\mathbb{F}_{p^m} : \mathbb{F}_p].$$

Mas pela Proposição A.0.14 temos $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ e $[\mathbb{F}_{p^m} : \mathbb{F}_p] = m$. Logo, da igualdade anterior resulta que m divide n.

Reciprocamente, suponha-se que m divide n. Então p^m-1 divide p^n-1. De facto, se $n = km$,

$$p^n - 1 = p^{km} - 1 = (p^m - 1)(1 + p^m + p^{2m} + \cdots + p^{(k-1)m}).$$

O mesmo argumento utilizado outra vez mostra que o polinómio $X^{p^m-1} - 1$ divide $X^{p^n-1} - 1$, e portanto

$$X^{p^m} - X \text{ divide } X^{p^n} - X.$$

Logo o corpo de fatorização de $X^{p^n} - X$ contém o corpo de fatorização de $X^{p^m} - X$. Isto diz-nos precisamente que $\mathbb{F}_{p^n}$ contém um subcorpo isomorfo a $\mathbb{F}_{p^m}$. Para ver que esse subcorpo é único, simplesmente observamos que qualquer elemento α de um tal subcorpo satisfaz $\alpha^{p^m} = \alpha$, e como tal há no máximo p^m elementos que podem pertencer a um tal subcorpo. □

Recordemos que uma extensão de corpos $L : K$ é *finita* se $[L : K] < \infty$.

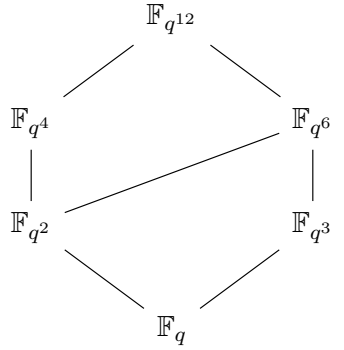
Corolário A.0.17. *Seja q uma potência de um primo. As extensões finitas de $\mathbb{F}_q$ são os corpos da forma $\mathbb{F}_{q^n}$, com n inteiro positivo, e tem-se $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. Além disso, $\mathbb{F}_{q^m}$ mergulha em $\mathbb{F}_{q^n}$ se e só se $m \mid n$, caso em que $\mathbb{F}_{q^m}$ é isomorfo a um único subcorpo de $\mathbb{F}_{q^n}$.*

Demonstração. Seja $q = p^k$, com p primo. As extensões finitas de $\mathbb{F}_q$ são corpos finitos de característica p e como tal são da forma $\mathbb{F}_{p^l}$, com l inteiro positivo. Queremos assim os valores de l para os quais $\mathbb{F}_{p^l}$ é uma extensão de $\mathbb{F}_{p^k}$; pela Proposição A.0.16 estes são os inteiros positivos da forma kn. Além disso, $\mathbb{F}_{p^{kn}} = \mathbb{F}_{q^n}$. Isto prova a primeira parte do Corolário. Note-se ainda que

$$[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{p^{kn}} : \mathbb{F}_{p^k}] = \frac{[\mathbb{F}_{p^{kn}} : \mathbb{F}_p]}{[\mathbb{F}_{p^k} : \mathbb{F}_p]} = \frac{kn}{k} = n.$$

O resto do corolário é uma consequência imediata da Proposição A.0.16, tendo em conta que km divide kn se e só se m divide n. □

O Corolário A.0.17 diz-nos de uma maneira muito explícita quais são as extensões (finitas) de um corpo finito e como se encaixam umas nas outras: esse "encaixe" é análogo à maneira como os números naturais se ordenam por divisibilidade. Isto pode ser formalizado: tanto as extensões de $\mathbb{F}_q$ ordenadas por inclusão como os números naturais ordenados por divisibilidade formam um *reticulado*, e esses reticulados são isomorfos. Vejamos por exemplo o aspeto do reticulado das extensões de $\mathbb{F}_q$ contidas em $\mathbb{F}_{q^{12}}$. Naturalmente, temos uma por cada divisor de 12.



É interessante analisar isto do ponto de vista da Teoria de Galois. Para isso vamos recordar algumas definições básicas.

Definição A.0.18. Seja K um corpo. Um *automorfismo* de K é uma função bijetiva $\sigma : K \to K$ tal que

$$\sigma(x+y) = \sigma(x) + \sigma(y) \quad \text{e} \quad \sigma(xy) = \sigma(x)\sigma(y) \quad \text{para quaisquer } x, y \in K.$$

Definição A.0.19. Seja $L : K$ uma extensão de corpos. O *grupo de Galois* $\mathrm{Gal}(L/K)$ é o grupo formado pelos automorfismos $\sigma : L \to L$ que fixam K ponto a ponto, isto é, tais que $\sigma(x) = x$ para todo o $x \in K$, com a operação de composição.

Pode-se provar que, para qualquer extensão finita $L : K$, se tem $|\mathrm{Gal}(L/K)| \leq [L : K]$; caso haja igualdade, a extensão diz-se uma *extensão de Galois*. Se $L : K$ é uma extensão finita de Galois, então há uma correspondência bijetiva natural

$$\{\text{extensões intermédias entre } L \text{ e } K\} \longleftrightarrow \{\text{subgrupos de } \mathrm{Gal}(L/K)\}.$$

Com isto em mente, vamos determinar o grupo de Galois de uma extensão de corpos finitos.

Lema A.0.20. *Seja q uma potência de um primo e seja n um inteiro positivo. Então o grupo* $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ *é cíclico, gerado pelo* automorfismo de Frobenius $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ *definido por*

$$\phi(x) = x^q \quad \textit{para todo o } x \in \mathbb{F}_{q^n}.$$

Este automorfismo tem ordem n, e portanto $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$.

Demonstração. Que ϕ é um automorfismo é uma consequência direta da Proposição A.0.9. Vejamos que ϕ tem ordem n:

- A composta $\underbrace{\phi \circ \cdots \circ \phi}_{n \text{ vezes}}$ envia x em x^{q^n}. Já observámos que $x^{q^n} = x$ para todo o $x \in \mathbb{F}_{q^n}$, logo $\underbrace{\phi \circ \cdots \circ \phi}_{n \text{ vezes}}$ é a identidade.

- Seja agora $0 < m < n$. A composta $\underbrace{\phi \circ \cdots \circ \phi}_{m \text{ vezes}}$ envia x em x^{q^m}. A equação $x^{q^m} = x$ tem no máximo $q^m < q^n$ soluções em $\mathbb{F}_{q^n}$, logo não é satisfeita por todo o $x \in \mathbb{F}_{q^n}$.

Isto mostra que ϕ tem ordem n. Assim o grupo cíclico gerado por ϕ tem n elementos e é isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Para concluir a prova, basta assim mostrar que $|\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)| \leq n$.

Para isso, seja α um gerador do grupo multiplicativo $\mathbb{F}_{q^n}^\times$. Então $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ e o polinómio mínimo de α sobre $\mathbb{F}_q$ tem grau n. Observemos que um elemento de $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ é determinado pela imagem de α, uma vez que todos os elementos não nulos de $\mathbb{F}_{q^n}$ são potências de α. Por outro lado, a imagem de α por um elemento de $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ é uma raiz do polinómio mínimo de α. De facto, se

$$f(X) = X^n + \cdots + a_1 X + a_0$$

é o polinómio mínimo de α, então $\alpha^n + \cdots + a_1\alpha + a_0 = 0$, e aplicando σ à igualdade anterior e usando que σ fixa $a_0, \ldots, a_{n-1}$ (por serem elementos de $\mathbb{F}_q$), obtemos

$$\sigma(\alpha)^n + \cdots + a_1\sigma(\alpha) + a_0 = 0.$$

Mas o polinómio mínimo de α tem no máximo n raízes em $\mathbb{F}_{q^n}$. Logo há no máximo n elementos de $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, terminando a prova. □

Vejamos os resultados do Corolário A.0.17 à luz deste lema. Como $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, o Lema A.0.20 diz-nos que $\mathbb{F}_{q^n} : \mathbb{F}_q$ é uma extensão de Galois, com grupo de Galois $\mathbb{Z}/n\mathbb{Z}$. Os subgrupos de $\mathbb{Z}/n\mathbb{Z}$ estão em correspondência com os divisores de n, tal como as extensões de $\mathbb{F}_q$ contidas em $\mathbb{F}_{q^n}$: é a Teoria de Galois a funcionar!

É importante salientar que é em grande parte a simplicidade da Teoria de Galois dos corpos finitos que os torna tão amigáveis, e *não* o facto de serem finitos: entre $\mathbb{F}_q$ e o fecho algébrico[3] $\overline{\mathbb{F}_q}$ (que pode ser pensado como o "limite" de todas as extensões finitas de $\mathbb{F}_q$) há toda uma teia de corpos intermédios K, mas entendemos perfeitamente como é que esses corpos se relacionam uns com os outros, há exatamente um com cada grau possível sobre $\mathbb{F}_q$, todos os grupos de Galois são cíclicos (e, em particular, abelianos)... toda esta simplicidade pode ser resumida dizendo que compreendemos o grupo de Galois $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, que rege toda esta teia. (Esse grupo pode ser pensado como o *limite inverso* dos grupos de Galois finitos $\mathbb{Z}/n\mathbb{Z}$ da mesma forma que $\mathbb{Z}_p$ é o limite inverso dos quocientes $\mathbb{Z}/p^k\mathbb{Z}$, e designa-se habitualmente por $\widehat{\mathbb{Z}}$, o *completamento profinito* de $\mathbb{Z}$.)

Por comparação, estamos muito longe de conseguir descrever de forma igualmente satisfatória as extensões de $\mathbb{Q}$; ninguém sabe muito bem o que é $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Lançar algumas luzes sobre ele é um dos objetivos do famoso *Programa de Langlands*.

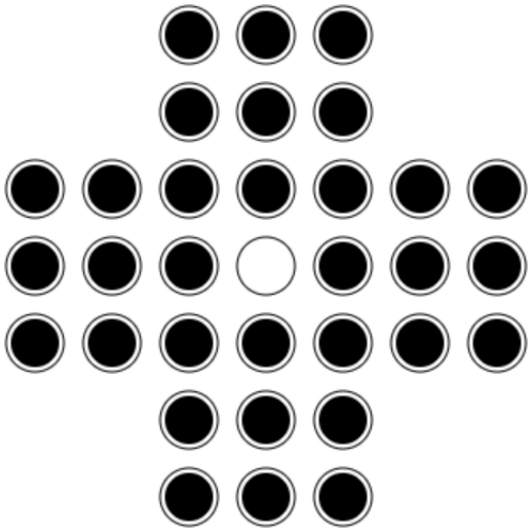
Aplicações

Para concluir este apêndice, vamos mostrar duas aplicações interessantes de corpos finitos. A primeira vem da Matemática Recreativa: está relacionada com o *solitário inglês*, um jogo cujas regras vamos descrever a seguir.

Suponha-se que temos uma configuração como a da figura a seguir, onde 33 buracos têm uma pedra e um, o buraco central, está vazio. Uma jogada permitida consiste em escolher uma pedra e, passando por cima de outra pedra adjacente, colocá-la numa casa vazia; a pedra por

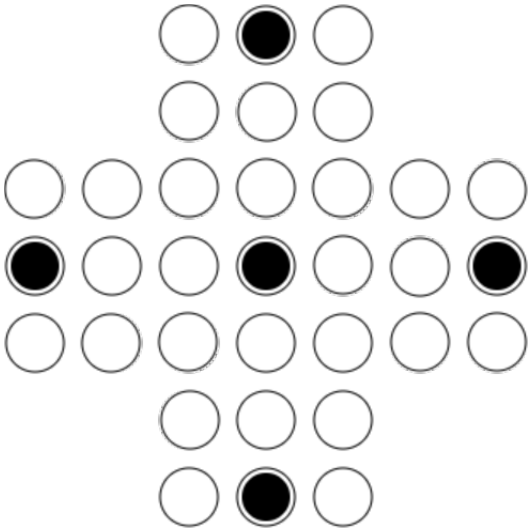
[3] O *fecho algébrico* de um corpo K é o menor corpo algebricamente fechado que contém K. Um corpo L é algebricamente fechado se todo o polinómio não constante com coeficientes em L tem um raiz em L.

cima da qual se passou é removida. O objetivo tradicional do solitário inglês é chegar a uma configuração em que todas as casas estejam vazias com exceção da casa central, que deve conter uma pedra.



A resolução do solitário tradicional fica como exercício para o leitor (mas asseguramos que é possível). É natural perguntarmo-nos se é possível resolver o puzzle análogo em que a pedra final deve ficar numa outra casa fixada à partida (não necessariamente a central).

Podemos ver de imediato que a resposta é sim. Vamos atribuir coordenadas às casas da maneira natural: a casa central é a casa $(0,0)$ e a primeira coordenada aumenta quando nos deslocamos para a direita, enquanto a segunda aumenta quando nos deslocamos para cima. Se podemos resolver o puzzle com o objetivo tradicional, então, na jogada imediatamente anterior à vitória, restam exatamente duas pedras; rodando se necessário o tabuleiro, podemos supor sem perda de generalidade que estas ocupam as casas $(1,0)$ e $(2,0)$. Mas, a partir desse estado, passando a pedra na casa $(1,0)$ por cima da pedra na casa $(2,0)$, obtemos uma única pedra na casa $(3,0)$. Portanto é possível colocar a pedra final na casa $(3,0)$. Por simetria, também podemos colocar a pedra final nas casas $(0,3)$, $(-3,0)$ e $(0,-3)$. As posições finais assinaladas na figura a seguir são, assim, possíveis.



A questão natural agora é se existem outras posições possíveis da pedra final. A resposta é não: isso foi provado por De Brujn em 1972 e, inesperadamente, a sua prova utiliza o corpo com 4 elementos, $\mathbb{F}_4$!

Recordemos que $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ onde $\alpha^2 + \alpha + 1 = 0$. Em cada momento do solitário, um certo conjunto X de casas contém uma pedra. Vamos associar a esse estado do jogo um elemento de $\mathbb{F}_4$ da seguinte forma: definimos

$$A(X) = \sum_{(x,y)\in X} \alpha^{x+y}.$$

Na posição inicial do jogo, temos:

n	número de casas ocupadas (x, y) com $x + y = n$
4	2
3	4
2	5
1	4
0	2
-1	4
-2	5
-3	4
-4	2

Portanto, se X é o conjunto de casas ocupadas inicialmente,

$$\begin{aligned} A(X) &= 2\alpha^4 + 4\alpha^3 + 5\alpha^2 + 4\alpha + 2 + 4\alpha^{-1} + 5\alpha^{-2} + 4\alpha^{-3} + 2\alpha^{-4} \\ &= \alpha^2 + \alpha^{-2} \\ &= \alpha^2 + \alpha = 1. \end{aligned}$$

Observe-se agora que, quando realizamos uma jogada, o valor de $A(X)$ não se altera. De facto, se X' é obtido a partir de X por uma jogada, por simetria podemos supor sem perda de generalidade que as duas pedras envolvidas na jogada estão numa mesma fila horizontal, digamos em casas (x, y) e $(x + 1, y)$. Essas casas deixam de ter pedras, e a casa $(x - 1, y)$ ou $(x + 2, y)$ passa a ter uma pedra; suponhamos que temos o segundo caso, o primeiro pode ser tratado de maneira análoga. Então

$$A(X') - A(X) = \alpha^{x+2+y} - \alpha^{x+1+y} - \alpha^{x+y} = \alpha^{x+y}(\alpha^2 + \alpha + 1) = 0,$$

como pretendido.

Como o valor de $A(X)$ não se altera ao longo do jogo, em qualquer momento do jogo temos $A(X) = 1$. Se (a, b) são as coordenadas da casa que contém a pedra final, devemos então ter $\alpha^{a+b} = 1$. Como α tem ordem 3 no grupo multiplicativo $\mathbb{F}_4^\times$, $a + b$ é divisível por 3.

Por outro lado, podemos também definir

$$B(X) = \sum_{(x,y)\in X} \alpha^{x-y}$$

e o mesmo raciocínio mostra que o valor de $B(X)$ é inicialmente igual a 1 e não se altera ao longo do jogo. Portanto também devemos ter $\alpha^{a-b} = 1$, e $a - b$ é divisível por 3.

Resulta que a e b são ambos divisíveis por 3, e portanto a casa final (a, b) é $(0, 0)$, $(3, 0)$, $(0, 3)$, $(-3, 0)$ ou $(0, -3)$, como pretendido!

O próximo exemplo que vamos apresentar tem a ver com o problema clássico de determinar se um inteiro é um quadrado módulo p, para um primo p. Especificamente, vamos concentrar-nos no caso em que esse inteiro é 2, e tentar responder à seguinte questão:

> Para que primos $p > 2$ é que a congruência $x^2 \equiv 2 \pmod{p}$ tem uma solução inteira?

Por outras palavras, queremos determinar os primos $p > 2$ para os quais a equação $x^2 = 2$ tem uma solução em $\mathbb{F}_p$. Notemos que uma solução desta equação existe sempre, porventura numa extensão de $\mathbb{F}_p$ (em $\mathbb{F}_{p^2}$, de facto). A questão é saber quando é que essa solução pertence a $\mathbb{F}_p$.

Para isso, vamos considerar uma oitava raiz primitiva da unidade, digamos, ζ_8; esta não existe necessariamente em $\mathbb{F}_p$, mas existe em alguma extensão. Uma maneira de ver isso é observando que uma raiz do polinómio $X^4 + 1$ é necessariamente uma oitava raiz primitiva da unidade, e esse polinómio tem uma raiz numa extensão finita de $\mathbb{F}_p$, por exemplo em $\mathbb{F}_{p^4}$ se o polinómio $X^4 + 1$ for irredutível em $\mathbb{F}_p[X]$ (de facto pode-se verificar que uma tal raiz pertence sempre a $\mathbb{F}_{p^4}$, mas isso não é necessário).

Pensemos em $\tau = \zeta_8 + \zeta_8^{-1}$. Temos

$$\tau^2 = \zeta_8^2 + \zeta_8^{-2} + 2 = 2$$

uma vez que, sendo $\zeta_8^4 = -1$, se tem $\zeta_8^2 + \zeta_8^{-2} = 0$. Ou seja, τ é uma raiz quadrada de 2 numa extensão de $\mathbb{F}_p$! E tudo o que temos de fazer é descobrir quando é que $\tau \in \mathbb{F}_p$.

Como testar se um elemento de $\overline{\mathbb{F}_p}$ pertence a $\mathbb{F}_p$? Há um teste simples a que podemos submetê-lo: temos $x \in \mathbb{F}_p$ se e só se $x^p = x$. De facto, isto é verdade para $x \in \mathbb{F}_p$, e é verdade para no máximo p valores de x, portanto não pode ser verdade para nenhum valor de x para além dos p elementos de $\mathbb{F}_p$.

Ora, temos, pela Proposição A.0.9,

$$\tau^p = (\zeta_8 + \zeta_8^{-1})^p = \zeta_8^p + \zeta_8^{-p} = \begin{cases} \zeta_8 + \zeta_8^{-1} & \text{se } p \equiv 1, 7 \pmod{8} \\ \zeta_8^3 + \zeta_8^{-3} & \text{se } p \equiv 3, 5 \pmod{8} \end{cases}.$$

Mas temos $\zeta_8 + \zeta_8^{-1} + \zeta_8^3 + \zeta_8^{-3} = 0$, uma vez que $\zeta_8 = -\zeta_8^{-3}$ e $\zeta_8^3 = -\zeta_8^{-1}$ (isto decorre de ζ_8 ser raiz de $X^4 + 1$). Portanto $\zeta_8^3 + \zeta_8^{-3} = -\tau$, e obtemos que

$$\tau^p = \begin{cases} \tau & \text{se } p \equiv 1, 7 \pmod{8} \\ -\tau & \text{se } p \equiv 3, 5 \pmod{8} \end{cases}.$$

Em particular, tem-se $\tau^p = \tau$ precisamente quando $p \equiv 1, 7 \pmod{8}$. Ou seja, a congruência $x^2 \equiv 2 \pmod{p}$ tem solução precisamente quando $p \equiv 1 \pmod{8}$ ou $p \equiv 7 \pmod{8}$!