TEORIA ALGÉBRICA DOS NUMEROS

MURILO CORATO ZANARELLA

19 de Agosto de 2019

1. Anéis e Corpos

1.1. **Generalidades.** Queremos analisar a aritimética de "coisas" como $\mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\omega]$ ao mesmo tempo. Para isso, é útil ter um pouco de vocabulário:

Definição 1. Um *anel* (comutativo) $(R, +, \cdot)$ é um, conjunto R munido de operações associativas e comutativas $+$ e $\cdot$ satisfazendo:

- (elemento neutro de $+$) existe $0 \in R$ tal que $a + 0 = 0 + a = a$ para todo $a \in R$,
- (inverso de $+$) para todo $a \in R$, existe $(-a) \in R$ tal que $a + (-a) = (-a) + a = 0$,
- (elemento neutro de $\cdot$) existe $1 \in R$ tal que $a \cdot 1 = 1 \cdot a = a$ para todo $a \in R$,
- (distributiva) para todos $a, b, c \in R$, temos $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(a + b) \cdot c = a \cdot c + b \cdot c$.

Exemplo 2. $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}[X]$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}[1/2] = \{\frac{a}{2^i} \colon a \in \mathbb{Z}, i \geq 0\}$, $\{f \colon [0,1] \to \mathbb{R}\}$ (com soma e multiplicação ponto a ponto), $\mathbb{Z}[\epsilon] = \{a + b\epsilon \colon a, b \in \mathbb{Z}\}$ onde $\epsilon \cdot \epsilon = 0$.

Definição 3. Um anel $(R, +, \cdot)$ é um *corpo* se $1 \neq 0$ e se também satisfaz

- (inverso de $\cdot$) para todo $0 \neq a \in R$, existe $a^{-1} \in R$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Exemplo 4. $\mathbb{Q}, \mathbb{Q}[i], \mathbb{Z}/p\mathbb{Z}$ para p primo, $\mathbb{Q}((X)) = \{\sum_{i=-M}^{\infty} a_i X^i \colon a_i \in \mathbb{Q}\}$.

Nós sabemos que temos fatoração única em $R = \mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\omega], \mathbb{Q}[X]$, mas o que isso significa exatamente? Em todos esses casos, temos a noção de elementos primos, e todo elemento de R é descrito como um produto único de primos a menos ordenação e de multiplicação por "algo": em $\mathbb{Z}$, a menos de ± 1; em $\mathbb{Z}[i]$, de $\pm 1, \pm i$; em $\mathbb{Z}[\omega]$, de $\pm 1, \pm\omega, \pm\omega^2$; em $\mathbb{Q}[X]$, a menos de $\mathbb{Q}^\times$. Uma descrição de o que é "algo" motiva a seguinte definição:

Definição 5. As *unidades* de um anel R, denotadas por $R^\times$, são os elementos $a \in R$ que possuem inverso multiplicativo.

Exemplo 6. $\mathbb{Z}/n\mathbb{Z}^\times = \{a \in \mathbb{Z}/n\mathbb{Z} \colon \text{mdc}(a,n) = 1\}$, $\mathbb{Z}[\frac{1}{2}]^\times = \{\pm 2^i \colon i \in \mathbb{Z}\}$ e também $\mathbb{Z}[\epsilon]^\times = \{\pm 1 + a\epsilon \colon a \in \mathbb{Z}\}$.

Exemplo 7. Um anel R é um corpo se e somente se $R^\times = R \setminus \{0\}$.

Por fim, o que é um "primo" em geral? Em $\mathbb{Z}$, podem ser definidos de duas formas:

(1) p possui exatamente quatro divisores: $\pm 1, \pm p$,

(2) $p \neq 0, \pm 1$, e se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Adaptando essas definições, temos:

Definição 8. Um elemento $a \in R$ que não é 0 e nem uma unidade é *irredutível* se $a = bc$ implica que b ou c é uma unidade.

Definição 9. Um elemento $a \in R$ que não é 0 e nem uma unidade é *primo* se $a \mid bc$ implica $a \mid b$ ou $a \mid c$.

Não é verdade que, em geral, essas duas definições são equivalentes.

1.2. **Corpos numéricos e Anéis de inteiros.**

Lema 10. *Se $f(X) \in \mathbb{Z}[X]$ (mônico) tem raízes $\alpha_1, \ldots, \alpha_n$, e $g(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$, então $g(\alpha_1, \ldots, \alpha_n)$ é raiz de um polinômio (mônico) inteiro.*

Demonstração. Seja $F(X) = \prod_{\sigma \in S_n} (X - g(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}))$. Os coeficientes de F são polinômios simétricos em $\alpha_1, \ldots, \alpha_n$. Como os polinômios simétricos elementares de α_i são inteiros (são $\pm$ os coeficientes de f), isso implica que $F(X) \in \mathbb{Z}[X]$. □

Corolário 11. *$\mathcal{O} = \{\alpha \colon f(\alpha) = 0$ para algum $f \in \mathbb{Z}[X]$ mônico$\}$ é um anel.*

Demonstração. Sejam $\alpha_1, \alpha_2 \in \mathcal{O}$, e seja $f(X) \in \mathbb{Z}[X]$ um polinômio mônico onde α_1 e α_2 são raízes. Escolhendo $g(X_1, \ldots, X_n) = X_1 + X_2$ ou $g(X_1, \ldots, X_n) = X_1 \cdot X_2$ mostra que $\alpha_1 + \alpha_2 \in \mathcal{O}$ e $\alpha_1 \cdot \alpha_2 \in \mathcal{O}$. □

Corolário 12. *$\overline{\mathbb{Q}} = \{\alpha \colon f(\alpha) = 0$ para algum $0 \neq f \in \mathbb{Q}[X]\}$ é um corpo.*

Demonstração. A mesma prova acima mostra que $\overline{\mathbb{Q}}$ é um anel. Seja $0 \neq \alpha \in \overline{\mathbb{Q}}$, e seja $f(X) \in \mathbb{Q}[X]$ seu polinômio minimal mônico. Se β é o produto das raízes de f diferentes de α, temos que $\alpha \cdot \beta = (-1)^{\deg(f)} f(0) \in \mathbb{Q}$. Como $\beta \in \overline{\mathbb{Q}}$, o inverso de α é $(-1)^{\deg(f)} f(0)^{-1} \cdot \beta \in \overline{\mathbb{Q}}$. □

Definição 13. Um *corpo numérico* K é um corpo da forma $K = \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ para $\alpha_i \in \overline{\mathbb{Q}}$. O *anel de inteiros* de K é $\mathcal{O}_K = K \cap \mathcal{O}$.

Por que tais K formam um corpo? Vamos provar isso para $n = 1$ (o caso geral segue por indução). Seja $f(x) \in \mathbb{Z}[x]$ é o polinómio minimal de α. Se $\beta \in K$, podemos escolher $g(x) \in \mathbb{Z}[x]$ com $g(\alpha) = \beta$. Se $\beta \neq 0$, temos que $f(x) \nmid g(x)$, e portanto por Bezout temos $a(x)f(x)+b(x)g(x) = 1$ para algum $a(x), b(x) \in \mathbb{Q}[x]$. Tomando $x = \alpha$ temos $a(\alpha)\beta = 1$, e portanto β possui um inverso.

Exemplo 14. $\mathbb{Z} \subset \mathbb{Q}$, $\mathbb{Z}[i] \subset \mathbb{Q}[i]$, $\mathbb{Z}[2^{1/3}] \subset \mathbb{Q}[2^{1/3}]$, $\mathbb{Z}\left[\frac{1+10^{1/3}+10^{2/3}}{3}\right] \subset \mathbb{Q}[10^{1/3}]$.

1.3. **Corpos Finitos.** Corpos finitos são simples de descrever. Vamos provar que todos os corpos finitos tem tamanho uma potência de primo, e que existe um único corpo de cada um desses tamanhos.

Lema 15. *Se K é um corpo finito, então existe um único primo p tal que $p = 0$ em K.*

Demonstração. Como K é finito, existe um inteiro $n > 1$ com $n = 0$ em K. Se $n = n_0 p$ é o menor tal n para um primo p e $n_0 > 1$, não podemos ter um inverso pra p. De fato, se $px = 1$, teríamos $0 = 0 \cdot x = n_0 px = n_0 \cdot 1 = n_0$. Portanto tal menor n tem que ser primo.

Agora é fácil ver que os $n \in \mathbb{Z}$ com $n = 0$ em K são exatamente os múltiplos de p. □

Corolário 16. *Se K é um corpo finito, $\#K = p^l$ para uma potência de primo p^l.*

Demonstração. Pelo lema acima, podemos ver K como um espaço vetorial sobre $\mathbb{F}_p$. □

Teorema 17. *Se K é o um corpo finito, então $\#K = p^l$ e K é isomorfo a um corpo da forma $\mathbb{F}_{p^l} = \{x \in \overline{\mathbb{F}_p} \colon x^{p^l} - x = 0\}$.*

Demonstração. Por Lagrange (ou seguindo a prova do pequeno teorema de Fermat), temos que se $x \in K$, então $x^{p^l} = x$. Como $x^{p^l} - x$ tem no máximo p^l raízes in $\overline{\mathbb{F}_p}$, e todos os elementos de K são raízes, então elas são todas as raízes. □

Proposição 18. *$\mathbb{F}_{p^l}$ tem uma raiz primitiva.*

Demonstração. Seja $a \in \mathbb{F}_{p^l}$ um elemento com ordem d. Então temos exatamente $\phi(d)$ elementos com ordem d, pois $1, a, a^2, \ldots, a^{d-1}$ são exatamente as raízes de $x^d = 1$.

Se N_d é a quantidade de elementos de ordem d, então temos $\sum_{d|p^l-1} N_d = p^l$, e temos ou $N_d = 0$ ou $N_d = \phi(d)$. Como $\sum_{d|p^l-1} \phi(d) = p^l - 1$, isso implica que $N_d = \phi(d)$. Portanto $N_{p^l-1} = \phi(p^l - 1)$ e existe uma raiz primitiva. □

Teorema 19. *Os automorfismos de* $\mathbb{F}_{p^l}$ *são dados por* $x \mapsto x^{p^k}$ *para* $k = 0, \dots, l-1$. *Em particular, eles são todos repetidas composições de* $x \mapsto x^p$, *e esse mapa é chamado de* elemento de Frobenius.

Demonstração. Um automorfismo de $\mathbb{F}_{p^l}$ é determinados pela imagem de uma raiz primitiva g. Mas se $f(x) \in \mathbb{F}_p[x]$ é o polinômio minimal de g, temos $\mathbb{F}_{p^l} \simeq \mathbb{F}_p[x]/f(x)$ e portanto que $\deg f = l$. Logo temos no máximo l automorfismos, pois a imagem de g é uma raiz de f. Mas já temos l autoformismos do enunciado, e portanto eles são todos. □

Exemplo 20. Se $p \equiv 3 \mod 4$ é um primo, $\mathbb{Z}[i]/p\mathbb{Z}[i]$ é isoformo a $\mathbb{F}_{p^2}$ e nesse corpo temos $(a+bi)^p = a^p + (bi)^p = a + bi^p = a - bi$, portanto a ação do Frobenius é simplesmente conjugação.

2. Ideais

2.1. **Generalidades.** Para estudar os inteiros, é muito importante considerar também os anéis $\mathbb{Z}/n\mathbb{Z}$. Essa construção de "olhar módulo n" pode ser feito em qualquer anel.

Definição 1. Se $a \in R$, podemos considerar o anel R/aR, onde identificamos $b \in R$ e $c \in R$ se $a \mid b - c$.

Em $\mathbb{Z}$, Bezout diz que olhar módulo n e m é o mesmo que olhar módulo $\mathrm{mdc}(n, m)$. Isso não necessariamente é verdade em outros anéis: em $R = \mathbb{Z}[X]$, podemos olhar módulo 2 e módulo X^2, obtendo o anel $\mathbb{Z}[X]/(2, X^2) = \mathbb{Z}/2\mathbb{Z} \oplus X \cdot \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2[\epsilon]$, e isso não pode ser obtido como R/aR para nenhum $a \in R$. Ideais são "as coisas que podem ser módulos".

Definição 2. Um *ideal* $\mathfrak{a}$ de R é um subconjunto de R tal que:

- se $a, b \in \mathfrak{a}$, então $a + b \in \mathfrak{a}$,
- se $a \in \mathfrak{a}$ e $b \in R$, então $a \cdot b \in \mathfrak{a}$.

Exemplo 3. $\{0\}$ e R são ideais para qualquer R, e também: $n\mathbb{Z} \subset \mathbb{Z}$, $2\mathbb{Z}[X] + X^2\mathbb{Z}[X] \subset \mathbb{Z}[X]$, e $\{f\colon [0,1] \to \mathbb{R}\colon f(0) = 0\} \subset \{f\colon [0,1] \to \mathbb{R}\}$.

Exemplo 4. R é um corpo se e somente se seus únicos ideais são $\{0\}$ e R.

Proposição 5. *Se $\mathfrak{a}$ é um ideal de R, podemos considerar o anel $R/\mathfrak{a}$, onde identificamos $b \in R$ e $c \in R$ se $b - c \in \mathfrak{a}$.*

Demonstração. A parte difícil é ver que soma e multiplicação são bem definidas. De fato, se $a - a' = x \in \mathfrak{a}$ e $b - b' = y \in \mathfrak{a}$ temos $(a + b) - (a' + b') = x + y \in \mathfrak{a}$, logo $a + b$ é bem definido, e também que $ab - a'b' = xb + a'y \in \mathfrak{a}$, logo ab é bem definido. □

Note que isso recupera a definição anterior, tomando $\mathfrak{a} = aR$. Chamamos tais ideais de *principais*. Também denotamos $(a_1, \ldots, a_n)$ o ideal gerado por $a_1, \ldots, a_n$, e chamamos tais ideais de *finitamente gerados*.

Proposição 6. *Em $R = \mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\omega]$, todo ideal é principal.*

Demonstração. Essa prova é essencialmente a prova de Bezout. Seja $\{0\} \neq \mathfrak{a} \subset R$ um ideal. Temos uma norma em R, e esses três anéis satisfazem divisão euclideana com tal norma. Seja $a \in \mathfrak{a}$ um elemento de menor norma. Então se $b \in \mathfrak{a}$ e $b = aq + r$ é a divisão euclideana, temos que

$r = b - aq \in \mathfrak{a}$. Mas como $a \in \mathfrak{a}$ é o elemento de menor norma, isso implica $r = 0$. Logo $b \in aR$, e portanto $\mathfrak{a} = aR$. □

Isso não é verdade para todo $\mathcal{O}_K$.

A utilidade de ideais é que mesmo quando $\mathcal{O}_K$ não possui fatoração única, $\mathcal{O}_K$ possui fatoração única *em ideais primos*. Para falar de fatoração, precisamos ter a noção de primos, mas primeiro a noção de multiplicação.

Definição 7. Se $\mathfrak{a}, \mathfrak{b} \subseteq R$ são ideais, então também temos os ideais

- $\mathfrak{a} + \mathfrak{b} := \{a + b \colon a \in \mathfrak{a},\ b \in \mathfrak{b}\}$.
- $\mathfrak{ab} := \{\sum_{i=1}^{n} a_i b_i \colon n \in \mathbb{Z}_{>0} \text{ e } a_i \in \mathfrak{a},\ b_i \in \mathfrak{b}\}$.

Nota 8. Se $R = \mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\omega]$ ou $\mathbb{Q}[x]$ então $(a) + (b) = (\mathrm{mdc}(a, b))$.

Podemos considerar noções (quase) análogas a *primo* e *irredutível* para ideais:

Definição 9. Um ideal $\mathfrak{a} \subseteq R$ é dito *primo* se $\mathfrak{a} \neq R$ e se $ab \in \mathfrak{a}$ implica $a \in \mathfrak{a}$ ou $b \in \mathfrak{a}$.

Definição 10. Um ideal $\mathfrak{a} \subseteq R$ é dito *maximal* se $\mathfrak{a} \neq R$ e se sempre que um ideal $\mathfrak{b}$ contém $\mathfrak{a}$, então ou $\mathfrak{b} = \mathfrak{a}$ ou $\mathfrak{b} = R$.

Lema 11. *Seja R um anel e $\mathfrak{a}$ um ideal de R. Então temos uma bijeção*

$$\{\textit{ideais de } R \textit{ contendo } \mathfrak{a}\} \longleftrightarrow \{\textit{ideais de } R/\mathfrak{a}\}.$$

Demonstração. Dado um ideal $\mathfrak{b} \supseteq \mathfrak{a}$, ele claramente nos dá um ideal $\mathfrak{b}'$ de $R/\mathfrak{a}$.

Dado um ideal $\mathfrak{b}'$ de $R/\mathfrak{a}$, considere o conjunto $\mathfrak{b} = \{b \in R \colon b \mod \mathfrak{a} \in \mathfrak{b}'\}$. É fácil ver que $\mathfrak{b}$ é um ideal.

Basta notar agora que essas duas operações são inversas. □

Corolário 12. *Um ideal $\mathfrak{a} \subseteq R$ é maximal se e somente se $R/\mathfrak{a}$ é um corpo.*

Demonstração. Pelo lema, os ideais que contém $\mathfrak{a}$ estão em bijeção aos ideais de $R/\mathfrak{a}$. $\mathfrak{a}$ é maximal se e somente se existem exatamente dois tais ideais, e $R/\mathfrak{a}$ é um corpo se e somente se também existem exatamente dois tais ideais. □

Corolário 13. *Se $\mathfrak{a} \subseteq R$ é maximal, então também é primo.*

Demonstração. Considere $ab \in \mathfrak{a}$. Como $R/\mathfrak{a}$ é um corpo e temos $ab = 0$ em $R/\mathfrak{a}$, isso significa que $a = 0$ ou $b = 0$ em $R/\mathfrak{a}$, ou seja, que $a \in \mathfrak{a}$ ou $b \in \mathfrak{a}$. □

Um exemplo de como podemos resolver problemas com fatoração única em ideais primos:

Exemplo 14. Vamos resolver $2y^3 = x^2 + 5$. Para $K = \mathbb{Q}[\sqrt{-5}]$, podemos fatorar em K: $2y^3 = (x + \sqrt{-5})(x - \sqrt{-5})$. Agora podemos fazer o mdc como de costume, mas em ideais. Seja $\mathfrak{a}_1 = (x + \sqrt{-5})$ e $\mathfrak{a}_2 = (x - \sqrt{-5})$. Se $\mathfrak{b} = \text{mdc}(\mathfrak{a}_1, \mathfrak{a}_2)$, então $\mathfrak{b} \mid (2\sqrt{-5})$. Acontece que $\sqrt{-5}$ é primo, e que $2 = (2, 1+\sqrt{-5})^2$. Como $\sqrt{-5} \nmid x+\sqrt{-5}$ (pois $5 \nmid x$) e $2 \nmid x+\sqrt{-5}$, temos que $\mathfrak{b} \mid (2, 1+\sqrt{-5})$. Isso significa que $\mathfrak{a}_1 = (2, 1 + \sqrt{-5})(\mathfrak{a}_1')^3$ para algum ideal $\mathfrak{a}_1'$. Multiplicando por 2, temos $2\mathfrak{a}_1 = ((2, 1 + \sqrt{-5})\mathfrak{a}_1')^3$. Como $\mathfrak{a}_1$ é principal, $((2, 1 + \sqrt{-5})\mathfrak{a}_1')^3$ também é. Uma análise dos ideais em $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ (a teoria de *grupos de classes* que veremos em breve) mostra que $(2, 1 + \sqrt{-5})\mathfrak{a}_1'$ também é principal, digamos igual a $(a + b\sqrt{-5})$. Isso significa que $2x + 2\sqrt{-5} = \pm(a + b\sqrt{-5})^3$ para algum $a, b \in \mathbb{Z}$. Então $\pm 2 = b(3a^2 - 5b^2)$, e uma análise dos casos chega na única possibilidade de $x = \pm 7$, $y = 3$.

2.2. **Primeiros passos para fatoração única.** O plano para provar fatoração única em ideais primos é o sequinte:

(1) $\mathfrak{a}$ está contido em um ideal maximal $\mathfrak{p}$. (análogo de existe p com $p \mid a$)
(2) Podemos "dividir" por $\mathfrak{p}$, isto é, escrever $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$,
(3) Repetindo o processo acima, queremos usar uma noção de "tamanho" para argumentar que o processo termina. Isso prova que $\mathfrak{a}$ pode ser fatorado em ideais maximais.
(4) Usando que ideais primos = ideais maximais, provaremos que a fatoração é única.

Vamos começar o plano acima. Iremos provar (1), introduzir o "tamanho" de um ideal $N(\mathfrak{a})$, e provaremos que primo = maximal.

Lema 15. *Qualquer ideal $\{0\} \neq \mathfrak{a} \subseteq \mathcal{O}_K$ pode ser escrito como $\mathfrak{a} = \alpha_1\mathbb{Z} \oplus \cdots \alpha_n\mathbb{Z}$ onde $n = [K : \mathbb{Q}]$. Em particular, $\mathfrak{a}$ é finitamente gerado.*

Demonstração. Seja $x_1, \ldots, x_n$ uma base de K sobre $\mathbb{Q}$. Isso significa que temos $K = \mathbb{Q}x_1 \oplus \cdots \oplus \mathbb{Q}x_n$. Podemos assumir que todos os $x_i \in \mathcal{O}_K$. Então temos que $\det(\text{Tr}(x_i x_j)) \neq 0$. Se fosse 0, então teríamos um $k \in K^\times$ tal que $\text{Tr}(x_i k) = 0$ para todo x_i. Isso significa que $\text{Tr}(k'k) = 0$ para todo $k' \in K$. Em particular, teríamos $\text{Tr}(1) = 0$, o que não é verdade. Então podemos achar $y_i \in K$ com $\text{Tr}(x_i y_j) = \delta_i^j$.

Seja $p_i\colon K \to \mathbb{Q}$ a projeção no i-ésimo fator. Então $p_i(\alpha) = \mathrm{Tr}(\alpha y_i)$. Se $d_i \in \mathbb{Z}$ é tal que $d_i y_i \in \mathcal{O}_K$, então isso significa que $d_i p_i(\alpha) \in \mathbb{Z}$. Agora $d_1 p_1(\mathfrak{a}) \subset \mathbb{Z}$ é um ideal, e então podemos escolher $\alpha_1 \in \mathfrak{a}$ tal que $d_1 p_1(\alpha_1)$ gere o ideal. Então agora para todo elemento $a \in \mathfrak{a}$, existe um único $a_1 \in \mathbb{Z}$ tal que $p_1(a - a_1\alpha_1) = 0$. Agora olhe para $d_2 p_2(a - a_1\alpha_1) \in \mathbb{Z}$ para todo $a \in \mathfrak{a}$. Isso gera um ideal, e podemos escolher α_2 tal que tal $d_2 p_2(\alpha_2)$ gere o ideal e que $p_1(\alpha_2) = 0$. Continuando dessa forma, temos que $\mathfrak{a} = \alpha_1\mathbb{Z} \oplus \cdots \alpha_n\mathbb{Z}$. □

Definição 16. $\mathcal{O}_K = \alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z}$ para algum $\alpha_1, \ldots, \alpha_n$. Tais α_i são chamados de uma *base integral*. O determinante $D_K = \det(\mathrm{Tr}(\alpha_i\alpha_j))$ considerado na prova acima é chamado de o *discriminante* de K.

Exemplo 17. Seja $K = \mathbb{Q}[\sqrt{d}]$ com d livre de quadrados. Se $d \not\equiv 1 \mod 4$, temos que $\{1, \sqrt{d}\}$ é uma base integral de $\mathcal{O}_K$, e portanto que $D_K = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{d}) \\ \mathrm{Tr}(\sqrt{d}) & \mathrm{Tr}(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d$. Se $d \equiv 1 \mod 4$, temos que $\{1, \frac{1+\sqrt{d}}{2}\}$ é uma base integral de $\mathcal{O}_K$, e portanto que $D_K = \det \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\frac{1+\sqrt{d}}{2}) \\ \mathrm{Tr}(\frac{1+\sqrt{d}}{2}) & \mathrm{Tr}(\frac{d+1+2\sqrt{d}}{4}) \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{pmatrix} = d$.

Teorema 18. *Se $\{0\} \neq \mathfrak{a} \subseteq \mathcal{O}_K$ é um ideal, então $N(\mathfrak{a}) := \#(\mathcal{O}_K/\mathfrak{a})$ é finito.*

Demonstração. Seja $\alpha \in \mathfrak{a}$. Basta provarmos que $\mathcal{O}_K/\alpha\mathcal{O}_K$ é finito. De fato, vamos provar que $\#\mathcal{O}_K/\alpha\mathcal{O}_K = |\mathrm{Nm}(\alpha)|$. Se α_i é uma base integral, então $\alpha\alpha_i$ é uma base do lattice $\alpha\mathcal{O}_K$ dentro do lattice $\mathcal{O}_K = \mathbb{Z}^n$. Pela definição de determinante, $|\mathrm{Nm}(\alpha)|$ é o volume de uma região fundamental. Isso também é $\#\mathcal{O}_K/\alpha\mathcal{O}_K$. □

Corolário 19. *Seja $\{0\} \neq \mathfrak{a} \subseteq \mathcal{O}_K$ um ideal com $\mathfrak{a} \neq \mathcal{O}_K$. Então existe um ideal maximal $\mathfrak{p}$ com $\mathfrak{a} \subseteq \mathfrak{p}$.*

Demonstração. Como $\mathcal{O}_K/\mathfrak{a}$ é finito, tem um ideal maximal $\mathfrak{p}'$. Isso nos dá um ideal maximal pelo Lema 11. □

Teorema 20. *Um ideal $\{0\} \neq \mathfrak{p} \subseteq \mathcal{O}_K$ é primo se e somente se é maximal.*

Demonstração. Assuma $\mathfrak{p}$ é primo. Queremos provar que $\mathcal{O}_K/\mathfrak{p}$ é um corpo, ou seja, que $\alpha \notin \mathfrak{p}$ tem um inverso em $\mathcal{O}_K/\mathfrak{p}$. O mapa : $\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_K/\mathfrak{p}$ dado por $x \mapsto \alpha x$ é injetor pois $\mathfrak{p}$ é primo. Mas $\mathcal{O}_K/\mathfrak{p}$ é finito, então por gira-gira α tem um inverso. □

3. Fatoraçao única

3.1. **Término da prova de fatoração única.** Lembrando do nosso plano, para qualquer ideal $\mathfrak{a} \neq \{0\}$, temos um ideal primo $\mathfrak{p}$ com $\mathfrak{a} \subseteq \mathfrak{p}$ (o que é o análogo de $p \mid a$). Então agora queremos poder "dividir" por $\mathfrak{p}$, isso é, escrever $\mathfrak{a} = \mathfrak{b}\mathfrak{p}$.

Definição 1. Seja $\{0\} \neq \mathfrak{p} \subset \mathcal{O}_K$ um ideal primo. Denote $\mathfrak{p}^{-1} = \{\alpha \in K \colon \alpha\mathfrak{p} \subseteq \mathcal{O}_K\} \subseteq K$.

Para $K = \mathbb{Q}$ e $\mathfrak{p} = p\mathbb{Z}$, temos $\mathfrak{p}^{-1} = \frac{1}{p}\mathbb{Z}$. Queremos ter $\mathfrak{b} = \mathfrak{a}\mathfrak{p}^{-1}$, então temos que provar que $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.

Lema 2. *Seja $\{0\} \neq \mathfrak{a} \subseteq \mathcal{O}_K$ um ideal. Se $\alpha \in K$ é tal que $\alpha\mathfrak{a} \subseteq \mathfrak{a}$, então $\alpha \in \mathcal{O}_K$.*

Demonstração. Escreva $\mathfrak{a} = \alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z}$. Como $\alpha\mathfrak{a} \subseteq \mathfrak{a}$, temos $\alpha\alpha_i = \sum_j a_{ij}\alpha_j$ para certos $a_{i,j} \in \mathbb{Z}$. Então

$$\begin{pmatrix} a_{1,1} - \alpha & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} - \alpha & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} - \alpha \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = 0,$$

logo o determinante da matrix é 0. Mas isso implicaria que $\alpha \in \mathcal{O}_K$, pois tal determinante é um polinômio mônico de coeficientes inteiros em α. □

Teorema 3. *Seja $\{0\} \neq \mathfrak{p} \subset \mathcal{O}_K$ um ideal primo. Então $\mathfrak{p}^{-1} \neq \mathcal{O}_K$ e $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.*

Demonstração. Pela definição de $\mathfrak{p}^{-1}$, temos que $\mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$ é um ideal. Como $\mathcal{O}_K \subseteq \mathfrak{p}^{-1}$, temos que $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1}$. Como $\mathfrak{p}$ é maximal, isso implica que $\mathfrak{p}\mathfrak{p}^{-1}$ só pode ser $\mathcal{O}_K$ ou $\mathfrak{p}$.

Primeiro vamos achar $\alpha \in \mathfrak{p}^{-1} \setminus \mathcal{O}_K$. Escolha $0 \neq \beta \in \mathfrak{p}$, e considere ideais primos $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ tal que $(\beta) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$ com r mínimo. Como $\mathfrak{p}$ é um ideal primo, o fato de que $(\beta) \subseteq \mathfrak{p}$ implica que $\mathfrak{p}_i \subseteq \mathfrak{p}$ para algum i. Mas $\mathfrak{p}_i$ é um ideal maximal, e logo $\mathfrak{p} = \mathfrak{p}_i$ para algum i, digamos para $i = 1$. Se $r = 1$, basta pegar $\alpha = \beta^{-1}$. Se $r > 1$, escolha $\beta_0 \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (\beta)$. Então $\beta_0/\beta \notin \mathcal{O}_K$, e $\beta_0/\beta \in \mathfrak{p}^{-1}$. Então podemos pegar $\alpha = \beta_0/\beta$.

Pelo lema anterior, temos que ter $\alpha\mathfrak{p} \neq \mathfrak{p}$, logo temos que ter $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$. □

Corolário 4. *Seja $\mathfrak{a} \subseteq \mathcal{O}_K$ um ideal. Então $\mathfrak{a}$ é um produto de ideais primos.*

Demonstração. Vamos provar isso por indução em $N(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})$. Temos um ideal primo $\mathfrak{p}$ com $\mathfrak{a} \subseteq \mathfrak{p}$. Multiplicando por $\mathfrak{p}^{-1}$, teríamos $\mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$. Logo $\mathfrak{b} = \mathfrak{a}\mathfrak{p}^{-1}$ é um ideal, e $\mathfrak{b}\mathfrak{p} = \mathfrak{a}$.

Escolhendo $\alpha \in \mathfrak{p}^{-1} \setminus \mathcal{O}_K$, temos $\alpha\mathfrak{a} \subseteq \mathfrak{b}$, e então $\mathfrak{b} \nsubseteq \mathfrak{a}$ pelo lema (pois $\alpha \notin \mathcal{O}_K$). Logo $\mathfrak{a} \subset \mathfrak{b}$ com $\mathfrak{a} \neq \mathfrak{b}$, e então temos que ter $\#\mathcal{O}_K/\mathfrak{a} > \#\mathcal{O}_K/\mathfrak{b}$. □

Corolário 5. *Sejam $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ dois ideais. Então $\mathfrak{a} \subseteq \mathfrak{b}$ se e somente se $\mathfrak{b} \mid \mathfrak{a}$.*

Demonstração. Se $\mathfrak{b} \mid \mathfrak{a}$, é fácil ver que $\mathfrak{a} \subseteq \mathfrak{b}$.

Agora se $\mathfrak{a} \subseteq \mathfrak{b}$, escrevendo $\mathfrak{b} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ como um produto de ideais primos, temos que $\mathfrak{a}\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1} \subseteq \mathcal{O}_K$ é um ideal, digamos $\mathfrak{a}_0$, e isso implica que $\mathfrak{a} = \mathfrak{a}_0\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{a}_0\mathfrak{b}$. □

Teorema 6. *$\mathcal{O}_K$ tem fatoração única em ideais primos.*

Demonstração. Basta provarmos que a fatoração é única. Vamos provar isso por indução em $\#\mathcal{O}_K/\mathfrak{a}$. Seja $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{p}'_1 \cdots \mathfrak{p}'_s$ duas fatorações. Como $\mathfrak{a} \subseteq \mathfrak{p}_1$, temos que ter $\mathfrak{p}'_i \subseteq \mathfrak{p}_1$ para algum i, o que implica em $\mathfrak{p}_1 = \mathfrak{p}'_i$ pois $\mathfrak{p}'_i$ é maximal. Digamos que isso acontece para $i = 1$. Multiplicando por $\mathfrak{p}_1^{-1}$ dos dois lados, e pela hipótese de indução, temos que $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$ é uma permutação de $\mathfrak{p}'_2, \ldots, \mathfrak{p}'_s$, e a indução está completa. □

3.2. **Como fatorar na prática.** Vamos ver como calcular a fatoração dos ideais $p\mathcal{O}_K$ para primos $p \in \mathbb{Z}$ em certos casos: nos casos que existe $\alpha \in \mathcal{O}_K$ com $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Note que isso é verdade para $K = \mathbb{Q}[\sqrt{d}]$ e $K = \mathbb{Q}[e^{2\pi i/p}]$, mas não é verdade sempre. Quando temos $\mathcal{O}_K = \mathbb{Z}[\alpha]$ para algum α, dizemos que $\mathcal{O}_K$ é *monogênico*.

Para isso, vamos usar a seguinte versão de Teorema Chinês dos Restos:

Teorema 7. *Se $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ são ideais de R relativamente primos dois a dois (o que significa $\mathfrak{a}_i + \mathfrak{a}_j = R$ para $i \neq j$), então*

$$\mathfrak{a} := \mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n \quad e \quad R/\mathfrak{a} \simeq R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_n.$$

Demonstração. Por indução em n, basta provar para $n = 2$ se verificarmos que $\mathfrak{a}_1 + \mathfrak{a}_2 \cdots \mathfrak{a}_n = 1$. De fato, como $\mathfrak{a}_1 + \mathfrak{a}_i = R$ para $i \neq 1$, existem $\alpha_i \in \mathfrak{a}_1$ e $\beta_i \in \mathfrak{a}_i$ com $\alpha_i + \beta_i = 1$. Mas então $1 = \prod_{i=2}^n (\alpha_i + \beta_i) = \prod_{i=2}^n \beta_i + \sum_{i=2}^n \alpha_i(\cdots) \in \mathfrak{a}_1 + \mathfrak{a}_2 \cdots \mathfrak{a}_n$ pois $\alpha_i \in \mathfrak{a}_1$ e $\prod_{i=2}^n \beta_i \in \mathfrak{a}_2 \cdots \mathfrak{a}_n$.

Sejam então $\mathfrak{a}, \mathfrak{b}$ ideais relativamente primos. Temos claramente a inclusão $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Para a inclusão contrária, escolha $a \in \mathfrak{a}$ e $b \in \mathfrak{b}$ com $a + b = 1$, o que é possível por $\mathfrak{a} + \mathfrak{b} = R$, e note que se $c \in \mathfrak{a} \cap \mathfrak{b}$, então $c = (a + b)c = ac + cb \in \mathfrak{a}\mathfrak{b}$.

Agora note que temos um mapa natural $R/\mathfrak{a}\mathfrak{b} \to R/\mathfrak{a} \times R/\mathfrak{b}$. Esse mapa é injetor, pois se c vai pra 0, isso significa que $c \in \mathfrak{a}$ e $c \in \mathfrak{b}$, ou seja, que $c \in \mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$. Para ver que o mapa é sobrejetor,

dados x e y vamos construir α com $\alpha \mapsto (x, y)$. Escolhemos $\alpha = bx + ay$ onde $a + b = 1$ com $a \in \mathfrak{a}$ e $b \in \mathfrak{b}$. Temos $\alpha \mapsto (x, y)$ pois $\alpha = x + a(y - x) = y + b(x - y)$. □

Como consequência de fatoração única e Teorema Chinês dos Restos, temos

Corolário 8. *Seja $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n} \subseteq \mathcal{O}_K$ um ideal e sua fatoração. Então*

$$\mathcal{O}_K/\mathfrak{a} \simeq \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_n^{e_n}$$

Demonstração. Basta provar que $\mathfrak{p}_i^{e_i}$ e $\mathfrak{p}_j^{e_j}$ são relativamente primos. Como $\mathfrak{p}_i$ e $\mathfrak{p}_j$ são maximais, temos que ter $\mathfrak{p}_i + \mathfrak{p}_j = \mathcal{O}_K$. Escolha $a \in \mathfrak{p}_i$ e $b \in \mathfrak{p}_j$ com $a + b = 1$. Então $1 = (a + b)^{e_i + e_j}$, mas isso é um elemento de $\mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j}$, logo $\mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j} = \mathcal{O}_K$. □

Agora vamos ver como podemos calcular a fatoração em vários casos:

Teorema 9. *Suponha que exista $\alpha \in \mathcal{O}_K$ com $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Seja $f(X) \in \mathbb{Z}[X]$ o polinômio minimal de α. Seja $f(X) = f_1(X)^{e_1} \cdots f_n(X)^{e_n}$ a fatoração de f em $\mathbb{F}_p[X]$. Seja $\mathfrak{p}_i = (p, f_i(\alpha))$. Então $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ é a fatoração de $\mathfrak{a}$.*

Demonstração. Note que $\mathcal{O}_K = \mathbb{Z}[\alpha]$ significa que $\mathbb{Z}[X]/(f(X)) \simeq \mathcal{O}_K$ onde $X \mapsto \alpha$. Então podemos escrever

$$\mathcal{O}_K/p\mathcal{O}_K = \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \simeq \mathbb{Z}[X]/(f(X), p) = \mathbb{F}_p[X]/(f(X)).$$

Pelo Teorema Chinês dos Restos, temos então que

$$\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{F}_p[X]/(f(X)) \simeq \mathbb{F}_p[X]/(f_1(X)^{e_1}) \times \cdots \times \mathbb{F}_p[X]/(f_n(X)^{e_n}).$$

Isso implica que se $\mathfrak{p} \supseteq p\mathcal{O}_K$ é um ideal maximal, então $\mathfrak{p} = \mathfrak{p}_i$ para algum i. Agora se d é o maior expoente tal que $\mathfrak{p}_i^d \supseteq p\mathcal{O}_K$, isso significa que d é o maior expoente tal que $(f_i(X)^d) \supseteq (f(X))$. Por definição, isso é $d = e_i$. □

De fato, o teorema acima vale se $K = \mathbb{Q}[\alpha]$ com $\alpha \in \mathcal{O}_K$ e $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]] = \sqrt{\frac{\operatorname{disc}(f)}{D_K}}$, pois daí ainda é verdade que $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \xrightarrow{\sim} \mathcal{O}_K/p\mathcal{O}_K$.

O próximo teorema é verdade em geral, mas podemos prová-lo para o caso $\mathcal{O}_K = \mathbb{Z}[\alpha]$ usando o teorema anterior:

Teorema 10. *Seja $p \in \mathbb{Z}$ um primo. Então $p\mathcal{O}_K$ é livre de quadrados se e somente se $p \nmid D_K$.*

Demonstração no caso $\mathcal{O}_K = \mathbb{Z}[\alpha]$. No caso $\mathcal{O}_K = \mathbb{Z}[\alpha]$, temos que $\alpha, \dots, \alpha^n$ é uma base integral para $\mathcal{O}_K$. Se $\alpha_1, \dots, \alpha_n$ são as raízes do polinómio minimal de α, então $\mathrm{Tr}(\alpha^i) = \sum_{k=1}^n \alpha_k^i$. Então temos que $D_K = \det(A)$ onde $a_{i,j} = \sum_{k=1}^n \alpha_k^{i+j}$. Temos $A = BB^t$ onde $b_{i,j} = \alpha_j^i$. Mas $\det(B)$ pode ser calculado por Vandermonde, logo $D_K = \det(A) = \prod_{i<j}(\alpha_i - \alpha_j)^2$, que é o discriminante polinomial de f.

Agora o teorema segue do fato que f tem raiz repetida módulo p se e somente se p divide o discriminante polinomial de f. □

O Teorema Chinês dos Restos também mostra que a norma de ideais é multiplicativa.

Teorema 11. *A norma* $N(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})$ *de um ideal é totalmente multiplicativa.*

Demonstração. Se $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$, é a fatoração de $\mathfrak{a}$, o Teorema Chinês dos Restos nos diz que $N(\mathfrak{a}) = \prod_{i=1}^n N(\mathfrak{p}_i^{e_1})$. Então basta provar que $N(\mathfrak{p}^n) = N(\mathfrak{p})^n$ para um ideal primo $\mathfrak{p} \neq \{0\}$. Vamos provar isso por indução em n.

Temos que $\#\mathcal{O}_K/\mathfrak{p}^n = \#\mathfrak{p}/\mathfrak{p}^n \cdot \#\mathcal{O}_K/\mathfrak{p}$, então basta provar que $\#\mathcal{O}_K/\mathfrak{p}^{n-1} = \#\mathfrak{p}/\mathfrak{p}^n$.

Seja $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Considere o mapa $\mathcal{O}_K/\mathfrak{p}^{n-1} \xrightarrow{\cdot\pi} \mathfrak{p}/\mathfrak{p}^n$. Ele é injetor, pois se $\pi\alpha \in \mathfrak{p}^n$, isso significa que $\mathfrak{p}^n \mid (\pi)(\alpha)$, logo $\mathfrak{p}^{n-1} \mid (\alpha)$, o que significa que $\alpha \in \mathfrak{p}^{n-1}$. Para provar que o mapa é sobrejetor, basta ver que $\mathfrak{p} = (\pi) + \mathfrak{p}^n$. Para isso, considere $\mathcal{O}_K/(\pi)$. Pelo Teorema Chinês dos Restos, se $(\pi) = \mathfrak{p}\mathfrak{a}$, temos $\mathcal{O}_K/(\pi) \simeq \mathcal{O}_K/\mathfrak{p} \times \mathcal{O}_K/\mathfrak{a}$, onde $\mathfrak{a}$ e $\mathfrak{p}$ são relativamente primos. Isso implica que $\mathfrak{a}$ e $\mathfrak{p}^n$ são relativamente primos, e logo que a imagem de $\mathfrak{p}^n$ em $\mathcal{O}_K/\mathfrak{p} \times \mathcal{O}_K/\mathfrak{a}$ é o ideal $\{0\} \times \mathcal{O}_K/\mathfrak{a}$. Mas isso corresponde ao ideal $\mathfrak{p}$, o que prova que $(\pi) + \mathfrak{p}^n = \mathfrak{p}$. □

Corolário 12. *Seja* $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ *a fatoração de* $p\mathcal{O}_K$. *Denote* $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$. *Então*

$$[K : \mathbb{Q}] = \sum_{i=1}^n e_i f_i.$$

Demonstração. Como $\mathcal{O}_K$ tem uma base integral, temos que $N(p\mathcal{O}_K) = p^{[K:\mathbb{Q}]}$. Mas pelo lema acima, temos

$$p^{[K:\mathbb{Q}]} = N(p\mathcal{O}_K) = \prod_{i=1}^n N(\mathfrak{p}_i)^{e_i} = \prod_{i=1}^n (p^{f_i})^{e_i}$$

e portanto $[K : \mathbb{Q}] = \sum_{i=1}^n e_i f_i$. □

Nota 13. Isso também é verdade para o caso L/K, ou seja, se $K \subseteq L$ são dois corpos numéricos e $\mathfrak{p}$ é um ideal primo de $\mathcal{O}_K$, podemos fatorar $\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$, e se $f_i = [\mathcal{O}_L/\mathfrak{p}_i : \mathcal{O}_K/\mathfrak{p}]$, então é verdade que $[L : K] = \sum_{i=1}^n e_i f_i$.

4. Grupo de Classes

A ideia do *grupo de classes* é olhar os ideais "módulo" os ideais principais. Ou seja, queremos dizer que $\mathfrak{a} \sim \mathfrak{b}$ se existe $\alpha \in K^\times$ com $\mathfrak{a} = (\alpha)\mathfrak{b}$.

Definição 1. O *grupo de classes* de K, denotado $\mathrm{Cl}(K)$, é o conjunto de ideais módulo a relação de equivalência $\mathfrak{a} \sim \mathfrak{b} \iff$ existem $\alpha, \beta \in \mathcal{O}_K$ com $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$. A operação de grupo é multiplicação de ideais. Denotamos por $[\mathfrak{a}]$ a imagem de $\mathfrak{a}$ em $\mathrm{Cl}(K)$.

Para ver que isso é bem definido, temos que ver que se $[\mathfrak{a}] = [\mathfrak{a}']$ e $[\mathfrak{b}] = [\mathfrak{b}']$, então $[\mathfrak{ab}] = [\mathfrak{a}'\mathfrak{b}']$. Se $\alpha, \alpha', \beta, \beta' \in \mathcal{O}_K$ com $(\alpha)\mathfrak{a} = (\alpha')\mathfrak{a}'$ e $(\beta)\mathfrak{b} = (\beta')\mathfrak{b}'$, então $(\alpha\beta)\mathfrak{ab} = (\alpha'\beta')\mathfrak{a}'\mathfrak{b}'$, logo $[\mathfrak{ab}] = [\mathfrak{a}'\mathfrak{b}']$.

Também temos que checar que existe elemento neutro e inversos. O elemento neutro é dado por $[\mathcal{O}_K]$, ou por $[(\alpha)]$ para qualquer $\alpha \in \mathcal{O}_K$. A existência de inverso é fácil: para qualquer $[\mathfrak{a}] \in \mathrm{Cl}(K)$, pegue $\alpha \in \mathfrak{a}$, então $\mathfrak{a} \mid (\alpha)$, ou seja, existe $\mathfrak{b}$ com $(\alpha) = \mathfrak{ab} \implies 1 = [(\alpha)] = [\mathfrak{a}][\mathfrak{b}]$.

O objetivo dessa aula é provar que $\mathrm{Cl}(K)$ é finito. Também queremos fazer isso de maneira efetiva, ou seja, queremos conseguir calcular $\mathrm{Cl}(K)$ para casos específicos.

4.1. **O caso $K = \mathbb{Q}[\sqrt{d}]$ com d livre de quadrados.** Se d não é resíduo quadrático módulo $p \geq 3$, sabemos que $p\mathcal{O}_K$ é primo. Se d é um resíduo quadrático módulo $p \geq 3$ e $p \nmid d$, podemos escolher, por Thue, $a, b \in \mathbb{Z}$ com $|a|, |b| \leq \lceil \frac{\sqrt{p}}{2} \rceil$ com $p \mid a^2 - db^2$, digamos $a^2 - db^2 = kp$. Então $|k|p \leq (1 + |d|)\lceil \frac{\sqrt{p}-1}{2} \rceil^2 < \frac{1+|d|}{4}(p + 1 + 2\sqrt{p})$, so $|k| < \frac{1+|d|}{4}(1 + 3/2) = \frac{5(1+|d|)}{8}$.

Chame $N_d = \frac{5(1+|d|)}{8}$. Isso significa que para qualquer $\mathfrak{p} \mid p\mathcal{O}_K$ temos $a, b \in \mathbb{Z}$ com $(a+b\sqrt{d}) = \mathfrak{pa}$ com $\mathfrak{a} \mid k\mathcal{O}_K$ com $k < N_d$. Então $[\mathfrak{p}] = [\mathfrak{a}^{-1}]$. Isso significa que:

Teorema 2. *$\mathrm{Cl}(K)$ é gerado por $[\mathfrak{p}]$ para primos $\mathfrak{p} \mid p\mathcal{O}_K$ com $p < N_d$ ou $p \mid 2d$.*

Exemplo 3. Se $d = -5$, temos $N_d = \frac{15}{4} < 4$. Como $-5\mathcal{O}_K = (\sqrt{-5})^2$, temos que $\mathrm{Cl}(K)$ é gerado pelos divisores de $2\mathcal{O}_K$ e $3\mathcal{O}_K$. Os divisores de $3\mathcal{O}_K$ são $(3, 1 \pm \sqrt{-5})$ e podemos ver que

$$(2, 1 \pm \sqrt{-5})(3, 1 \pm \sqrt{-5}) = (6, 2 \pm 2\sqrt{-5}, 3 \pm 3\sqrt{-5}, -4 + 2\sqrt{-5}) = (6, 1 + \sqrt{-5}) = (1 + \sqrt{-5}).$$

Como $\mathfrak{a} = (2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5})$ satisfaz $\mathfrak{a}^2 = (2)$ que é principal, temos $[(3, 1 \pm \sqrt{-5})][\mathfrak{a}] = 1 \implies [(3, 1 \pm \sqrt{-5})] = [\mathfrak{a}]^{-1} = [\mathfrak{a}]$. Então $\mathrm{Cl}(K)$ é gerado por $[\mathfrak{a}]$. De fato, $\mathfrak{a}$ não é principal pois $\#\mathcal{O}_K/\mathfrak{a} = 2$ e não existe $\alpha \in \mathcal{O}_K$ com $|\mathrm{Nm}(\alpha)| = 2$. Portanto, $\mathrm{Cl}(\mathbb{Q}[\sqrt{-5}]) = \{1, [(2, 1 + \sqrt{-5})]\}$. Por exemplo, temos que $[\mathfrak{a}^2] = [\mathfrak{a}]^2 = 1$ para todo ideal $\mathfrak{a}$, o que significa que $\mathfrak{a}^2$ é principal.

No caso que $d \equiv 1 \mod 4$, podemos fazer uma estimativa melhor, pois se $\alpha = \frac{1+\sqrt{d}}{2}$, temos $(a+\alpha b)(a+\overline{\alpha}b) = a^2 + ab + \frac{1-d}{4}b^2$. Se $p \nmid 2d$ é tal que d é resíduo quadrático, então por Thue exsitem a, b com $p \mid a^2 + ab + \frac{1-d}{4}b^2$ e $a, b \leq \lceil \frac{\sqrt{p}-1}{2} \rceil$. Se $a^2 + ab + \frac{1-d}{4}b^2 = pk$, uma conta similar a antes mostra que $|k| < N_d = \frac{5}{8}\left(1 + \frac{|d-5|}{4}\right)$.

Exemplo 4. Se $d = -15$, temos $N_d < 4$, então temos que fatorar $2\mathcal{O}_K, 3\mathcal{O}_K$ e $5\mathcal{O}_K$. Como o polinômio minimal de α é $x^2 - x + 4 = 0$, temos $2\mathcal{O}_K = (2, \alpha)(2, 1+\alpha) = \mathfrak{p}_2\mathfrak{p}_2'$, $3\mathcal{O}_K = (3, \alpha+1)^2 = \mathfrak{p}_3^2$ e $5\mathcal{O}_K = (5, \alpha+2)^2 = \mathfrak{p}_5^2$. Então $\mathrm{Cl}(K)$ é gerado por $[\mathfrak{p}_2], [\mathfrak{p}_2'], [\mathfrak{p}_3], [\mathfrak{p}_5]$. Temos claramente que $[\mathfrak{p}_3]^2 = [\mathfrak{p}_5]^2 = 1$ e podemos ver que $\mathfrak{p}_3\mathfrak{p}_5 = (2\alpha - 1)$. Logo $[\mathfrak{p}_3] = [\mathfrak{p}_5]$. Agora vemos que $\mathfrak{p}_2'\mathfrak{p}_3 = (6, \alpha+1) = (\alpha+1)$, logo $[\mathfrak{p}_2'] = [\mathfrak{p}_3]$. Mas $[\mathfrak{p}_2'][\mathfrak{p}_2] = 1$, o que implica que $[\mathfrak{p}_2] = [\mathfrak{p}_2'] = [\mathfrak{p}_3] = [\mathfrak{p}_5]$. Podemos ver que eles não são 1 pois $\#\mathcal{O}_K/\mathfrak{p}_2 = 2$ e não existe $\alpha \in \mathcal{O}_K$ com $|\mathrm{Nm}(\alpha)| = 2$. Portanto, $\mathrm{Cl}(\mathbb{Q}[\sqrt{-15}]) = \{1, [\mathfrak{p}_2]\}$.

4.2. **O caso geral (ideias).** Iremos provar o seguinte:

Teorema 5 (Cota de Minkowski)**.** *Seja $\mathfrak{a} \subseteq \mathcal{O}_K$ um ideal. Então existe uma constante M_K tal que exista $\alpha \in \mathfrak{a}$ com*

$$|\mathrm{Nm}(\alpha)| \leq M_K \cdot \#\mathcal{O}_K/\mathfrak{a}.$$

Corolário 6. *Para qualquer $c \in \mathrm{Cl}(K)$, existe $\mathfrak{b} \subseteq \mathcal{O}_K$ com $[\mathfrak{b}] = c$ e $\#\mathcal{O}_K/\mathfrak{b} \leq M_K$. Em particular, $\mathrm{Cl}(K)$ é finito.*

Demonstração. Seja $c = [\mathfrak{a}]^{-1} \in \mathrm{Cl}(K)$ uma classe, e escolha $\alpha \in \mathfrak{a}$ como no teorema. Então seja $\mathfrak{b} = (\alpha)\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$. Temos que $[\mathfrak{b}] = c$ e que $\mathrm{Nm}(\alpha) = \#\mathcal{O}_K/\mathfrak{a}\mathfrak{b} = \#\mathcal{O}_K/\mathfrak{a} \cdot \#\mathcal{O}_K/\mathfrak{b}$. Então $\#\mathcal{O}_K/\mathfrak{b} \leq M_K$. □

Ideia da demonstração da Cota de Minkowski. Vamos assumir por simplicidade que $K = \mathbb{Q}[\alpha]$ para algum $\alpha \in \mathcal{O}$. (Sempre existe tal α, mas não vamos provar isso)

Considere o polinômio minimal $f(X) \in \mathbb{Z}[X]$ de α. Sejam $\alpha = \alpha_1, \ldots, \alpha_n$ suas raízes. Algumas delas são reais, e outras complexas. As complexas vem em pares de conjugados, então podemos escrever as raízes como

$$\alpha_1, \ldots, \alpha_r, \alpha_{r+1}, \overline{\alpha_{r+1}}, \ldots, \alpha_{r+s}, \overline{\alpha_{r+s}},$$

com $\alpha_1, \ldots, \alpha_r \in \mathbb{R}$ e $r + 2s = n$. Como $K \simeq \mathbb{Q}[X]/(f(X))$, podemos considerar os mapas

$$p_i \colon K \simeq \mathbb{Q}[X]/(f(X)) \xrightarrow{X \mapsto \alpha_i} \mathbb{R} \quad \text{para } 1 \leq i \leq r,$$

e

$$p_i \colon K \simeq \mathbb{Q}[X]/(f(X)) \xrightarrow{X \mapsto \alpha_i} \mathbb{C} \quad \text{para } r+1 \leq i \leq r+s.$$

Combinando todos esses mapas, temos $p \colon K \to \mathbb{R}^r \oplus \mathbb{C}^s$. O que vai acontecer é que um ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ será mapeado para um lattice $\Lambda_\mathfrak{a}$ em $\mathbb{R}^r \oplus \mathbb{C}^s$.

Então temos um lattice $\Lambda_\mathfrak{a} \subset \mathbb{R}^r \oplus \mathbb{C}^s \simeq \mathbb{R}^n$ e queremos encontrar um ponto "pequeno" em $\Lambda_\mathfrak{a}$. Para isso podemos usar o teorema de Minkowski: qualquer região simétrica fechada de volume maior ou igual que $2^n \cdot \mathrm{Vol}(\Lambda_\mathfrak{a})$ possui um ponto de $\Lambda_\mathfrak{a}$ diferente da origem.

É verdade que $\mathrm{Nm}(\alpha) = p_1(\alpha) \cdots p_r(\alpha) |p_{r+1}(\alpha)|^2 \cdots |p_{r+s}(\alpha)|^2$, então queremos considerar o subconjunto

$$X(t) = \left\{ (x_1, \ldots, x_r, z_{r+1}, \ldots, z_{r+s}) \colon \sum_{i=1}^{r} |x_i| + 2 \sum_{i=r+1}^{r+s} |z_i| \right\} \subset \mathbb{R}^r \oplus \mathbb{C}^s.$$

Por desigualdade das médias, temos que se $p(\alpha) \in X(t)$, então $|\mathrm{Nm}(\alpha)| \leq \frac{t^n}{n^n}$. Um pouco de cálculo mostra que $\mathrm{Vol}(X(t)) = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}$.

Então escolhendo t tal que $\mathrm{Vol}(X(t)) = 2^n \cdot \mathrm{Vol}(\Lambda_\mathfrak{a})$, podemos conseguir $\alpha \in \mathfrak{a}$ com

$$|\mathrm{Nm}(\alpha)| \leq \frac{2^n \cdot \mathrm{Vol}(\Lambda_\mathfrak{a}) \cdot n!}{2^r \cdot (\pi/2)^s \cdot n^n} = \left(\frac{4}{\pi}\right)^s \cdot \frac{n!}{n^n} \cdot (2^s \cdot \mathrm{Vol}(\Lambda_\mathfrak{a})).$$

Finalmente, temos que $\mathrm{Vol}(\Lambda_\mathfrak{a}) = \mathrm{Vol}(\Lambda_{\mathcal{O}_K}) \cdot \#\mathcal{O}_K/\mathfrak{a}$. E na verdade, um pouco de álgebra linear mostra que $2^s \cdot \mathrm{Vol}(\Lambda_{\mathcal{O}_K}) = \sqrt{|D_K|}$. Então temos

$$|\mathrm{Nm}(\alpha)| \leq \sqrt{|D_K|} \cdot \left(\frac{4}{\pi}\right)^s \cdot \frac{n!}{n^n} \cdot \#\mathcal{O}_K/\mathfrak{a}. \qquad \square$$

Exemplo 7. Tomemos $K = \mathbb{Q}[7^{1/3}]$. A mesma técnica da tarefa de casa para $\mathbb{Q}[2^{1/3}]$ prova que $\mathcal{O}_K = \mathbb{Z}[7^{1/3}]$. Podemos então calcular que $D_K = -3^3 \cdot 7^2 = -1323$. Então nesse caso $M_K = 21 \cdot \sqrt{3} \cdot \frac{4}{\pi} \cdot \frac{6}{27} = \frac{56}{\pi\sqrt{3}} < 11$, então temos que analisar ideais primos $\mathfrak{p}$ com $\#(\mathcal{O}_K/\mathfrak{p}) \leq 10$.

- $p = 7$: temos $7\mathcal{O}_K = (7^{1/3})^3$, e $(7^{1/3})$ é principal.
- $p = 5$: temos que 7 é resíduo cúbico módulo 5 de exatamente uma forma, então $5\mathcal{O}_K = \mathfrak{p}_5\mathfrak{p}_5'$ com $N(\mathfrak{p}_5) = 5$ e $N(\mathfrak{p}_5') = 5^2$. Somente $\mathfrak{p}_5$ interessa, e temos $\mathfrak{p}_5 = (5, 7^{1/3} - 3)$.
- $p = 3$: temos que $x^3 - 7 \equiv (x-1)^3 \mod 3$, então $3\mathcal{O}_K = \mathfrak{p}_3^3 = (3, 7^{1/3} - 1)^3$.
- $p = 2$: temos que $x^3 - 7 \equiv (x-1)(x^2 + x + 1) \mod 2$, então

$$2\mathcal{O}_K = \mathfrak{p}_2(\mathfrak{p}_2')^2 = (2, 7^{1/3} - 1)(2, 1 + 7^{1/3} + 7^{2/3})^2.$$

Das fatorações acima, temos $[\mathfrak{p}_2][\mathfrak{p}_2']^2 = 1$. Agora note que

$$\mathfrak{p}_2\mathfrak{p}_3 = (2, 7^{1/3}-1)(3, 7^{1/3}-1) = \left(6, 3(7^{1/3}-1), 2(7^{1/3}-1), (7^{1/3}-1)^2\right) = (6, 7^{1/3}-1) = (7^{1/3}-1)$$

pois $6 = (7^{1/3}-1)(1+7^{1/3}+7^{2/3})$, e que

$$\mathfrak{p}_2\mathfrak{p}_5 = (10, 2(7^{1/3}-3), 5(7^{1/3}-3), (7^{1/3}-3)^2) = (10, 7^{1/3}-3)$$

e então

$$\mathfrak{p}_2^2\mathfrak{p}_5 = (20, 10(7^{1/3}-3), 2(7^{1/3}-3), (7^{1/3}-3)^2) = (20, 2(7^{1/3}-3), (7^{1/3}-3)^2) = (7^{1/3}-3)$$

pois $-20 = (7^{1/3}-3)(7^{2/3}+3\cdot 7^{1/3}+9)$ e $(2, 7^{1/3}-3, 9+3\cdot 7^{1/3}+7^{2/3}) = (2, 7^{1/3}-1, 13) = (1)$.

Então $\mathrm{Cl}(K)$ é gerado por $\mathfrak{p}_2'$. É fácil ver que $\mathfrak{p}_2'$ não é principal, e temos que

$$(\mathfrak{p}_2')^3 = (8, 4(1+7^{1/3}+7^{2/3}), 2(15+9\cdot 7^{1/3}+3\cdot 7^{2/3}), 99+45\cdot 7^{1/3}+27\cdot 7^{2/3})$$

que é

$$(8, 4(1+7^{1/3}+7^{2/3}), -2+2\cdot 7^{1/3}-2\cdot 7^{1/3}, 3-3\cdot 7^{1/3}+3\cdot 7^{2/3}) = (8, 1-7^{1/3}+7^{2/3}, 4(1+7^{1/3}+7^{2/3})$$

que é $= (1-7^{1/3}+7^{2/3})$ pois $8 = (1-7^{1/3}+7^{2/3})(1+7^{1/3})$ e também $4(1+7^{1/3}+7^{2/3}) = (1-7^{1/3}+7^{2/3})(4+7^{1/3}+7^{2/3})$.

Então segue que $\mathrm{Cl}(K) = \{1, [\mathfrak{p}_2'], [\mathfrak{p}_2']^2\} \simeq \mathbb{Z}/3\mathbb{Z}$.

Exemplo 8. Tomemos $L = \mathbb{Q}[\sqrt{-1}, \sqrt{6}]$. Podemos calcular que $D_L = 2304 = 2^8 \cdot 3^2$. Então $M_L = 2^4 \cdot 3 \cdot \frac{24}{4^4} = \frac{9}{2}$, então temos que ver primos $\mathfrak{p}$ com $\#\mathcal{O}_K/\mathfrak{p} \leq 4$. Temos que 3 ramifica em $\mathbb{Q}[\sqrt{6}]$ e que é inerte em $\mathbb{Q}[\sqrt{-1}]$, então isso significa que $3\mathcal{O}_L = \mathfrak{p}_3^2 = (3, \sqrt{6})^2$. Agora 2 ramifica em todos os 3 subcorpos quadráticos, então $2\mathcal{O}_L = \mathfrak{p}_2^4$. Como $\mathfrak{p}_2^2 = (1+i)\mathcal{O}_L$, temos que $[\mathfrak{p}_2]^2 = 1$. Também, temos $(\sqrt{6}) = \mathfrak{p}_3\mathfrak{p}_2^2$, de onde concluímos que $[\mathfrak{p}_3] = 1$. De fato, $\mathfrak{p}_2$ não é principal, o que implica que $\mathrm{Cl}(K) \simeq \mathbb{Z}/2\mathbb{Z}$.

4.3. **Teorema das unidades de Dirichlet.** Vimos que o grupo de classes nos permite entender ideias em termos dos ideais principais. Para entendermos os ideais principais, resta entendermos as unidades ${\mathcal{O}_K}^\times$ do corpo numérico. Isso é feito pelo seguinte teorema:

Teorema 9 (Dirichlet)**.** *Temos* ${\mathcal{O}_K}^\times \simeq \mu(K) \times \mathbb{Z}^{r+s-1}$*, onde* $\mu(K)$ *denotam as raízes da unidade dentro de* K*.*

Ideia da demonstração. A ideia é considerar o mapa $\mathrm{Log}\colon K^\times \to \mathbb{R}^{r+s}$ dado por

$$\mathrm{Log}(x) = (\log|p_1(x)|, \dots, \log|p_{r+s}(x)|).$$

Como $|\mathrm{Nm}(x)| = |p_1(x)| \cdots |p_r(x)| \cdot |p_{r+1}(x)|^2 \cdots |p_{r+s}(x)|^2$, temos que

$$\mathrm{Log}({\mathcal{O}_K}^\times) \subseteq \{(x_1, \dots, x_{r+s})\colon x_1 + \cdots + x_r + 2(x_{r+1} + \cdots x_{r+s}) = 0\} =: \mathbb{R}_0^{r+s} \simeq \mathbb{R}^{r+s-1}.$$

E como $\mathrm{Ker}\,(\mathrm{Log}\colon \mathcal{O}_K \to \mathbb{R}^{r+s}) = \mu(K)$ (são raízes de polinômios inteiros tal que todas as raízes tem módulo 1), basta provarmos que $\mathrm{Log}({\mathcal{O}_K}^\times)$ é um lattice em $\mathbb{R}_0^{r+s}$. Isso pode ser feito combinando dois ingredientes: (1) $\mathrm{Log}({\mathcal{O}_K}^\times) \cap \{(x_1, \dots, x_{r+s})\colon |x_i| \leq R\}$ é finito e (2) existe uma constante B tal que todo $h \in \mathbb{R}_0^{r+s}$ tem um ponto de $\mathrm{Log}({\mathcal{O}_K}^\times)$ com distância no máximo B. Para (1), note que $\mathrm{Log}({\mathcal{O}_K}^\times) \cap \{(x_1, \dots, x_{r+s})\colon |x_i| \leq R\}$ são a imagem de elementos $x \in {\mathcal{O}_K}^\times$ tal que seus conjugados tem valor absoluto no máximo e^R, e só existem finitos polinômios inteiros com raízes desse tipo. Para (2), por Minkowski será possível achar $\gamma \in \mathcal{O}_K$ com $\mathrm{Log}(\gamma)$ com distância no máximo B' de h e com $|\mathrm{Nm}(\gamma)| \leq B'$. Escrevendo $(\alpha_1), \dots, (\alpha_m)$ todos os ideais principais de norma $\leq B'$, temos que existe i com $\gamma/\alpha_i \in {\mathcal{O}_K}^\times$, e daí $\mathrm{Log}(\gamma/\alpha_i) = \mathrm{Log}(\gamma) - \mathrm{Log}(\alpha_i)$ está a distância no máximo B de h, onde B combina a comtribuição de B' e dos $\mathrm{Log}(\alpha_i)$. □

Exemplo 10. Se $K = \mathbb{Q}[\sqrt{d}]$ com $d > 1$ livre de quadrados, temos $r = 2,\ s = 0$, então ${\mathcal{O}_K}^\times \simeq \{\pm 1\} \times \mathbb{Z}$. A unidade fundamental nesse caso é relacionada com a solução fundamental da equação de Pell.

Exemplo 11. Se $K = \mathbb{Q}[2^{1/3}]$, temos $r = s = 1$, então ${\mathcal{O}_K}^\times \simeq \{\pm 1\} \times \mathbb{Z}$. A unidade fundamental nesse caso é $2^{1/3} - 1$.

5. Elemento de Frobenius

Para essa seção, vamos considerar corpos numéricos da forma $K = \mathbb{Q}[\alpha]$. É verdade que todo corpo numérico é dessa forma, mas não vamos provar isso.

Se $F(X) \in \mathbb{Z}[X]$ é o polinômio minimal de α, chamamos suas raízes de *conjugados* de α.

Definição 1. Um corpo numérico $K = \mathbb{Q}[\alpha]$ é chamado *Galois* se todos os conjugados de α estão em K.

Exemplo 2. $K = \mathbb{Q}[\sqrt{d}]$ e $K = \mathbb{Q}[\zeta_n]$ são Galois, mas $K = \mathbb{Q}[2^{1/3}]$ não é.

Se $K = \mathbb{Q}[\alpha]$ tem grau n, lembre que definimos mapas $\sigma_i \colon K \to \mathbb{C}$ para $1 \leq i \leq n$, que levam $\alpha \mapsto \alpha_i$ onde α_i são os conjugados de α. Se K é Galois, então esses mapas tem imagem em K, ou seja, temos $\sigma_i \colon K \to K$.

Teorema 3. *Seja $K = \mathbb{Q}[\alpha]$ Galois. O conjunto $G = \{\sigma_i \colon K \to K\}$ forma um grupo por composição. Ele é chamado de* grupo de Galois *de K, e denotado $G = \mathrm{Gal}(K)$.*

Demonstração. Seja $G' = \{\sigma \colon K \to K$ mapas bijetores de corpos que fixam $\mathbb{Q}\}$. G' é claramente um grupo. Vamos provar que $G = G'$.

Como $F(\alpha) = 0$, temos que ter $0 = \sigma(F(\alpha)) = F(\sigma(\alpha))$, logo $\sigma(\alpha) = \alpha_i$ para algum i. Isso prova que $G' \subseteq G$.

Então basta provar que os σ_i são bijetores. Isso é o mesmo que provar que $K = \mathbb{Q}[\alpha_i]$ para todo i. Isso é verdade porque claramente $\mathbb{Q}[\alpha_i] \subseteq K$ e eles tem a mesma dimensão sobre $\mathbb{Q}$, pois o polinômio minimal de α_i também é $F(X)$. □

Exemplo 4. Para $K = \mathbb{Q}[\sqrt{d}]$, o elemento não trivial de $\mathrm{Gal}(K)$ é $a + b\sqrt{d} \mapsto a - b\sqrt{d}$. Para $K = \mathbb{Q}[\zeta_n]$, temos $\mathrm{Gal}(K) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ com $\sigma_i \colon \zeta_n \mapsto \zeta_n^i$ para $i \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Extensões Galois deixam nossa vida mais fácil. Por exemplo, temos

Proposição 5. *Para $\beta \in K$, temos* $\mathrm{Tr}(\beta) = \sum_{\sigma \in \mathrm{Gal}(K)} \sigma(\beta)$.

Demonstração. Isso é claro para $\beta = \alpha$ pois o polinômio característico de multiplicação por α é $F(X)$, então os autovalores são α_i. Isso também é claro para potências de α pois os autovalores vão ser as potências dos autovalores para α. Como $1, \alpha, \ldots, \alpha^{n-1}$ é uma $\mathbb{Q}$-base de K, por linearidae também é verdade para β. □

Corolário 6. *Se $\beta \in K$ satisfaz $\sigma(\beta) = \beta$ para todo β, então $\beta \in \mathbb{Q}$.*

Demonstração. Temos $n\beta = \sum_{\sigma \in \mathrm{Gal}(K)} \sigma(\beta) = \mathrm{Tr}(\beta) \in \mathbb{Q}$, logo $\beta \in \mathbb{Q}$. □

Também é verdade que $\mathrm{Nm}(\beta) = \prod_{\sigma \in \mathrm{Gal}(K)} \sigma(\beta)$.

Também podemos aplicar $\sigma \in \mathrm{Gal}(K)$ em ideais:

Definição 7. Se $\sigma \in \mathrm{Gal}(K)$ e $\mathfrak{a} \subseteq \mathcal{O}_K$ é um ideal, então temos o ideal $\sigma(\mathfrak{a}) = \{\sigma(a) \mid a \in \mathfrak{a}\}$.

Proposição 8. *$\sigma(\mathfrak{a})$ é primo se e somente se $\mathfrak{a}$ é primo. Se eles são primos, então $f(\mathfrak{a}) = f(\sigma(\mathfrak{a}))$.*

Demonstração. Temos $\mathcal{O}_K/\mathfrak{a} \xrightarrow[\sim]{\sigma} \mathcal{O}_K/\sigma(\mathfrak{a})$, então $\mathfrak{a}$ ser maximal e $\sigma(\mathfrak{a})$ ser maximal é o mesmo que eles serem corpos. Se $\mathfrak{a}$ é primo, $\#\mathcal{O}_K/\mathfrak{a} = p^{f(\mathfrak{a})}$, então $f(\mathfrak{a}) = f(\sigma(\mathfrak{a}))$. □

Proposição 9. *Seja $p \in \mathbb{Z}$ um primo e sejam $\mathfrak{p}, \mathfrak{p}' \subseteq \mathcal{O}_K$ primos acima de p. Então existe $\sigma \in \mathrm{Gal}(K)$ com $\mathfrak{p}' = \sigma(\mathfrak{p})$.*

Demonstração. Use TCR para achar $\alpha \in \mathfrak{p} \setminus \mathfrak{p}^2$, mas $\alpha \notin \mathfrak{p}_0$ para todo outro $\mathfrak{p}_0$ acima de p. Então considere $S = \prod_{\sigma \in \mathrm{Gal}(K)} \sigma(\alpha)\mathcal{O}_K$. Temos $(S) = \prod_{\sigma \in \mathrm{Gal}(K)} \sigma(\mathfrak{p}) \cdot \mathfrak{a}$ onde $\mathfrak{a}$ não é divisível por primos acima de p. S é invariante por $\mathrm{Gal}(K)$, então $S \in \mathbb{Z}$. Como $\mathfrak{p} \mid (\alpha) \mid (S)$, temos que ter $p \mid S$. Logo $\mathfrak{p}' \mid S$, mas então $p\mathcal{O}_K \mid \prod_{\sigma \in \mathrm{Gal}(K)} \sigma(\mathfrak{p})$, ou seja, se $\mathfrak{p}' \mid p\mathcal{O}_K$, temos $\mathfrak{p}' = \sigma(\mathfrak{p})$ para algum σ. □

Corolário 10. *Se $p \nmid D_K$, então $p = \mathfrak{p}_1 \cdots \mathfrak{p}_g$ com $n = fg$ onde $f = f(\mathfrak{p}_i)$.*

Demonstração. Pelos resultados acima, $f = f(\mathfrak{p}_i)$ é igual para todo i. Como $n = \sum_i e_i f_i$ e $e_i = 1$ porque $p \nmid D_K$, temos $n = fg$. □

Isso é uma generalização de algo que voçês provaram na tarefa de casa no caso de $K = \mathbb{Q}[\zeta_p]$:

Exemplo 11. Seja $K = \mathbb{Q}[\zeta_n]$. Temos que $p \nmid n \implies p \nmid D_K$, e então se $p \mid \Phi_n(a)$ para algum a, isso significa que existe $\mathfrak{p} \mid p\mathcal{O}_K$ com $f(\mathfrak{p}) = 1$. Logo $p\mathcal{O}_K = \prod_{\sigma \in \mathrm{Gal}(K)} \sigma(\mathfrak{p})$.

Agora considere $p \nmid D_K$ e $D(\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(K) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\} \subseteq \mathrm{Gal}(K)$. Como $\#\mathrm{Gal}(K) = n$, o resultado acima diz que $\#D(\mathfrak{p}) = f$. Agora, se $\sigma \in D(\mathfrak{p})$, temos um mapa bijetor $\mathcal{O}_K/\mathfrak{p} \xrightarrow{\sigma} \mathcal{O}_K/\mathfrak{p}$.

Daqui em diante, vamos considerar $\mathcal{O}_K = \mathbb{Z}[\alpha]$ por simplicidade. As demonstrações vão ficar mais simples, mas os resultados valem em geral.

Teorema 12. *Seja $p \nmid D_K$. Então o mapa $D(\mathfrak{p}) \to \mathrm{Aut}(\mathcal{O}_K/\mathfrak{p})$ é um isomorfismo.*

Demonstração. Ambos tem tamanho f, então basta provar que é injetor. Se não fosse, isso implicaria que teríamos $\sigma_i\colon \alpha \mapsto \alpha_i$ com $\alpha \neq \alpha_i$ e $\alpha - \alpha_i \in \mathfrak{p}$. Mas isso significaria que $F(X)$ tem uma raiz dupla módulo $\mathfrak{p}$. Mas daí teríamos $\mathfrak{p} \mid (D_K)$, ou seja, que $p \mid D_K$. □

Mas como $\mathcal{O}_K/\mathfrak{p}$ é um corpo finito, sabemos que $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_{p^f}$. Portanto $D(\mathfrak{p})$ é cíclico de tamanho f, e possui um gerador canônico, que corresponde a $x \mapsto x^p$ em $\mathcal{O}_K/\mathfrak{p}$. Tal gerador é chamado de *elemento de Frobenius* $\mathrm{Frob}(\mathfrak{p}) \in \mathrm{Gal}(K)$. Como $D(\mathfrak{p})$ tem tamanho f, então $\mathrm{Frob}(\mathfrak{p})$ tem ordem f em $\mathrm{Gal}(K)$. Ele é definido únicamente por $\mathrm{Frob}(\mathfrak{p})(\beta) \equiv \beta^p \mod \mathfrak{p}$.

Proposição 13. *Se $p \nmid D_K$ e $\mathfrak{p} \mid p\mathcal{O}_K$, então $\mathrm{Frob}(\sigma(\mathfrak{p})) = \sigma\mathrm{Frob}(\mathfrak{p})\sigma^{-1}$. Em particular, se $\mathrm{Gal}(K)$ é abeliano então $\mathrm{Frob}(\mathfrak{p})$ só depende de p, e denotamos $\mathrm{Frob}(p)$.*

Demonstração. Basta ver que de $\mathrm{Frob}(\mathfrak{p})(\sigma^{-1}(\beta) \equiv (\sigma^{-1}(\beta)) \mod \mathfrak{p}$ segue que $(\sigma\mathrm{Frob}(\mathfrak{p})\sigma^{-1})(\beta) \equiv \beta^p \mod \sigma(\mathfrak{p})$. □

Exemplo 14. Podemos calcular $\mathrm{Frob}(p)$ nos exemplos mais simples:

- $K = \mathbb{Q}[\sqrt{d}]$. Temos $\mathrm{Gal}(K) \simeq \mathbb{Z}/2\mathbb{Z} \simeq \{\pm 1\}$. Para $p \nmid D_K$, temos que $\mathrm{Frob}(p) = 1 \iff f(p) = 1 \iff \left(\frac{d}{p}\right) = 1$ e $\mathrm{Frob}(p) = -1 \iff f(p) = 2 \iff \left(\frac{d}{p}\right) = -1$. Logo $\mathrm{Frob}(p) = \left(\frac{d}{p}\right)$.
- $K = \mathbb{Q}[\zeta_n]$. Temos $\mathrm{Gal}(K) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. Considere o elemento $\sigma_p\colon \zeta_n \mapsto \zeta_n^p$ de $\mathrm{Gal}(K)$. Como $\sigma_p(\beta) \equiv \beta^p \mod p$, temos também $\sigma_p(\beta) \equiv \beta^p \mod \mathfrak{p}$ para qualquer $\mathfrak{p} \mid p\mathcal{O}_K$. Isso significa que $\sigma_p = \mathrm{Frob}(\mathfrak{p}) = \mathrm{Frob}(p)$. Na identificação $\mathrm{Gal}(K) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, temos que $\mathrm{Frob}(p) = p \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Teorema 15. *Sejam $K \subset L$ dois corpos numéricos Galois, e $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$ primos de L e K. Então no mapa natural $\mathrm{Gal}(L) \to \mathrm{Gal}(K)$, temos $\mathrm{Frob}(\mathfrak{P}) \mapsto \mathrm{Frob}(\mathfrak{p})$.*

Demonstração. Isso é óbvio, pois $\mathrm{Frob}(\mathfrak{P})(\beta) \equiv \beta^p \mod \mathfrak{P}$ para todo $\beta \in \mathcal{O}_L$ implica que $\mathrm{Frob}(\mathfrak{P})(\beta) \equiv \beta^p \mod \mathfrak{p}$ para $\beta \in \mathcal{O}_K$. □

Teorema 16 (Reciprocidade quadrática)**.** *Sejam $p, q > 2$ primos distintos. Então*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Além disso, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Demonstração. Seja $p^* = (-1)^{(p-1)/2}$. Temos que $\mathbb{Q}[\sqrt{p^*}] \subset \mathbb{Q}[\zeta_p]$. Isso é porque $\left(\sum_{a=1}^{p} \left(\frac{a}{p}\right) \zeta_p^a\right)^2 = p^*$. Uma vez que provarmos isso, temos

$$\mathrm{Frob}(q) = \left(\frac{p^*}{q}\right) \in \mathrm{Gal}(\mathbb{Q}[\sqrt{p^*}]) = \{\pm 1\}$$

e

$$\mathrm{Frob}(q) = \sigma_q \in \mathrm{Gal}(\mathbb{Q}[\zeta_p]).$$

Queremos comparar esses dois Frobenius, então temos que entender o mapa $\mathrm{Gal}(\mathbb{Q}[\zeta_p]) \to \mathrm{Gal}(\mathbb{Q}[\sqrt{p^*}])$. Como $\sqrt{p^*} = \pm \sum_{a=1}^{p} \left(\frac{a}{p}\right) \zeta_p^a$, podemos ver que $\sigma_i(\sqrt{p^*}) = \left(\frac{i}{p}\right) \sqrt{p^*}$. Então o mapa é $\sigma_a \mapsto \left(\frac{a}{p}\right)$.

Comparando os Frobenius, isso nos diz que

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right),$$

ou seja, que

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Agora se o primo q fosse 2, ainda temos que $\mathrm{Frob}(2) = \sigma_2 \in \mathrm{Gal}(\mathbb{Q}[\zeta_p])$, e portanto comparando os Frobenius temos que $\mathrm{Frob}(2) = \left(\frac{2}{p}\right) \in \mathrm{Gal}(\mathbb{Q}[\sqrt{p^*}])$. Então $\left(\frac{2}{p}\right) = 1$ se e somente se 2 quebra em $\mathbb{Q}[\sqrt{p^*}]$, ou seja, se o polinômio $x^2 - x - \frac{p^*-1}{4}$ tem uma raiz módulo 2, o que é equivalente a $8 \mid p^* - 1$. Mas isso é o mesmo que $p \equiv \pm 1 \mod 8$. □

Exemplo 17 (OBM 2017/6)**.** Se $\alpha^3 - 3\alpha + 1 = 0$, vimos anteriormente que $K = \mathbb{Q}[\alpha] \subseteq L = \mathbb{Q}[\zeta_9]$. É fácil ver que ele é Galois. Então para $p \nmid D_K = 81$, existe a com $p \mid a^3 - 3a + 1$ se e somente se $\mathrm{Frob}(p) = 1 \in \mathrm{Gal}(K)$. Mas é fácil ver que $\sigma_a(\alpha) = \alpha$ se e somente se $a \equiv \pm 1 \mod 9$, pois $\alpha = \zeta_9 + \zeta_9^{-1}$.

Exemplo 18. Você pode fazer exatamente como no exemplo anterior para as seguinte situações:

- $L = \mathbb{Q}[\zeta_7]$, $\alpha = \zeta_7 + \zeta_7^{-1}$, $P(X) = x^3 + x^2 - 2x - 1$,
- $L = \mathbb{Q}[\zeta_{13}]$, $\alpha = \zeta_{13} + \zeta_{13}^5 + \zeta_{13}^{-5} + \zeta_{13}^{-1}$, $P(X) = x^3 + x^2 - 4x + 1$,
- $L = \mathbb{Q}[\zeta_{15}]$, $\alpha = \zeta_{15} + \zeta_{15}^4$, $P(X) = x^4 - x^3 + 2x^2 + x + 1$,
- $L = \mathbb{Q}[\zeta_{20}]$, $\alpha = \zeta_{20} + \zeta_{20}^9$, $P(X) = x^4 + 3x^2 + 1$,

para obter que

- $p \mid a^3 + a^2 - 2a - 1$ se e somente se $p = 7$ ou $p \equiv \pm 1 \mod 7$,
- $p \mid a^3 + a^2 - 4a + 1$ se e somente se $p = 13$ ou $p \equiv \pm 1, \pm 5 \mod 13$,

- $p \mid a^4 - a^3 + 2a^2 + a + 1$ se e somente se $p \equiv 1, 4 \mod 15$,
- $p \mid a^4 + 3a^2 + 1$ se e somente se $p = 5$ ou $p \equiv 1, 9 \mod 20$.

Você também pode obter qualquer subconjunto $G \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$ desse modo: Considere $L = \mathbb{Q}[\zeta_n]$ e considere $K = \{x \in L \colon gx = x \text{ para todo } g \in G\}$. Isso será um corpo numérico, e você pode escolher um $\alpha \in \mathcal{O}_K$ com $K = \mathbb{Q}[\alpha]$ e usar o algoritmo de fatoração. Nos exemplos acima, acontece que K é monogênico. Mas mesmo se K não for monogênico podemos obter um resultado da forma acima.

6. Teoria dos corpos de classe

Seja K um corpo numérico. Essa teoria foi desenvolvida durante o século 20, e descreve extensões abelianas L de um corpo numérico K.

Vamos começar descrevendo o caso de $K = \mathbb{Q}$. O teorema seguinte foi anunciado inicialmente por Kronecker em 1853, mas uma prova completa só foi dada por Hilbert em 1896.

Teorema 1 (Kronecker-Weber)**.** *Seja L uma extensão abeliana de $\mathbb{Q}$. Então existe n tal que $L \subseteq \mathbb{Q}[\zeta_n]$.*

O menor tal n é (essencialmente) chamado de o *condutor* $\mathfrak{f}$ de L. Sabemos que os primos que dividem o condutor são exatamente os primos que ramificam em L, ou seja, os primos que dividem D_L.

Um grande objetivo da teoria dos corpos de classe é obter um teorema análogo para o caso $K \neq \mathbb{Q}$. Assim como temos um índice n no teorema acima, no caso geral teremos um *modulus* como índice.

Definição 2. Um *modulus* de K é $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, onde $\mathfrak{m}_0$ é um ideal de K e $\mathfrak{m}_\infty$ é um subconjunto dos r mapas injetores de corpos $\{\sigma\colon K \to \mathbb{R}\}$. Também chamamos de *lugares* os ideais primos de $\mathcal{O}_K$ junto com os mapas injetores de corpos $K \to \mathbb{R}$.

Nota 3. Na verdade, os *lugares* também devem incluir os mapas injetores de corpos $K \to \mathbb{C}$ módulo conjugação complexa, de modo que temos r lugares reais e s lugares complexos.

Em geral, o condutor de uma extensão abeliana $L/\mathbb{Q}$ é um modulus de $\mathbb{Q}$. Se denotarmos por ∞ o único mapa $\mathbb{Q} \to \mathbb{R}$, e se n é o menor n tal que $L \subseteq \mathbb{Q}[\zeta_n]$, então temos $\mathfrak{f}_{L/\mathbb{Q}} = (n)$ se L é real, e $\mathfrak{f}_{L/\mathbb{Q}} = (n)\infty$ se L não é real.

Teorema 4. *Dado um corpo numérico K, existem corpos numéricos $K[\mathfrak{m}]$ para cada modulus $\mathfrak{m}$ tal que toda extensão abeliana L/K está contida em algum $K[\mathfrak{m}]$. O condutor $\mathfrak{f}_{L/K}$ é o menor $\mathfrak{m}$ tal que isso é verdade. O corpo $K[\mathfrak{m}]$ é chamado de o* corpo de classe de Ray de modulus $\mathfrak{m}$*.*

No caso $K = \mathbb{Q}$, temos $\mathbb{Q}[(n)\infty] = \mathbb{Q}[\zeta_n]$ e $\mathbb{Q}[(n)] = \mathbb{Q}[\zeta_n + \zeta_n^{-1}] = \mathbb{Q}[\zeta_n] \cap \mathbb{R}$. Dada a seguinte definição de ramificação para mapas $\sigma\colon K \to \mathbb{R}$, vamos ter que os lugares que dividem o condutor $\mathfrak{f}_{L/\mathbb{Q}}$ são exatamente os lugares ramificados.

Definição 5. Um lugar $\sigma\colon K \to \mathbb{R}$ é ramificado em L/K se não existe lugar $L \to \mathbb{R}$ que extende σ.

Teorema 6. *Os lugares de dividem o condutor $\mathfrak{f}_{L/K}$ são exatamente os lugares que ramificam em L/K.*

Para entendermos porque os corpos $K[\mathfrak{m}]$ são chamados de corpos de classe, vamos considerar os grupos de classe de Ray.

Definição 7. Seja $I^{\mathfrak{m}}$ o grupo de ideais fracionários relativamente primos com $\mathfrak{m}_0$. Denote

$$K_{\mathfrak{m},1} = \left\{ \frac{\alpha}{\beta} \colon (\alpha) + \mathfrak{m}_0 = (\beta) + \mathfrak{m}_0 = \mathcal{O}_K,\ \alpha \equiv \beta \mod \mathfrak{m}_0 \text{ e } \sigma\left(\frac{\alpha}{\beta}\right) > 0 \text{ para } \sigma \in \mathfrak{m}_\infty \right\}.$$

O *grupo de classes de Ray de modulus* $\mathfrak{m}$ é o grupo $\mathrm{Cl}_{\mathfrak{m}}(K) = I^{\mathfrak{m}}/\iota(K_{\mathfrak{m},1})$ onde $\iota(\alpha) = \alpha\mathcal{O}_K$.

Exemplo 8. Para o modulus trivial $\mathfrak{m} = \mathcal{O}_K$, temos que $\mathrm{Cl}_{\mathfrak{m}}(K)$ é o grupo de classes.

Com essa definição, temos a seguinte descrição essencial dos grupos de Galois $\mathrm{Gal}\left(K[\mathfrak{m}]/K\right)$.

Teorema 9. *Temos um isomorfismo $\mathrm{Cl}_{\mathfrak{m}}(K) \xrightarrow{\sim} \mathrm{Gal}\left(K[\mathfrak{m}]/K\right)$ dado pelo Frobenius em ideais primos e extendido multiplicativamente.*

Um exemplo essencial é o caso do modulus trivial $\mathfrak{m} = \mathcal{O}_K$. Nesse caso, $K[\mathfrak{m}] = H_K$ é chamado do *corpo de classe de Hilbert* de K, e temos $\mathrm{Cl}(K) \xrightarrow{\sim} \mathrm{Gal}\left(H_K/K\right)$. Então podemos ver se primos são principais em $\mathcal{O}_K$ vendo se eles tem Frobenius trivial em H_K.

Junto com a teoria de Galois, isso implica que todos os grupos de Galois de extensões abelianas L/K são quocientes de algum $\mathrm{Cl}_{\mathfrak{m}}(K)$, e de fato podemos explicitamente descrever esse quociente:

Teorema 10. *Se L/K é abeliano e $\mathfrak{f}_{L/K} \mid \mathfrak{m}$, temos o isomorfismo*

$$I_K^{\mathfrak{m}}/\iota(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}_{L/K}(I_L^{\mathfrak{m}}) \xrightarrow{\sim} \mathrm{Gal}\left(L/K\right)$$

definido pelo Frobenius, onde $\mathrm{Nm}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}$ é extendido multiplicativamente.

6.1. **Primos da forma $p = n^2 + km^2$ com $k > 0$.** Uma aplicação interessante disso é caracterizar os primos da forma $n^2 + km^2$ para $k > 0$. Escreva $k = dl^2$ com d livre de quadrados e $K = \mathbb{Q}[\sqrt{d}]$ com $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Se $\mathfrak{m} = (l')$, com $l = l'$ se $d \not\equiv 1 \mod 4$ e $l' = 2l$ se $d \equiv 1 \mod 4$, então podemos considerar a subextensão $K(l') \subseteq K[\mathfrak{m}]$ com

$$\mathrm{Cl}_{\mathfrak{m}}(K)/\iota(\mathbb{Q}^{l'}) \xrightarrow{\sim} \mathrm{Gal}\left(K(l')/K\right).$$

Isso é tal que um primo $\mathfrak{p}$ tem Frobenius trivial em $K(l)$ exatamente se $\mathfrak{p} = (\alpha)(\beta)$ com $\alpha \in K_{\mathfrak{m},1}$ e $\beta \in \mathbb{Q}^{l'}$, ou seja, $\mathfrak{p} = (\frac{r}{s}(a + b\alpha))$ com $l' \mid b,\ a \equiv 1 \mod l'$ e $\mathrm{mdc}(r, l) = \mathrm{mdc}(s, l) = 1$. Podemos ver que isso é o mesmo que $\mathfrak{p} = (a + b\sqrt{d})$ com $l \mid b$.

Isso implica que um primo $p \in \mathbb{Z}$ é da forma $n^2 + km^2$ se e somente se p quebra completamente em $K(l')$. Pode-se provar que $K(l')/\mathbb{Q}$ é Galois, então temos o seguinte teorema.

Teorema 11. *Existe um polinômio mônico $f(x) \in \mathbb{Z}[x]$ e um inteiro D tal que $p \nmid D$ é da forma $n^2 + km^2$ se e somente se $p \mid f(a)$ para algum a.*

Demonstração. Seja f o polinômio minimal de um elemento primitivo $\alpha \in \mathcal{O}_L$ de $L/\mathbb{Q}$, e escolha $D = \mathrm{disc}(f)$. Então o teorema segue pelas considerações anteriores. □

7. Reciprocidades

Vamos considerar generalizações de reciprocidade quadrática para outros expoentes.

Definição 1. Seja K um corpo numérico que contém $\mathbb{Q}[\zeta_n]$. Seja $\mathfrak{p} \subseteq \mathcal{O}_K$ um ideal primo com $\mathfrak{p} \nmid (n)$. Não é difícil provar que $N(\mathfrak{p}) \equiv 1 \mod n$. Se $\alpha \in \mathcal{O}_K \setminus \mathfrak{p}$, definimos o *power residue symbol*

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n = \zeta_n^s$$

por $\alpha^{\frac{N(\mathfrak{p})-1}{n}} \equiv \zeta_n^s \mod \mathfrak{p}$. Em geral, se $\beta \in \mathcal{O}_K$ é relativamente primo com n e $(\beta) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}$, definimos

$$\left(\frac{\alpha}{\beta}\right)_n = \prod_{i=1}^{k} \left(\frac{\alpha}{\mathfrak{p}_i}\right)_n^{e_i}.$$

O fato que deixa possível usar a teoria dos corpos de classe para provar uma forma de reciprocidade é que o power residue symbol pode ser definido em termos da *teoria de corpos de classe local*.

Definição 2. Para um corpo numérico K e um primo $\mathfrak{p}$, podemos considerar o *corpo local* $K_\mathfrak{p} = \mathrm{Frac}(\mathcal{O}_{K_\mathfrak{p}})$ onde $\mathcal{O}_{K_\mathfrak{p}} = \lim_n \mathcal{O}_K/\mathfrak{p}^n$. Seus elementos são sequências de elementos $\alpha_n \in \mathcal{O}_K/\mathfrak{p}^n$ que são compatíveis: $\alpha_n \equiv \alpha_{n-1} \mod \mathfrak{p}^{n-1}$. Se temos um lugar $\sigma\ K \to \mathbb{C}$, definimos $K_\sigma = \mathbb{R}$ ou $\mathbb{C}$ se σ é real ou não.

Proposição 3. *Se L/K é Galois e $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$ são dois primos, temos que $L_\mathfrak{P}/K_\mathfrak{p}$ é Galois com grupo de Galois $D(\mathfrak{P} \mid \mathfrak{p})$.*

Teorema 4 (Teoria dos corpos de classe local)**.** *Se $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ é abeliano, então existe um mapa canônico*

$$K_{\mathfrak{p}}{}^{\times}/\mathrm{Nm}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(L_{\mathfrak{P}}{}^{\times}) \xrightarrow{\sim} \mathrm{Gal}\left(L_{\mathfrak{P}}/K_{\mathfrak{p}}\right).$$

Para $\alpha \in K_{\mathfrak{p}}{}^{\times}$, denotamos a sua imagem por $(\alpha, L_{\mathfrak{P}}/K_{\mathfrak{p}})$. Além disso, se $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ e $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ não é ramificado, então $(\pi, L_{\mathfrak{P}}/K_{\mathfrak{p}}) = \mathrm{Frob}(\mathfrak{p})$.

Com isso, definimos os *símbolos de Hilbert* para $\alpha, \beta \in K^{\times}$ com $K \supseteq \mathbb{Q}[\zeta_n]$ por

$$\langle \beta, \alpha \rangle_{n,\mathfrak{p}} := \frac{(\beta,\ K_{\mathfrak{p}}[\alpha^{1/n}]/K_{\mathfrak{p}})(\alpha^{1/n})}{\alpha^{1/n}}.$$

Agora, se $K \supseteq \mathbb{Q}[\zeta_n]$, se $\mathfrak{p} \nmid (n\alpha)$, pode-se provar que $K[\alpha^{1/n}]/K$ não é ramificado em $\mathfrak{p}$. Isso implicaria que

$$\langle \pi, \alpha \rangle_{n,\mathfrak{p}} = \frac{(\pi,\ K_{\mathfrak{p}}[\alpha^{1/n}]/K_{\mathfrak{p}})(\alpha^{1/n})}{\alpha^{1/n}} = \frac{\mathrm{Frob}(\mathfrak{p})(\alpha^{1/n})}{\alpha^{1/n}} \equiv \frac{\alpha^{N(\mathfrak{p})/n}}{\alpha^{1/n}} \equiv \alpha^{\frac{N(\mathfrak{p})-1}{n}} \mod \mathfrak{p},$$

ou seja, que

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n = \langle \pi, \alpha \rangle_{n,\mathfrak{p}}.$$

Lema 5. *O símbolo de Hilbert $(\cdot,\cdot) = \langle \cdot, \cdot \rangle_{n,\mathfrak{p}}$ satisfaz as seguintes propriedades:*

(a) $(aa', b) = (a, b)(a', b)$ *e* $(a, bb') = (a, b)(a, b')$ *para* $a, a', b, b' \in K_{\mathfrak{p}}{}^{\times}$. *Em particular, temos* $(a, b) = 1$ *se* $a \in (K^{\times})^n$ *ou* $b \in (K^{\times})^n$

(b) $(1 - a, a) = 1 = (a, 1 - a)$ *para* $a \in K_{\mathfrak{p}}{}^{\times} \setminus \{1\}$.

(c) $(a, b^{-1}) = (a, b)^{-1} = (a^{-1}, b)$ *e* $(1, a) = (a, 1) = 1 = (a, -a)$ *para* $a, b \in K_{\mathfrak{p}}{}^{\times}$.

(d) $(a, b) = (b, a)^{-1}$, *para* $a, b \in K_{\mathfrak{p}}{}^{\times}$.

Demonstração. A parte (a) segue diretamente da definição. Para provar a parte (b), note que para isso é suficiente provar que $1 - a$ é uma norma de $K_{\mathfrak{p}}[a^{1/n}]/K_{\mathfrak{p}}$, o que é verdade pois

$$1 - a = \prod_{i=1}^{n} (1 - \zeta_n^i a^{1/n}).$$

Para provar (c), note que $(1, a) = 1$ é trivial por definição. Note que por (a) temos $(a, 1)(a, 1) = (a, 1)$, logo $(a, 1) = 1$ e então $(a, b)(a, b^{-1}) = (a, 1) = 1$, e analogamente para $(a^{-1}, b) = (a, b)^{-1}$. Finalmente, como $-a = \frac{1-a}{1-a^{-1}}$, temos $(a, -a) = (a, 1-a)(a, 1-a^{-1})^{-1} = (a, 1-a)(a^{-1}, 1-a^{-1}) = 1$ por (b).

Para provar (d), começamos usando (c): temos $(ab, -ab) = 1$, e então por (a) e (c) temos

$$(a,-a)(a,b)(b,a)(b,-b) = 1 \iff (a,b)(b,a) = 1. \qquad \square$$

Corolário 6. *Se $\alpha \in K$ e $\beta \in K$ relativaemnte primos e relativamente primos com n, então temos*

$$\left(\frac{\alpha}{\beta}\right)_n = \prod_{\mathfrak{p}|(\beta)} \langle \beta, \alpha \rangle_{n,\mathfrak{p}}$$

Demonstração. Primeiro note que é fácil ver que $K_\mathfrak{p}[\alpha^{1/n}]/K_\mathfrak{p}$ não é ramificado nas condições acima.

Agora basta provar que se $L_\mathfrak{P}/K_\mathfrak{p}$ não é ramificado, então $(u, L_\mathfrak{P}/K_\mathfrak{p}) = 1$ se $u \in {\mathcal{O}_{K_\mathfrak{p}}}^\times$. Mas sabemos que $(\pi, L_\mathfrak{P}/K_\mathfrak{p}) = \mathrm{Frob}(\mathfrak{p})$ gera $\mathrm{Gal}\left(L_\mathfrak{P}/K_\mathfrak{p}\right)$, e junto com o fato de que $\mathrm{Nm}({\mathcal{O}_{L_\mathfrak{P}}}^\times) \subseteq {\mathcal{O}_{K_\mathfrak{p}}}^\times$ e $\mathrm{Nm}(\pi) \in \pi^f {\mathcal{O}_{K_\mathfrak{p}}}^\times$, isso implica que de fato temos que ter $\mathrm{Nm}({\mathcal{O}_{L_\mathfrak{P}}}^\times) = {\mathcal{O}_{K_\mathfrak{p}}}^\times$, e portanto que $(u, L_\mathfrak{P}/K_\mathfrak{p}) = 1$. $\square$

O que possibilita a reciprocidade é o seguinte teorema da teoria de corpos de classe.

Teorema 7 (Reciprocidade de Artin)**.** *Se L/K é abeliano e $\alpha \in K^\times$, então*

$$\prod_v (\alpha, L_w/K_v) = 1$$

onde v percorre todos os lugares de K. Note que isso significa que todos menos finitos termos desse produto são 1.

Corolário 8 (Reciprocidade de Hilbert)**.** *Se $a, b \in K^\times$ e $K \supseteq \mathbb{Q}[\zeta_n]$, então*

$$\prod_v \langle a, b \rangle_{n,v} = 1$$

onde v percorre todos os lugares de K. Note que isso significa que todos menos finitos termos desse produto são 1.

Demonstração. Segue imediatamente to teorema anterior tomando $L = K[\alpha^{1/n}]$. $\square$

Com isso, podemos finalmente provar a reciprocidade.

Teorema 9 (Lei da reciprocidade de potências)**.** *Seja $K \supseteq \mathbb{Q}[\zeta_n]$ e $\alpha, \beta \in K^\times$ relativamente primos e primos com n. Então temos*

$$\left(\frac{\alpha}{\beta}\right)_n = \left(\frac{\beta}{\alpha}\right)_n \cdot \prod_{v|(n)\infty} \langle \alpha, \beta \rangle_{n,v}.$$

Demonstração. Utilizando o fato que

$$\left(\frac{\alpha}{\beta}\right)_n = \prod_{\mathfrak{p}|(\beta)} \langle \beta, \alpha \rangle_{n,\mathfrak{p}} = \prod_{\mathfrak{p}|(\beta)} \langle \alpha, \beta \rangle_{n,\mathfrak{p}}^{-1} \quad \text{e} \quad \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{\mathfrak{p}|(\alpha)} \langle \alpha, \beta \rangle_{n,\mathfrak{p}},$$

basta provarmos que $\prod_{v|(\alpha\beta n)\infty} \langle \alpha, \beta \rangle_{n,v} = 1$. Pela reciprocidade de Hilbert, isso é o mesmo que

$$\prod_{\mathfrak{p}\nmid(n\alpha\beta)} \langle \alpha, \beta \rangle_{n,\mathfrak{p}} = 1.$$

De fato, é verdade que todos os termos desse produtório são 1, pois se $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ não é ramificado, então $(u, L_{\mathfrak{P}}/K_{\mathfrak{p}}) = 1$ se $u \in {\mathcal{O}_{K_{\mathfrak{p}}}}^{\times}$. □

Vamos ver como isso implica reciprocidade qudrática:

Corolário 10 (Reciprocidade quadrática)**.** *Sejam a, b ímpares positivos relativamente primos. Então temos $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$.*

Demonstração. Pelo teorema anterior, basta ver que $\langle a, b \rangle_{2,2} \langle a, b \rangle_{2,\infty} = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$.

Pode se ver que $\langle a, b \rangle_{2,\infty} = (-1)^{\frac{\mathrm{sgn}(a)-1}{2}\cdot\frac{\mathrm{sgn}(b)-1}{2}}$, que é 1 pois $a, b > 0$.

Para calcular $\langle a, b \rangle_{2,2}$, e como ${\mathcal{O}_{\mathbb{Q}_2}}^{\times}/({\mathcal{O}_{\mathbb{Q}_2}}^{\times})^2 = \{\pm 1, \pm 5\}$, pelas propriedades do símbolo de Hilbert basta calcularmos $\langle 5, -1 \rangle_{2,2}, \langle 5, 5 \rangle_{2,2}, \langle -1, -1 \rangle_{2,2}$, que podem ser calculados como $1, 1, -1$. Então, disso segue o que queremos. □

Outro exemplo é a reciprocidade cúbica:

Corolário 11 (Reciprocidade cúbica)**.** *Seja $K = \mathbb{Q}[\sqrt{-3}]$. Se $\alpha, \beta \in \mathcal{O}_K$ com $\alpha, \beta \equiv \pm 1 \mod 3$, então*

$$\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\beta}{\alpha}\right)_3.$$

Demonstração. Como K é imaginário, seu lugar infinito é complexo, e é fácil ver que os símbolos de Hilbert para tais lugares são triviais. Então pela reciprocidade acima, basta provar que $\langle \alpha, \beta \rangle_{3,(1-\omega)} = 1$ se $\alpha, \beta \equiv \pm 1 \mod 3$.

Como ${\mathbb{Q}_3}^{\times}/({\mathbb{Q}_3}^{\times})^3 = \{1, 2, 4\}$, e $K_{(1-\omega)} \simeq \mathbb{Q}_3$, temos que $\alpha \equiv \pm 1 \mod (1-\omega)^2$ implica em $\alpha \in ({K_{(1-\omega)}}^{\times})^3$. □