Voltemos agora à classificação dos corpos finitos.

Teorema. *Seja F um corpo finito. Então F tem p^n elementos, onde $p = car(F)$ e n é a dimensão $[F : P]$ de F como extensão do seu subcorpo primo P.*

Demonstração. Como F é finito, F é uma extensão finita do seu subcorpo primo P e a sua característica é um primo p. Já sabemos que $P \cong \mathbb{F}_p$. Suponhamos que $[F : P] = n$ e seja $\{\theta_1, \theta_2, \ldots, \theta_n\}$ uma base do espaço vectorial F sobre o corpo P. Cada elemento de F escreve-se de forma única como combinação linear dos vectores $\theta_1, \theta_2, \ldots, \theta_n$, pelo que

$$F = \Big\{ a_1\theta_1 + a_2\theta_2 + \cdots + a_n\theta_n \mid a_1, a_2, \ldots, a_n \in P \Big\}.$$

É claro que, como P tem p elementos, o número destas combinações lineares é igual a p^n (número de arranjos com repetição de p elementos n a n). Portanto, $|F| = p^n$. ∎

A partir dos corpos primos $\mathbb{F}_p$, podemos construir outros corpos finitos pelo processo de adjunção de raízes descrito no capítulo anterior. Se $p(x) \in \mathbb{F}_p[x]$ é um polinómio de grau n, irredutível sobre $\mathbb{F}_p$, então juntando uma raiz de $p(x)$ a $\mathbb{F}_p$ obtemos um corpo finito com p^n elementos. Contudo, não é claro, nesta altura, que exista, para qualquer natural n, um tal polinómio irredutível de grau n. Assim, de modo a provarmos que para cada primo p e para cada natural n existe um corpo com p^n elementos, seguiremos uma abordagem sugerida pelo seguinte resultado.

Proposição. *Seja F um corpo com p^n elementos. Então F é isomorfo à extensão de decomposição do polinómio $x^{p^n} - x$ sobre $\mathbb{F}_p$.*

Demonstração. O grupo multiplicativo $(F \setminus \{0\}, \cdot)$ tem ordem $p^n - 1$, pelo que, para qualquer $a \in F$ diferente de 0, $a^{p^n-1} = 1$. Isto significa que $a^{p^n} \cdot a^{-1} = 1$, isto é, $a^{p^n} = a$.

`[Este facto será decisivo: em qualquer corpo` F
`com` q `elementos, cada` $a \in F$ `satisfaz` $a^q = a$`]`

Portanto, todos os elementos de F são raízes do polinómio $p(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Como este polinómio tem grau p^n e $|F| = p^n$, isto mostra que F contém todas as suas raízes e

$$x^{p^n} - x = \prod_{a \in F} (x - a).$$

Portanto F contém uma extensão de decomposição de $p(x)$. Mas F é exactamente o conjunto das raízes de $p(x)$, pelo que, necessariamente, F é a extensão de decomposição de $p(x)$. ∎

Corolário. [E. H. Moore, 1893]

Dois corpos finitos com o mesmo número de elementos são isomorfos.

Demonstração. É consequência imediata da proposição anterior e da unicidade, a menos de isomorfismo, das extensões de decomposição, provada no capítulo anterior.

∎

Estamos agora em condições de provar o recíproco do primeiro teorema da aula.

Teorema. [Teorema de Galois]

Para cada primo p e cada $n \in \mathbb{N}$, existe um corpo com p^n elementos, único a menos de isomorfismo.

Demonstração. Provemos somente a existência de tal corpo, estando a unicidade assegurada pelo corolário anterior.

Para $q = p^n$, consideremos o polinómio $p(x) = x^q - x$ de $\mathbb{F}_p[x]$. Seja ainda F a extensão de decomposição de $p(x)$.

[Observe que um elemento a de um corpo K é uma *raiz múltipla* de $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ se e só se é uma raiz de $p(x)$ e da sua derivada $D(p(x)) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$]

Como, neste caso $D(p(x)) = qx^{q-1} - 1 = -1 \neq 0$, todas as raízes de $p(x)$ são simples. Portanto, o conjunto $R = \{a \in F \mid a^q - a = 0\}$ das raízes de $p(x)$ em F tem cardinal q. Mas R é um subcorpo de F.

[Verifique]

Está assim encontrado um corpo com p^n elementos: o corpo R das raízes de $p(x)$ em F, que coincide forçosamente com F, uma vez que $p(x)$ se decompõe em factores lineares em R. ∎

Em conclusão:

CLASSIFICAÇÃO DOS CORPOS FINITOS
• Todo o corpo finito tem p^n elementos, para algum primo p e algum natural n. • Para cada primo p e cada natural n, existe um corpo com p^n elementos. • Qualquer corpo com p^n elementos é isomorfo à extensão de decomposição de $x^{p^n} - x$ sobre $\mathbb{F}_p$.

A unicidade no Teorema de Galois justifica que se fale *no* corpo finito (ou *no* corpo de Galois) com q elementos:

CORPO DE GALOIS de ordem q
A este corpo (único, a menos de isomorfismo) chama-se o *corpo de Galois com q elementos*, que se denota por $\mathbb{F}_q$ (ou por $\mathbf{GF}(q)$).

Uma aplicação dos corpos finitos à Teoria dos Números

Como ilustração do que se pode fazer com os resultados que vimos até ao momento, vamos agora apresentar uma prova extremamente elegante, retirada dos apontamentos de Álgebra II de A. Machiavelo [DMUP, 1997-99], do seguinte resultado de Fermat que descreve os primos que podem ser diagonais de triângulos rectângulos de lados inteiros:

Se $p \in \mathbb{N}$ é primo e $p \equiv 1 \mod 4$ então p é soma de dois quadrados.

Para isso começamos por determinar todos os primos p para os quais -1 é um quadrado módulo p, ou seja, para os quais $\mathbb{F}_p$ tem uma raiz quadrada de -1.

Quando $p = 2$ a resposta é óbvia: $-1 = 1 = 1^2$. Suponhamos pois $p \neq 2$. Seja F uma extensão de decomposição sobre $\mathbb{F}_p$ do polinómio $x^2 + 1 \in \mathbb{F}_p[x]$, e denotemos por i uma das duas raízes deste polinómio em F. Como vimos na proposição no início da aula, para cada $a \in F$ tem-se que $a \in \mathbb{F}_p$ se e só se $a^p = a$. Assim, em particular, $i \in \mathbb{F}_p$ se e só se $i^p = i$. Mas

$$i^p = (i^2)^{\frac{p-1}{2}} i = (-1)^{\frac{p-1}{2}} i,$$

que é igual a i quando e só quando $(-1)^{\frac{p-1}{2}} = 1$, ou seja, quando e só quando $p \equiv 1 \mod 4$. Portanto, a equação $x^2 \equiv -1 \mod p$ (p primo) tem solução se e só se $p = 2$ ou $p \equiv 1 \mod 4$.

Seja agora p um primo tal que $p \equiv 1 \mod 4$. Então, pelo que acabámos de ver, $p^2 \equiv -1 \mod p$, logo $p|(m^2+1)$ para algum inteiro m. Isto implica que, no domínio $\mathbb{Z}[i]$ dos inteiros de Gauss, $p|(m+i)(m-i)$. Como $p \nmid (m+i)$ e $p \nmid (m-i)$, resulta que p não é primo em $\mathbb{Z}[i]$.

[Como $\mathbb{Z}[i]$ é um domínio de ideais principais, isto significa que p é redutível, ou seja, existem inteiros a, b tais que $(a+bi)|p$]

Daqui decorre facilmente que $p = a^2 + b^2$, como Fermat afirmou.

Exercício:

(1) Seja p um primo ímpar e F uma extensão de decomposição sobre $\mathbb{F}_p$ do polinómio x^2+1. Designando por i uma das raízes em F de x^2+1, use a relação $(1+i)^2 = 2i$ para determinar quais os primos p tais que 2 é um quadrado módulo p.

(2) Use (1) para provar o seguinte resultado de Euler:

Se p é um primo tal que $p \equiv 3 \mod 4$ e $2p+1$ é primo, então $(2p+1)|(2^p-1)$.

[Este resultado de Euler mostra, em particular, que o *número de Mersenne* $2^p - 1$ não é primo para $p > 3$ nas condições enunciadas; por exemplo: $23|2^{11}-1$, $47|2^{23}-1$]

[Mais uma vez, note a utilidade da introdução do conceito de polinómio como função definida em $\mathbb{N}_0$ com suporte finito (Aula 5), distinguindo-os assim das respectivas funções polinomiais. De facto, pelo Teorema pequeno de Fermat ("para cada a não divisível pelo primo p, $a^{p-1} \equiv 1 \mod p$"), existe apenas um número finito de funções polinomiais $\mathbb{F}_p \to \mathbb{F}_p$ (por exemplo, a função $x \mapsto x^p$ é igual a $x \mapsto x$), enquanto que os polinómios permitem construir uma infinidade de extensões de $\mathbb{F}_p$, para cada primo p, e tais extensões permitem-nos obter resultados não triviais sobre, por exemplo, os números inteiros, como acabámos de ilustrar]