

Sobre Corpo de Galois

Substituir o parágrafo “Pode-se provar que ...” na pg 269 do livro pelo que segue.

Pode-se provar que existe pelo menos um polinômio irredutível $f(x)$ em $Z_p[x]$ para qualquer primo p e qualquer grau $m \geq 1$. Logo existe um corpo finito com p^m elementos para todo primo p e todo inteiro m . Pode existir mais de um polinômio irredutível de grau m em $Z_p[x]$. Pode-se provar que corpos finitos construídos considerando-se quaisquer dois polinômios irredutíveis de um certo grau fixo m em $Z_p[x]$ são isomorfos entre si. Assim, a menos de isomorfismo, existe um *único* corpo finito com p^m elementos (p primo, $m \geq 1$), que é denotado $GF(p^m)$ (também chamado *corpo estendido*). Mais ainda, pode-se provar que não existe corpo finito com k elementos a não ser que k seja da forma $k = p^m$ para algum inteiro $m \geq 1$ e p primo.