MAT5728 Álgebra

Lista 8

2009

CORPOS FINITOS

1. Seja K um corpo finito. Sabemos que o corpo primo de K é isomorfo a $\mathbb{Z}_p$ para algum número primo p. Usando que K pode ser visto como um espaço vetorial sobre $\mathbb{Z}_p$, mostre que $|K| = p^n$ para algum inteiro $n \geq 1$.

2. Vamos agora provar que para todo inteiro $n = 1, 2, ...$ e para todo número primo p existe um corpo com p^n elementos. Para isso, mostre que se K é um corpo de raízes do polinômio $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ então $|K| = p^n$. Observe que K é *exatamente* o conjunto das raízes do polinômio $f(x)$.

3. Seja agora K um corpo finito com $|K| = p^n$ onde p é um número primo e $n > 0$. Como K um corpo finito, sabemos que o grupo multiplicativo $(K^*, .)$ é um grupo cíclico de ordem $p^n - 1$. Sendo assim, todo elemento não nulo de K é raiz do polinômio $x^{p^n-1} - 1$. Prove todas essas afirmações. Conclua então que K tem que ser corpo de raízes do polinômio $f(x)$ do exercício anterior. Conclua daí que dois corpos finitos com o mesmo número de elementos são isomorfos.

4. Seja K um corpo finito com $|K| = p^n$ e L/K uma extensão finita com $[L : K] = r$. Seja $G = \text{Gal}(L/K)$. Seja $\sigma : L \to L$ o automorfismo definido por $\sigma(a) = a^{p^n}$ para todo $a \in L$. Mostre que $G =< \sigma >$. Use o Teorema Fundamental da Teoria de Galois para concluir que $\text{Inv}G = K$.

5. Para L e K como no exercício anterior, mostre que L/K é uma extensão simples, isto é, mostre que existe $z \in L$ tal que $L = K(z)$. (*Sugestão:* Use o fato de que o grupo multiplicativo de L é cíclico.)

GRUPOS SOLÚVEIS

6. Mostre que o grupo diedral D_n é solúvel, para todo n.

7. Mostre que um grupo é simples e solúvel se e somente se ele for cíclico de ordem prima.

8. Sejam A e B dois subgrupos normais de G. Mostre que se A e B forem solúveis então AB também é solúvel.

9. Mostre que se G e H são grupos então $G \times H$ é solúvel se e somente se G e H forem solúveis.

10. Mostre que todo grupo de ordem pq, onde p e q são primos, é solúvel.

11. Mostre que todo grupo de ordem p^2q, onde p e q são primos, é solúvel.

12. Mostre que, se $p < q$ são primos, então todo grupo de ordem pq^n é solúvel.

13. Mostre que todo grupo de ordem menor que 60 é solúvel.

TEORIA DE GALOIS

14. Suponha que $f = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ é irredutível e tem apenas uma raiz real e seja L um corpo de raízes de f sobre $\mathbb{Q}$. Mostre que $\mathrm{Gal}(L/\mathbb{Q})$ é isomorfo a S_3.

15. Seja $f = x^4 + ax^2 + b$ um polinômio irredutível sobre $\mathbb{Q}$ e seja L um corpo de raízes de f.

    (a) Mostre que $\mathrm{Gal}(L/\mathbb{Q})$ é isomorfo a um dos seguintes grupos:

    $$\text{(i) } \mathbb{Z}_4, \quad \text{(ii) } \mathbb{Z}_2 \times \mathbb{Z}_2 \quad \text{ou} \quad \text{(iii) } D_4$$

    (b) Mostre que (i) ocorre se e somente se $\frac{\alpha}{\beta} - \frac{\beta}{\alpha} \in \mathbb{Q}$, onde $\pm\alpha, \pm\beta$ são as raízes de f em L e que (ii) ocorre se e somente se $\alpha\beta \in \mathbb{Q}$.

16. Seja L/K uma extensão galoisiana tal que $[L : K] = p^n m$, onde p é um primo que não divide m. Mostre que existe um corpo F, $K \subseteq F \subseteq L$, com $[F : K] = m$.

17. Sejam p, q primos distintos e seja $L = \mathbb{Q}(\sqrt{p}, \sqrt{q})$.

    (a) Mostre que $\mathrm{Gal}(L/\mathbb{Q})$ é isomorfo ao grupo de Klein.

    (b) Mostre que todo subcorpo de L de grau 2 sobre $\mathbb{Q}$ é da forma $\mathbb{Q}(\sqrt{m})$, onde $m \in \{p, q, pq\}$.

18. Mostre que o polinômio $x^5 - 4x + 2$ não é solúvel por radicais sobre $\mathbb{Q}$.

19. Seja p um número primo e $f \in \mathbb{Q}[x]$ um polinômio irredutível de grau p. Se f tem exatamente duas raízes não reais em um corpo de raízes L mostre que $\mathrm{Gal}(L/\mathbb{Q})$ é isomorfo a S_p.