Álgebra 1

Lista 11

11.1. (**Corpos finitos**). Se F é um corpo finito, mostre que o subgrupo do grupo aditivo de F gerado por 1 possui ordem prima p, e é um subcorpo de F isomorfo ao corpo $\mathbb{F}_p$ das classes de congruência módulo p.

11.2. (**Geradores**). Faça uma tabela de conjuntos minimais que geram $(\mathbb{Z}/m\mathbb{Z})^\times$ para $1 \leq m \leq 24$.

11.3. (**Grupos cíclicos I**). Sejam G um grupo comutativo, x um elemento de G de ordem m e y um elemento de G de ordem n. Prove que se $\gcd(m, n) = 1$, então

$$x^a y^b = 1 \iff x^a = 1 = y^b,$$

donde conclua que o grupo gerado por x e y é cíclico de ordem mn, gerado por xy.

11.4. (**Grupos não cíclicos**). Demonstre que, se $m > 2$, $n > 2$ e $\gcd(m, n) = 1$, então o grupo multiplicativo das classes de congruência primas a mn módulo mn não é cíclico.
Dica: use o Teorema Chinês dos Restos e o fato de que um grupo cíclico possui no máximo um subgrupo de ordem 2.

11.5. (**Grupos cíclicos II**). Encontre todos os valores de n para os quais o grupo multiplicativo das classes de congruência ímpares módulo 2^n é cíclico.
Dica: se a é ímpar, então $a^{2^{n-2}} \equiv 1 \pmod{2^n}$ para cada $n \geq 3$.

11.6. (*n-torção de grupos abelianos*). Verifique que, se G é um grupo comutativo e n é um inteiro > 0, então o conjunto de todos os elementos de G cujas ordens dividem n é um subgrupo de G.

11.7. (*Elementos de ordem 2*). Prove que, se G é um grupo comutativo finito, então o produto de todos os elementos de G é ou 1 ou um elemento de ordem 2. Prove que, se p é um primo, então

$$(p-1)! \equiv -1 \pmod{p}.$$

11.8. (*Grupos abelianos I*). Seja G um grupo aditivo comutativo gerado por $\{x_1, \ldots, x_k\}$ e sejam $c_1, \ldots, c_k$ inteiros tais que $\text{mdc}(c_1, \ldots, c_k) = 1$. Mostre que existe um conjunto $\{y_1, \ldots, y_k\}$ que gera G tal que

$$y_1 = c_1 x_1 + \cdots + c_k x_k.$$

Dica: suponha que cada $c_i \geq 0$ e proceda por indução sobre $s = c_1 + \cdots + c_k$.

11.9. (*Grupos abelianos II*). Dentre todos os conjuntos minimais $\{x_1, \ldots, x_k\}$ que geram um grupo aditivo comutativo G, tome um deles tal que x_1 possua a menor ordem possível. Use o Exercício 11.8 para ver que não existem inteiros positivos $m_1, \ldots, m_k$ tais que

$$m_1 x_1 + \cdots + m_k x_k = 0 \quad \text{com } m_1 x_1 \neq 0.$$

Conclua, por indução, que existe $\{g_1, \ldots, g_k\}$ que gera G tal que se

$$g = n_1 g_1 + \cdots + n_k g_k$$

com cada n_i inteiro, então $n_i g_i = 0$ para cada i.