Semestre 2023/1 Algebra Moderna
Christof Geiss

Tarea 5

Ejercicio 21
Sea $n \in \mathbb{N}_{\geq 3}$. Demuestra:

(a) Sean $a, b \in \{1, 2, \ldots, n\}$ dos elementos diferentes. El grupo alternante $\mathfrak{A}_n$ es generado por los 3-ciclos (a, b, k) con $k \in \{1, 2, \ldots, n\} \setminus \{a, b\}$. Pista: Es suficiente, expresar todo 3-ciclo como producto de los 3-ciclos mencionados. Distingue los casos (a, u, b), (a, u, v), (b, u, v) y (u, v, x) para $u, v, x \in \{1, 2, \ldots, n\} \setminus \{a, b\}$.

(b) Sea $N \lhd \mathfrak{A}_n$ un subgrupo normal. Si N contiene un 3-ciclo, entonces $N = \mathfrak{A}_n$. Pista: Sea (a, b, c) un 3-ciclo. Encuentra para todo $k \in \{1, 2, \ldots, n\} \setminus \{a, b\}$ una permutación $\sigma_k \in \mathfrak{A}_n$ tal que $(a, b, k) = \sigma_k(a, b, c)\sigma_k^{-1}$.

(c) Sea ahora $n \geq 5$ y $N \lhd \mathfrak{A}_n$. Si $N \neq \mathfrak{A}_n$ y $\sigma \in N \setminus \{\mathrm{Id}_n\}$ entonces $\mathrm{Mov}(\sigma) := |\{k = 1, 2, \ldots, n \mid \sigma(k) \neq k\}| \geq 5$.

(d) El grupo $\mathfrak{A}_n$ es simple si $n \geq 5$. Pista: Sea $N \lhd \mathfrak{A}_n$ un subgrupo normal no trivial. Consideraremos un $\sigma \in N \setminus \{\mathrm{Id}_n\}$ tal que $\mathrm{Mov}(\sigma)$ sea minimal en $N \setminus \{\mathrm{Id}_n\}$. Escribimos σ como producto de ciclos ajenos, con los ciclos mas largos primero. Por (b) y (c) solo tenemos que distinguir los siguientes casos: $\sigma = (a, b, c, d, \ldots)\cdots$, $\sigma = (a, b, c)(d, e, \ldots)\cdots$ y $\sigma = (a, b)(c, d)(e, f)\cdots$. Estudia $\sigma' := \tau^{-1}\sigma^{-1}\tau\sigma \in N$ con $\tau = (b, c, d)$ para llegar a una contradicción.

Ejercicio 22
Un grupo G con elemento neutro e se llama *nilpotente* si tiene una serie central inferior finita, es decir una serie familia de subgrupos

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_n = \{e\} \quad \text{con} \quad G_i = [G, G_{i-1}] \quad i = 1, 2, \ldots, n.$$

Demuestra:

(a) G es nilpotente si y solamente tiene una serie central superior finita, es decir una serie de subgrupos

$$\{e\} = Z_0 \lhd Z_1 \lhd \cdots \lhd Z_m = G \quad \text{con} \quad Z_i/Z_{i-1} = Z(G/Z_{i-1}) \quad i = 1, 2, \ldots, m.$$

(b) Un grupo nilpotente es soluble. Cada subgrupo y cada cociente de un grupo nilpotente es nilpotente.

(c) Cada p-grupo finito es nilpotente (p un primo).

(d) Para cada campo $\mathbb{F}$ y $n \in \mathbb{Z}_{\geq 1}$ el grupo multiplicativo $U_n(F)$ de matrices $n \times n$ unitriangulares superiores con entradas en $\mathbb{F}$ es nilpotente.

(e) Un grupo *finito* es nilpotente si y solamente si es producto directo de sus subgrupos de Sylow.

Ejercicio 23
Consideramos los anillos cociente $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ para $m \in \mathbb{N}_{\geq 2}$.

(a) Demuestra: $k + m\mathbb{Z} \in \mathbb{Z}_m$ es una unidad si y solamente si $\text{mcd}(k, m) = 1$.

(b) Demuestra que el grupo de unidades $\mathbb{Z}_m^*$ es isomorfo al grupo de automorfismos $\text{Aut}(\mathbb{Z}_m, +)$ del grupo aditivo.

(c) Demuestra que en caso $\text{mcd}(m_1, m_2) = 1$ se tiene $\mathbb{Z}_{m_1 \cdot m_2}^* \cong \mathbb{Z}_{m_1}^* \times \mathbb{Z}_{m_2}^*$.

Ejercicio 24
Sea R un anillo conmutativo con $0 \neq 1_R \in R$, y $n \in \mathbb{N}_{\geq 2}$. Consideramos el anillo de matrices $S := \text{Mat}(n \times n, R)$. Demuestra:

(a) S es anillo no conmutativo con 1, no libre de divisores de 0.

(b) Los ideales de S son precisamente de la forma $\text{Mat}(n \times n, I)$ para algún ideal I de R. Pista: Para $i, j \in \{1, 2, \ldots, n\}$ y $m \in \text{Mat}(n \times n, R) = S$ sea $m_{i,j}$ la componente (i, j) de m. Si $J \subset S$ es un ideal demuestra que $J_{i,j} := \{m_{i,j} \mid m \in J\}$ es un ideal de R, que no depende de i y j.

(c) Encuentra un ejemplo de un anillo simple (i.e. que no tiene ideales no triviales) que no sea un campo.

Ejercicio 25

(a) Deduzca del teorema Chino de Residuos (la versión vista en clase) el siguiente resultado: Sean $z_1, z_2, \ldots, z_n \in \mathbb{Z}$ con $\text{mcd}(z_i, z_j) = 1$ para todo $i \neq j$. Entonces para cualquier $(r_1, \ldots, r_n) \in \mathbb{Z}^n$ existe un $x \in \mathbb{Z}$ con $x \equiv r_i \pmod{z_i}$ para $i = 1, 2, \ldots, n$. Si x' es otra solución, entonces $x - x' \in z_1 z_2 \cdots z_n \mathbb{Z}$.

(b) Encuentra todos los $x \in \mathbb{Z}$ que cumplan las siguientes 4 congruencias: $x \equiv 1 \pmod 7$, $x \equiv 2 \pmod 8$, $x \equiv 3 \pmod 9$, $x \equiv 4 \pmod{11}$.

A discutir en la Ayudantía a partir del **7 de Octubre**.