

Álgebra Moderna Clase 11

Tomás Ricardo Basile Álvarez
316617194

24 de noviembre de 2020

Ejercicio 9.10

a) Sea $a \in G$ y G finito. Entonces $a^{|G|} = e$

Digamos que el orden de a es n , entonces, $a^n = e$. Además, entonces la cardinalidad de $\langle a \rangle$ es n . Pero como $\langle a \rangle$ es un subgrupo de G , por el teorema de Lagrange tenemos que $|\langle a \rangle|$ divide a $|G| \Rightarrow n$ divide $|G|$ y entonces existe un entero k tal que $|G| = kn$. Luego:

$$a^{|G|} = a^{nk} = (a^n)^k = e^k = e$$

b) Sea G finito y $H \leq G$ tal que $[G : H] = 2$. Probar que $x^2 \in H \forall x \in G$

Sea $x \in G$. Si $x \in H$, entonces claramente $x^2 \in H$ porque H es un grupo.

Si $x \notin H$, entonces consideramos el conjunto xH . Como $[G : H] = 2$, entonces la partición inducida por \sim_H separa a G en dos clases de equivalencia.

En particular, como $x \notin H$, y como $x = xe \in xH$ (porque $e \in H$), entonces xH y H son disjuntos y por tanto son los dos conjuntos que forman la partición de G .

Consideramos ahora el conjunto x^2H . Como las clases de equivalencia o son disjuntas o son iguales, el conjunto x^2H tiene que ser igual a H o igual a xH (porque estos dos forman la partición de G).

Suponemos que $x^2H = xH$. Como $x^2 = x^2e \in x^2H$, entonces $x^2 \in xH$, lo que implica que existe una $h \in H$ tal que $x^2 = xh$, de donde se deduce que $h = x$ y por tanto $x \in H$, una contradicción.

Por lo tanto, x^2H tiene que ser igual a H . En este caso, como $x^2 \in x^2H$, entonces $x^2 \in H$.

d) Prueba o da un contraejemplo de las siguientes afirmaciones

d1) Si $|G|$ es un entero primo, entonces $G \simeq \mathbb{Z}_p$

Sí. Como vimos en las notas, si G es de orden primo, entonces es cíclico y por tanto, existe un $a \in G$ tal que $G = \langle a \rangle$. Por otro lado, consideramos \mathbb{Z}_p donde $p = |G|$ también es cíclico, pues es igual a $\langle \bar{1} \rangle$.

Consideramos ahora la función $f : G \rightarrow \mathbb{Z}_p$ definida como $\forall a^k \in G$ (todos los elementos de G tienen esta forma para $k \in \mathbb{Z}$ porque G es cíclico), $f(a^k) = \bar{k}$

Probamos que es un isomorfismo:

- **Morfismo:** Sean $a^m, a^n \in G$ con $m, n \in \mathbb{Z}$ dos elementos arbitrarios de G . Entonces:
$$f(a^m \cdot a^n) = f(a^{m+n}) = \overline{m+n} = \bar{m} + \bar{n} = f(a^m) + f(a^n).$$
- **Inyectiva:** Si $a^n \neq a^m$ en G , quiere decir que $a^{n-m} \neq e_G$. Y por tanto $n-m$ no es múltiplo de $|G| = p$. Porque en $G = \langle a \rangle$, los elementos que son iguales a e_G son a^{kp} .
Entonces, $f(a^n) = \bar{n}$, $f(a^m) = \bar{m}$. Y como $n-m$ no es múltiplo de p , entonces $\bar{n} \neq \bar{m}$ y por tanto $f(a^n) \neq f(a^m)$
- **Suprayectiva:** Sea $\bar{k} \in \mathbb{Z}_p$, entonces existes $a^k \in G$ tal que $f(a^k) = \bar{k}$

d3) Si |