Tarea I

Nicholas Mc-Donnell

2do semestre 2017

Índice

1. Grupos

1.3

Let S be a set with an associative law of composition and with an identity element. Prove that the subset of S consisting of the invertible elements is a group.
Dem: Primero, la identidad pertenece al conjunto de los invertibles:

$$e \circ e = e \quad \text{/Por definición de la identidad}$$

$\therefore$ La operación es asociativa por definición.
Clausura sobre el subconjunto:
Se asume que existen elementos invertibles a y b, tal que $a \circ b$ no es invertible.

$$\begin{aligned} (a \circ b) \circ b^{-1} = a \quad & \text{Asociatividad e invertiblidad de } b \\ \left((a \circ b) \circ b^{-1}\right) \circ a^{-1} &= e \\ (a \circ b) \circ \left(b^{-1} \circ a^{-1}\right) &= e \\ \implies a \circ b \text{ es invertible} & \\ \implies \circ \text{ es cerrado sobre los invertibles} & \end{aligned} \tag{1}$$

Esto implica que los invertibles de S son un grupo.

1.11

Let G be a group with multiplication notation, we define an opposite group G° with law of composition $a \circ b$ as follows: The underlying set is the same as G, but the law of composition is the opposite, that is, we define $a \circ b = ba$.
Prove that this defines a group.
Dem:

1. Clausura, $a, b \in G^\circ$
   $ab \in G$
   $\therefore b \circ a \in G^\circ$

2. Asociatividad, $a, b, c \in G^\circ$
   $(a \circ b) \circ c = (ba) \circ c = cba = a \circ (cb) = a \circ (b \circ c)$

3. Identidad, $e \in G \implies e \in g^\circ$
   $\therefore \forall a \in G^\circ$
   $e \circ a = ae = a = ea = a \circ e$

4. Inverso, $\forall a \in G, \exists a^{-1} \in G : aa^{-1} = e = a^{-1}a$
   $\therefore a \circ a^{-1} = a^{-1}a = e = aa^{-1} = a^{-1} \circ a$

G° es un grupo.

2. Subgrupos

2.3

Which of the following are subgroups:

(a) $GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$
Dem:

1. Clausura, la multiplicación de matrices en $\mathbb{R}$ es cerrada, por consecuencia de que la multiplicación en $\mathbb{R}$ es cerrada.
2. Asociatividad, se hereda de $GL_n(\mathbb{C})$
3. Identidad, la matriz identidad es una matriz con det = 1 y con coeficientes 1 y 0. Por ende la matriz pertenece a $GL_n(\mathbb{R}$
4. Invertibilidad, ya que todas las matrices en $GL_n(\mathbb{R})$ cumplen que det $\neq 1$, están son invertibles.

(b) $\{1, -1\} \subset \mathbb{R}^\times$
Dem:

1. Clausura
   $1 \times 1 = 1, 1 \times (-1) = -1$
2. Asociatividad, se hereda de los Reales.
3. Identidad, $1 \times (-1) = -1 = (-1) \times 1$ además $1 \times 1 = 1$
4. Invertibilidad, $1 \times 1 = 1 = (-1) \times (-1)$

Lo que implica que $\{1, -1\}$ es subgrupo.

(c) The set of all positive integers in $\mathbb{Z}^+$
Dem:
0 no es mayor a 0, por ende el neutro aditivo no pertenece a los enteros positivos, lo que a su vez implica que no son subgrupo.

(d) The set of all positive reals in $\mathbb{R}^\times$

1. Clausura, por propiedad de los reales, $a, b > 0 \implies ab > 0$
2. Asociatividad, se hereda de los reales
3. Identidad, $1 > 0$ y 1 es la identidad en los reales
4. Invertibilidad, sea $a > 0$, se sabe que $\forall x \in \mathbb{R} : x^2 \geq 0$, por lo que $0 < a(a^{-2}) = a^{-1}$, por lo que los elementos son invertibles.

Lo que implica que son subgrupo.

(e) The set of all matrices $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$, with $a \neq 0$, in $GL_2(\mathbb{R})$

1. Clausura
   Sean $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}$
   $AB = \begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix} = BA$ el cual es de la forma deseada, además la operación es conmutativa

2. Asociatividad, se hereda
3. Identidad, sea $I = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

   $\therefore AI = IA = \begin{bmatrix} 1 \cdot a & 0 \\ 0 & 0 \end{bmatrix} = A$ por ser conmutativa.
4. Invertibilidad

   Sean $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}, a^{-1} \in \mathbb{R} : a^{-1}a = 1 = aa^{-1}$

   Luego, sea $A^{-1} = \begin{bmatrix} a^{-1} & 0 \\ 0 & 0 \end{bmatrix}$

   $\therefore AA^{-1} = A^{-1}A = \begin{bmatrix} a \cdot^{-1} & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = I$

Es grupo, pero no subgrupo, ya que no es subconjunto.

2.11

Prove that in any group the order of ab and of ba are equal.
Dem:
Sea n el orden de a y m el orden de b.
Si n o m son infinito el orden de ab y de ba es el mismo, infinito.
Si n y m son finitos, sea k el orden de ba y q el orden de ab, luego:

$$(ab)^{k+1} = (ab)(ab)...(ab) \quad k+1 \text{ veces}$$

Luego asociando:

$$(ab)^{k+1} = a(ba)...(ba)b \quad k \text{ veces}$$

Lo que implica que:

$$(ab)^{k+1} = aeb = ab$$

Aplicando inverso:

$$(ab)^{k+1}(ab)^{-1} = (ab)^k = e$$

Esto es, k es multiplo de q, por lo mismo $q \leq k$
Usando un argumento análogo $k \leq q$, lo que implica que $k = q$, en otras palabras el orden de ab y de ba es el mismo.

2.17

Prove that a group in which every element except the identity has order 2 is abelian.
Dem:

$$\forall a \in G, a^2 = e \implies a = a^{-1}$$

Sean $a, b \in G$:

$$(ab)(ba) = e$$

Además, por la implicancia recién mostrada:

$$ab = ba$$

Lo que implica que G es abeliano.

2.21

Prove that the set of elements of finite order in an abelian group is a subgroup.
Dem:

1. Clausura
   Sean $a, b \in S, a^n = e, b^m = e\, n, m \in \mathbb{N}$
   Se define $q = \text{mín}\{p \in \mathbb{N} : p = nk = ml,\ k, l \in \mathbb{N}\}$

$$a^q b^q = ee = e$$

$$\therefore (ab)^q = (ab)(ab)...(ab) \quad q \text{ veces}$$

$$\therefore (ab)^q = (aa...a)(bb...b) \quad q \text{ veces, por conmutatividad}$$

$$\implies (ab)^q = a^q b^q = e$$

$$\implies ab \in S$$

2. Asociatividad, se hereda
3. Identidad, $e^1 = e \implies e \in S$
4. Invertibilidad, sea $a \in S, a^n = e \implies aa^{n-1} = e \implies a^{-1} = a^{n-1}$

3. Isomorfismos

3.3

Let a, b be elements of a group G, and let $a' = bab^{-1}$. Prove that $a' = a$ if and only if a and b conmute.
$\implies$

$$a = a' \iff a = bab^{-1} \quad / \cdot b$$

$$\iff ab = ba$$

a y b conmutan.
Los pasos son reversibles.

3.11

Prove that the set Aut G of automorphisms of a group G forms a group, the law of composition being composition of functions.
Dem:

$$AutG \subset S_{|G|} = \{\text{Las biyecciones de } G \text{ en si mismo}\}$$

Por definición de automorfismo.

- Clausura: Sean $\varphi, \tau \in AutG$

$$\therefore \varphi(ab) = \varphi(a)\varphi(b) \in G, \tau(ab) = \tau(a)\tau(b) \in G, \forall a, b \in G$$

$$\varphi \circ \tau(ab) = \varphi(\tau(a)\tau(b)) = \varphi(\tau(a))\varphi(\tau(b)) \in G, \forall a, b \in G$$

$$\implies \varphi \circ \tau \in AutG$$

- Asociatividad: Se hereda
- Identidad: Sea Id_G la función identidad, la cual cumple lo siguiente $Id_G(a) = a, \forall a \in G$, entonces $Id_G(ab) = ab = Id_G(a)Id_G(b)$, luego la función identidad es automorfismo, lo que implica que $Id_G \in AutG$
- Invertibilidad: Los automorfismos son morfismos biyectivos, lo que implica que $\forall \varphi \in AutG \, \exists \varphi^{-1} \in S_{|G|} : \varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = Id_G$, por lo que solo hay que demostrar que el inverso es isomorfismo:

$$\varphi(ab) = \varphi(a)\varphi(b)$$

$$\varphi^{-1} \circ \varphi(ab) = ab = \varphi^{-1} \circ \varphi(a)\varphi^{-1} \circ \varphi(b)$$

Sea $\varphi(a) = c, \varphi(b) = d$

$$\varphi^{-1} \circ \varphi(ab) = \varphi^{-1}(c)\varphi^{-1}(d)$$

$$\varphi^{-1} \circ \varphi(ab) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(cd)$$

$$\implies \varphi^{-1}(cd) = \varphi^{-1}(c)\varphi^{-1}(d)$$

$$\implies \varphi^{-1} \in AutG$$

3.13

(a) Let G be group of order 4. Prove that every element in G has order 1, 2, or 4.

(b) Classify groups of order 4 by considering the following two cases:

(I) G contains an element of order 4

(II) Every element of G has order < 4

(a) Esto es equivalente a demostrar que en todo grupo de orden 4, no hay elemento de orden 3. Dem: Supongamos que $\exists x \in G : x^3 = e$

$$\{e, x, x^2, y\} = G$$

Lo que implica que y es de orden 2 (si no su inverso pertenece a $G \implies \rightarrow\leftarrow$), tomemos el elemento xy, este tiene que pertenecer a G, pero no puede ser la identidad ($xy = e \implies x = y^{-1} \rightarrow\leftarrow$), tampoco puede ser x ($xy = x \implies y = e \rightarrow\leftarrow$), tampoco puede ser x^2 ($xy = x^2 \implies x = y \rightarrow\leftarrow$) y por ultimo no puede ser y ($xy = y \implies x = e \rightarrow\leftarrow$).

$$\rightarrow\leftarrow$$

Por lo que no hay elementos de orden 3 en un grupo de orden 4

(b) Se toman los siguientes grupos:

(I) $G = \{e, x, x^2, x^3\} =< x >$

(II) $G = \{e, x, y, xy\} =< x, y >$, todos los elementos, excepto la identidad, son de orden 2

Todos los otros grupos son isomorfos al primero, o al segundo

4. Homomorfismos

4.3

Prove that the kernel and image of homomorphism are subgroups.
Dem: Sea $\varphi : G \to H$ homomorfismo.
El kernel:

$$\ker \varphi = \{a \in G : \varphi(a) = e_H\}$$

1. Clausura: Sean $a, b \in \ker \varphi$

$$\varphi(ab) = \varphi(a)\varphi(b) = e_H e_H = e_H$$
$$\implies ab \in \ker \varphi$$

2. Asociatividad: Se hereda

3. Identidad: por propiedad de los homomorfismos $\varphi(e_G) = e_H$

$$\therefore e_G \in \ker \varphi$$

4. Invertibilidad: Sea $a \in \ker \varphi$

$$e_H = \varphi(e_G) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^-1) = e_H\varphi(a^{-1}) = \varphi(a^{-1})$$
$$\therefore \varphi(a^{-1}) = e_H \implies a^{-1} \in \ker \varphi$$

$$\implies \ker \varphi < G$$

La imagen:

$$\varphi(G) = \{a \in H : \exists b \in G, \varphi(b) = a\}$$

1. Clausura: Sean $a, b \in \varphi(G)$

$$\implies \exists c, d \in G : \varphi(c) = a, \varphi(d) = b$$
$$\therefore \varphi(cd) = \varphi(c)\varphi(d) = ab$$
$$\implies ab \in \varphi(G)$$

2. Asociatividad: se hereda

3. Identidad: Por propiedad de homomorfismos $\varphi(e_G) = e_H$

$$\implies e_H \in \varphi(G)$$

4. Invertibilidad: Sea $a \in \varphi(G)$

$$\implies \exists b \in G : \varphi(b) = a$$

Se toma b^{-1}:

$$e_H = \varphi(e_G) = \varphi(bb^{-1}) = \varphi(b)\varphi(b^{-1} = a\varphi(b^{-1})$$
$$\implies \varphi(b^{-1}) = a^{-1} \implies a^{-1} \in \varphi(G)$$

$$\implies \varphi(G) < H$$

4.7

Prove that the absolute value map $||:\mathbb{C}^\times \to \mathbb{R}^\times$ sending $a \mapsto |a|$ is a homorphism, and determine its kernel and image.
Notación: Para facilitar la lectura $|,|$ sera usada como φ Dem: Sea $x, y \in \mathbb{C}$

$$\varphi(x)\varphi(y), \varphi(xy) \in \mathbb{R}$$

$$x = a + bi, y = c + di$$

$$\varphi(x) = \sqrt{a^2+b^2}, \varphi(y) = \sqrt{c^2+d^2}$$

$$xy = ac - bd + i(ad + bc) \implies \varphi(xy) = \sqrt{(ac-bd)^2 + (ad+bc)^2}$$

$$\therefore \varphi(xy) = \sqrt{(ac)^2 - 2abcd + (bd)^2 + (ad)^2 + 2abcd + (bc)^2} = \sqrt{(ac)^2 + (bd)^2 + (ad)^2 + (bc)^2}$$

$$\implies \varphi(xy) = \sqrt{a^2(c^2+d^2) + b^2(c^2+d^2)} = \sqrt{(a^2+b^2)(c^2+d^2)} = \sqrt{a^2+b^2}\sqrt{c^2+d^2} = \varphi(x)\varphi(y)$$

$$\implies \varphi(xy) = \varphi(x)\varphi(y)$$

Lo que implica que el mapeo de valor absoluto es homomorfismo.
Luego el kernel y la imagen del mapeo son las siguientes:

$$\ker\varphi = \{z \in \mathbb{C}^\times : \varphi(z) = 1\} = \{z \in \mathbb{C}^\times : \Re(z)^2 + \Im(z)^2 = 1\} = \{z \in \mathbb{C}^\times : z\bar{z} = 1\} = \{z \in \mathbb{C}^\times : z = \bar{z}^{-1}\}$$

$$\varphi(\mathbb{C}) = \{x \in \mathbb{R}^\times : \exists z \in \mathbb{C}^\times, \varphi(z) = x\} = \mathbb{R}^\times_{>0} \quad \varphi(x) \geq 0 \forall x, 0 \notin \mathbb{C}^\times \implies \varphi(x) > 0 \forall x \in \mathbb{C}^\times$$

4.13

(a) Let H be a subgroup of G, and let $g \in G$. The *conjugate subgroup* gHg^{-1} is defined to be the set of all conjugates ghg^{-1}, where $h \in H$. Prove that gHg^{-1} is a subgroup of G

(b) Prove that a subgroup H of a group G is normal if and only if $gHg^{-1} = H$ for all $g \in G$.

Dem:

(a) Sea $g \in G$, $gHg^{-1} = \{ghg^{-1} : h \in H\}$

1. Clausura: Sea $a, b \in H$

$$gag^{-1}, gbg^{-1} \in gHg^{-1}$$

$$\therefore gag^{-1}gbg^{-1} = gaebg^{-1} = gabg^{-1}$$

$$ab \in H \implies gabg \in gHg^{-1}$$

$$\implies gag^{-1}gbg^{-1} \in gHg^{-1}$$

2. Asociatividad: Se hereda
3. Identidad: Sea $e \in H$

$$geg^{-1} = gg^{-1} = e \in gHg^{-1}$$

4. Invertibilidad: Sea $a, a^{-1} \in H$

$$gag^{-1}, ga^{-1}g^{-1} \in gHg^{-1}$$

$$\therefore gag^{-1}ga^{-1}g^{-1} = gaea^{-1}g^{-1} = gaa^{-1}g^{-1} = geg^{-1} = e$$

$$\implies (gag^{-1})^{-1} \in gHg^{-1}$$

$$\implies gHg^{-1} < G$$

(b) Recordemos la definición de subgrupo normal: $N \lhd G \iff \forall n \in N, \forall g \in G : gng^{-1} \in N$

$\implies$

$\subseteq$

$$\forall h \in H, \forall g \in G : ghg^{-1} \in H \implies \forall g \in G, gHg^{-1} \subseteq H \quad \text{Por definición de } gHg^{-1}$$

$\supseteq$

Ya que $H \lhd G$, se toma g^{-1}.

$$g^{-1}hg = h' \in H$$
$$\implies h = gh'g^{-1} \in H \implies H \subset gHg^{-1}$$
$$\implies gHg^{-1} = H$$

$\impliedby$

$$H = gHg^{-1} \quad \forall g \in G \implies \forall g \in G, \forall h \in H : ghg^{-1} \in H$$
$$\implies H \lhd G$$

5. Relaciones de equivalencia y particiones

5.3

Determine the number of equivalence relations on a set of five elements.

Dem:

Notar que el numero de relaciones de equivalencia en un conjunto de cinco elementos, es la cantidad de particiones del mismo. Esto es la cantidad de formas que se puede separar en 1,2,3,4 y 5 partes. Se puede tomar la siguiente función recursiva que da las particiones de un conjunto de n elementos en k partes:

$$P : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

$$P(n,k) = P(n-1,k-1) + k \cdot P(n-1,k)$$

Donde $P(a,a) = 1$, $P(n,1) = 1$ y $P(n,k) = 0, n < k$.

Esto se explica de la siguiente forma:

Al dividir un conjunto de n elemento en n partes solo puedes dividirlo tomando n subconjuntos de tamaño 1, similarmente cuando divides el conjunto en 1 parte solo puedes tomar un subconjunto, el conjunto mismo. Por ultimo no puedes participar un conjunto en más partes que elementos, por ende hay 0 formas de hacer esto.

El caso recursivo se ve al notar que, dividir un conjunto en k partes, es lo mismo que, dividir el conjunto de $n-1$ elementos en $k-1$ partes y después agregar el elemento n como otra partición, o dividir el conjunto de $n-1$ elemento en k partes, y después elegir una de las k partes donde poner el elemento n.

Puesto de otra manera, la cantidad de formas de particionar un conjunto de n elementos en k partes, es la cantidad de formas que puedes particionar el mismo conjunto sin 1 elemento en $k-1$ partes y después agregar la partición del elemento por separado, más la cantidad de formas que puedes particionar el mismo conjunto sin 1 elemento en k partes y después poner el elemento en alguna de las k particiones (o sea, k veces la cantidad de formas de particionar $n-1$ elementos k veces). Y esto es como se define la función.

Tomando un ejemplo, $P(4,2)$:
Viendo las posibles particiones del conjunto $\{a,b,c,d\}$:

$$[d, abc]$$

$$[a, bcd], [ad, bc]$$

$$[b, acd], [bd, ac]$$

$$[a, bcd], [ad, bc]$$

Notemos que, la primera forma particionamos 3 elementos en 1 partición y después pusimos el elemento restante como parte de la partición faltante. En el resto de las formas, particionamos el subconjunto $\{a,b,c\}$ en 2 partes y después agregamos la partición restante a una de las particiones, como hay dos posibles particiones cada forma tiene dos variaciones.
Ahora la formula nos da los siguiente:

$$P(4,2) = P(3,1) + 2 \cdot P(3,2) = P(3,1) \cdot (P(2,1) + 2 \cdot P(2,2))$$

$$P(n,n) = 1, P(n,1) = 1 \implies P(4,2) = 1 + 2 \cdot (1 + 2 \cdot 1) = 1 + 2 \cdot 3 = 7$$

Aquí se ve que la formula da el resultado esperado.
Por lo que aplicando la formula para $n = 5$ y para $k = 1, 2, 3, 4, 5$, y sumando los resultados nos da lo siguiente:

$$\sum_{i=1}^{5} P(5,i) = P(5,1) + P(5,2) + P(5,3) + P(5,4) + P(5,5)$$

$$\therefore \sum_{i=1}^{5} P(5,i) = 1 + (P(5,1) + 2 \cdot P(4,2)) + (P(4,2) + 3 \cdot P(4,3)) + (P(4,3) + 4 \cdot P(4,4)) + 1$$

Usando lo ya calculado y la definición de la función:

$$\therefore \sum_{i=1}^{5} P(5,i) = 2 + (1 + 2 \cdot 7) + (7 + 3 \cdot (P(3,2) + 3 \cdot P(3,3))) + ((P(3,2) + 3 \cdot P(3,3)) + 4 \cdot 1)$$

Sumando los términos y usando valores calculados anteriormente:

$$\therefore \sum_{i=1}^{5} P(5,i) = 2 + 15 + 7 + 3 \cdot (3 + 3 \cdot 1) + (3 + 3 \cdot 1) + 4$$

$$\therefore \sum_{i=1}^{5} P(5,i) = 28 + 3 \cdot 6 + 6$$

$$\therefore \sum_{i=1}^{5} P(5,i) = 34 + 18$$

$$\therefore \sum_{i=1}^{5} P(5,i) = 52$$

Por lo que hay 52 relaciones de equivalencia en un conjunto de 5 elementos

5.9

Describe the smallest equivalence relation on the set of real numbers which contains the line $x - y = 1$ in the (x, y)-plane, and sketch it.
Tomemos la siguiente relación $x \sim y \iff x - y \in \mathbb{Z}$. Veamos que esta es relación de equivalencia:

- Transitividad: Sea $a, b, c \in \mathbb{R}$ y $a \sim b, b \sim c$

$$\implies a - b \in \mathbb{Z}, b - c \in \mathbb{Z}$$

$$\therefore (a - b) + (b - c) = a - c \in \mathbb{Z}$$

  Por clausura de la suma en los enteros.

$$\implies a \sim c$$

- Simetria: $a, b \in \mathbb{R}, a \sim b \implies a - b \in \mathbb{Z}$ por la invertibilidad de los enteros $b - a \in \mathbb{Z} \implies b \sim a$
- Reflexiva: $a \in \mathbb{R}$, luego $a - a = 0 \in \mathbb{Z} \implies a \sim a$, a es arbitrario por lo que se cumple para todos los números reales

La recta $L = \{(x, y) \in \mathbb{R}^2 : x - y = 1\}$ esta contenida, ya que son todos los puntos cuya resta es 1, el cual es un numero entero.
Ahora asumamos que hay otra relación de equivalencia, R, más pequeña que esta, y que ademas contenga esa recta.

$$\therefore (x, y) \in L \implies xRy$$

Por propiedad simétrica:

$$xRy \implies yRx$$

Sabemos que $x - y = 1 \implies y - x = -1$, entonces sea $L' = \{(x, y) \in \mathbb{R}^2 : x - y = -1\}$

$$\therefore (x, y) \in L' \cup L \implies xRy$$

De nuevo por propiedad transitiva:

$$(x, y), (y, z) \in L \cup L' \implies x - y = \pm 1, y - z = \pm 1 \implies xRy, yRz \implies xRz, x - z \in \{-2, 0, 2\}$$

Esto se puede extender de la siguiente forma:

$$xRy, yRz \implies yRz, x - y, y - z \in \{-2, -1, 0, 1, 2\} \implies x - z \in \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$$

Se denota al conjunto $\{-a_n, .., 0, ..., a_n\} = A_n \subseteq \mathbb{Z}, a_n = 2^n$
Por inducción, claramente:

$$xRy, yRz \implies x - y, y - z \in A_n, xRz \implies x - z \in A_{n+1}$$

Por ende $\forall (x, y) \in \mathbb{R}^2 : xRy \implies x - y \in \mathbb{Z}$, la cual es la relación de equivalencia propuesta, ya que demostramos que cualquier releí de equivalencia que contenga a L ademas contiene la relación propuesta, esa relación es la mas pequeña.

6. Clases laterales

6.3

Prove that every group whose order is a power of a prime p contains an element of order p Dim: Por teorema de Lagrange $x \in G, |G| = n, |x| = k \implies k|n$.

$$n = p^l \implies k|p^l$$

Esto implica que $k = p^a, a|l$.
Por clausura $< x > \subseteq G$, luego se toma el elemento $x^{p^{a-1}}$.
Notar que $(x^{p^{a-1}})^p = x^{p^{a-1}p} = x^{p^a} = e$, por lo que el orden de este elemento es p.

6.5

Let H, K be subgroups of a group G of orders $3, 5$ respectively. Prove that $H \cap K = \{e\}$
Sea $x \in H \cap K$

$$\implies x \in H \wedge x \in K$$

Denotemos $|x| = n, |H| = m, |K| = l$ y por el teorema de Lagrange:

$$n|m \wedge n|l$$

Pero $\text{mcd}(3, 5) = 1 \implies n = 1$, por ende:

$$H \cap K = \{e\}$$

6.9

Let H be a subgroup of G. Prove that the number of left cosets is equal to the number of right cosets (a) if G is finite and (b) in general.

7. Restricciones de homomorfismos a subgrupos

7.1

Let G and G' be finite groups whose order have no common factor. Prove that the only homomorhpism $\varphi : G \to G'$ is the trivial one $\varphi(x) = e$ for all x. Dem: Sea k, l, m, n los ordenes de $G, G', \ker\varphi, \varphi(G)$ respectivamente. Se sabe que $\varphi G \subseteq G'$
Lo que implica por teorema de Lagrange:

$$n|l$$

Ademas se sabe que $k = m \cdot n$

$$\implies n|k \wedge n|l$$

Y se sabe que $\text{mcd}(k, l) = 1$

$$\implies n|1 \implies n = 1$$

En otras palabras el orden de $\varphi(G)$ es 1, lo que implica que solo $e \in \varphi(G)$, lo que a su vez implica que el único homomorfismo posible es $\varphi(x) = e$

7.7

Prove that a group of order 30 can at most have 7 subgroups of order 5.
Dem: Por corolario del Teorema de Lagrange todo grupo de orden p, donde p es un primo, es isomorfo al grupo $\mathbb{Z}/p\mathbb{Z}$, como consecuencia son grupos cíclicos y generados por uno de sus elementos.
Luego, supongamos que un grupo de orden 30 puede contener 8 subgrupos distintos de orden 5, $H_1, H_2, ..., H_8$, donde $H_j \cap H_i = \{e\}, \forall i \neq j$.
Si no es así, $|H_k \cap H_l| \geq 2 \implies \exists x \in H_k \cap H_l \implies x^2 \in H_k \cap H_l \implies ... \implies x^4 \in H_k \cap H_l \implies H_k = H_l$ por clausura en cada conjunto por separado, pero esto es una contradicción, ya que estos eran distintos entre si.
Entonces, se sabe que

$$\bigcup_{i=1}^{8} H_i = \{e\} \cup \bigsqcup_{i=1}^{8} H_i \setminus \{e\} \subseteq G$$

Luego notamos que

$$|G| \geq |\bigcup_{i=1}^{8} H_i| = |\{e\} \cup \bigsqcup_{i=1}^{8} H_i \setminus \{e\}| = 1 + |\bigsqcup_{i=1}^{8} H_i \setminus \{e\}|$$

Sabemos que $|H_i| = 5$

$$\implies |H_i \setminus \{e\}| = 4$$

Por ende

$$|G| \geq 1 + \sum_{i=1}^{8} 4 = 1 + 4 \cdot 8 = 33$$

Pero G era de orden 30

$$\rightarrow\leftarrow$$

Notar que $29 = 1 + 4 \cdot 7$, por lo que pueden haber 7 subgrupos de orden 5 en un grupo de orden 30, pero no más.

8. Producto de grupos

8.3

Prove that a finite cyclic group of order rs is isomorphic to the product of cyclic groups of orders r and s if and only if r and s have no common factor.
Dem: Se sabe que todo grupo ciclico de orden n es isomorfo a $\mathbb{Z}/n\mathbb{Z}$, por ende en esta demostración se va a trabajar con grupos de esa forma.
Se toman

$$\varphi : \mathbb{Z}/rs\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$$

$$x \mapsto (x \mod r, x \mod s)$$

$$\tau : \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z} \to \mathbb{Z}/rs\mathbb{Z}$$

$$(a, b) \mapsto -(as + br) \mod rs$$

8.7

(a) Let H, K be subgroups of a group G. Show that the set of products $HK = \{hk : h \in H, k \in K\}$ is a subgroup if and only if $KH = HK$.

(b) Give an example of a group G and two subgroups H, K such that HK is not a subgroup.

Dem:

(a) $\implies$

$\subseteq$ Sea $a \in HK$

$$\implies \exists h \in H, \exists k \in K : a = hk$$

Luego $a^{-1} \in HK$, ya que es grupo.

$$\implies \exists h' \in H, \exists k' \in K : a^{-1} = h'k'$$

$$\therefore k^{-1}h^{-1} = h'k' \implies$$

Por definición de HK

Ya que a, b son arbitrarios

$$\implies HK = KH$$

$\impliedby$

Si $HK = KH \implies \forall h \in H, \forall k \in K : hk, kh \in HK$

1. Clausura, sean $h, h' \in H, k, k' \in K$

$$hk, h'k' \in HK$$

$$kh' \in KH \implies kh' \in HK$$

$$he, ek \in HK \implies h, k \in HK$$

$$\therefore hkh'k' = h(kh')k'$$

2. Asociatividad, se hereda.
3. Identidad, $e \in H, e \in K$ por definición de subgrupo, luego $ee = e \implies e \in HK$
4. Invertibilidad, sean $h \in H, k \in K \implies hk \in HK$, luego ya que $HK = KH$

$$k^{-1}h^{-1} \in KH$$

$$\therefore (hk)^{-1} \in HK$$

(b)

9. Aritmetica modular

9.3

(a) Prove that 2 has no inverse modulo 6

(b) Determine all integers n such that 2 has an inverse modulo n

Dem:

(a) Sea $k \in \mathbb{Z}$

$$\therefore 2k \equiv 0 \mod 6 \vee 2k \equiv 2 \mod 6 \vee 2k \equiv 4 \mod 6$$

$$\implies \nexists k \in \mathbb{Z} : 2k \equiv 1 \mod 6$$

Puesto de otro modo 2 no tiene inverso modular

(b) Sea $n, k \in \mathbb{Z}$

$$2n = pq + r, 2k = p'q' + r'$$

Luego sea $p = p' = 2l, l \in \mathbb{Z}$

$$\implies 2n = 2lq + r, 2k = 2lq' + r'$$

$$\therefore r = 2(n - lq), r' = 2(k - lq') \quad r, r' \text{ son multiplos de 2}$$

$$\implies 2n \equiv 2(k + e) \mod 2l \quad \big(2n - 2k = 2l(q - q') + r - r', r - r' = 2e\big)$$

En modulos pares, para todo $n \in \mathbb{Z}$, $2n$ es congruente con otro número par.

$$\implies \nexists n \in \mathbb{Z} : 2n \equiv 1 \mod 2l$$

Tomando el otro caso $p = p' = 2l + 1, l \in \mathbb{Z}$

$$\implies 2n = (2l + 1)q + r, 2k = (2l + 1)q' + r'$$

$$\therefore r = 2(n - lq) - q, r' = (k - lq') - q'$$

r, r' son múltiplos de 2 solo si q y q' son múltiplos de 2 respectivamente

$$\implies 2n \equiv 2k + e \mod 2l + 1 \quad \big(2n - 2k = (2l + 1)(q - q') + r - r', e = r' - r\big)$$

Por lo que eligiendo bien un n, podemos generar todos los números pares e impares, en particular se puede generar el 1. Lo que implica que para todos los enteros impares existe un inverso modular, puesto de otra manera, para todos los enteros que son coprimos con 2 existe inverso modular.

Nota: Usando la identidad de bézout, uno llega mucho más rápido al resultado pedido. En ambas preguntas.

9.7

Prove the associative and conmutative laws for multiplication in $\mathbb{Z}/n\mathbb{Z}$
Dem: Sean $a, b, c \in \mathbb{Z}/n\mathbb{Z}$.

$$\exists \varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \quad \text{homomorfismo}$$

Ya que $\mathbb{Z}/n\mathbb{Z}$ son clases de equivalencia de $\mathbb{Z}$
Sean $a, b, c \in \mathbb{Z}$

$$\therefore a(bc) = (ab)c = (ba)c$$

$$\varphi(a(bc)) = \varphi(a)\varphi(bc) = \varphi(a)(\varphi(b)\varphi(c))$$

$$\varphi((ab)c) = \varphi(ab)\varphi(c) = (\varphi(a)\varphi(b))\varphi(c)$$

$$\varphi((ba)c) = \varphi(ba)\varphi(c) = (\varphi(b)\varphi(a))\varphi(c)$$

$$\implies \varphi(a)(\varphi(b)\varphi(c)) = (\varphi(a)\varphi(b))\varphi(c) = (\varphi(b)\varphi(a))\varphi(c)$$

$$\implies \bar{a}(\bar{b}\bar{c}) = (\bar{a}\bar{b})\bar{c} = (\bar{b}\bar{a})\bar{c}$$

Como a, b, c son arbitrarios, la operación es asociativa para todo elemento en $\mathbb{Z}/n\mathbb{Z}$
Se fija $c = 1$

$$\implies (\bar{a}\bar{b})\bar{1} = (\bar{b}\bar{a})\bar{1}$$

$$\implies \bar{a}\bar{b} = \bar{b}\bar{a}$$

Como a, b son arbitrarios, la operación es conmutativa.

10. Grupos Cocientes

10.5

10.7

10.11