TAREA 1

KEVIN VELEZ

7.1 BASIC DEFINITIONS AND EXAMPLES

Problema 1 (13). *An element x in R is called* nilpotent *if $x^m = 0$ fo some $m \in \mathbb{Z}^+$*

1. *Show that if $n = a^k b$ form some integers a and b then ab is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$.*
2. *If $a \in \mathbb{Z}$ is an integer, show that the element $a \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if every prime divisor of n is also a divisor of a. In particular, determine the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ explicitly.*
3. *Let R be the ring of functions from a nonempty set X to a field F. Prove that R contains no nonzero nilpotent elements.*

Demostración.

1. Let $n = a^k b$ for some integers a and b. Then
$$(ab)^k = a^k b^k = (a^k b) b^{k-1} = n b^{k-1} \equiv 0 \mod n$$
2. Suppose $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent. Then $\overline{a}^k = \overline{0}$ for some $k \in \mathbb{Z}^+$. Then $a^k \equiv 0 \mod n$, so $n|a^k$. Now, if p is a prime divisor of n, then $p|a^k$ and therefore $p|a$.

   Now, Suppose that every prime divisor of n is a divisor of a. let $n = {p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k}$ and $a = {p_1}^{\beta_1} \cdots {p_k}^{\beta_k} m$ where $1 \leq \alpha_i, \beta_i$ for all i and for some integer m. Let $s = \max \alpha_i$. Then
$$a^s = \left({p_1}^{\beta_1} \cdots {p_k}^{\beta_k} m\right)^s = {p_1}^{\beta_1 s} \cdots {p_k}^{\beta_k s} m^s$$
   where $\beta_i s \geq \alpha i$, thus
$$a^s = n {p_1}^{\beta_1 s - \alpha_1} \cdot {p_k}^{\beta_k s - \alpha_k} m$$
   And therefore $a \equiv 0 \mod n$

   $72 = 2^3 3^2$, then the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ are $\{0, 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66\}$.
3. Suppose $\alpha \in R$ is nilpotent. If $\alpha \neq 0$, then exists $x \in X$ such that $\alpha(x) \neq 0$. Let m be the smallest integer such that $\alpha(x)^m = 0$; note that $m \geq 1$. Then $\alpha(x)\alpha(x)^{m-1}$, where $\alpha(x)$ and $\alpha(x)^{m-1}$ are not zero. Thus F contains zero divisor, which is a contradiction. Thus R contains no nonzero nilpotent elements.

□

Problema 2 (21). *Let X e any nonempty set and let $\mathcal{P}(X)$ the set of all subsets of X (the power set of X). Define addition and multiplication on $\mathcal{P}(X)$ by*

$$A + B = (A - B) \cup (B - A) \qquad \textit{and} \qquad A \times B = A \cap B$$

i.e. addition is the symmetric difference and multiplication is the intersection.

1. *Prove that $\mathcal{P}(X)$ is a ring under these operations ($\mathcal{P}(X)$ and its subrings are often referred to as rings of sets).*
2. *Prove that this ring is commutative, has a identity and is a Boolean ring.*

Demostración.

Fecha: Octurbe, 2022.

1. Sean $A, B, C \in \mathcal{P}(X)$, entonces

$$
\begin{aligned}
& (A+B)+C \\
&= ((A-B)\cup(B-A))+C \\
&= (((A-B)\cup(B-A))-C)\cup(C-((A-B)\cup(B-A))) \\
&= ((A-B)-C)\cup((B-A)-C)\cup((C-(A-B))\cap(C-(B-A))) \\
&= (A-(B\cup C))\cup(B-(A\cup C))\cup(((C-A)\cup(C\cap B))\cap((C-B)\cup(C\cap A))) \\
&= [(A-B)\cap(A-C)]\cup[(B-A)\cap(B-C)]\cup[(C-A)\cap(C-B)] \\
&\qquad \cup[(C-A)\cap C\cap A]\cup[(C-B)\cap C\cap B]\cup[C\cap B\cap C\cap A] \\
&= [(A-B)\cap(A-C)]\cup[(B-A)\cap(B-C)]\cup[(C-A)\cap(C-B)]\cup[A\cap B\cap C] \\
&= [(A-B)\cap(A-C)]\cup[(B-A)\cap(B-C)]\cup[(C-A)\cap(C-B)] \\
&\qquad \cup[(A-B)\cap(A\cap B)]\cup[(A-C)\cap(A\cap C)]\cup[A\cap B\cap A\cap C] \\
&= [((A-B)\cup(A\cap C))\cap((A-C)\cup(A\cap B)]\cup[(B-A)\cap(B-C)]\cup[(C-A)\cap(C-B)] \\
&= [(A-(B-C))\cap(A-(C-B))]\cup[((B-A)\cap(B-C))\cup((C-A)\cap(C-B))] \\
&= (A-((B-C)\cup(C-B)))\cup[(B-(C\cup A))\cup(C-(B\cup A))] \\
&= (A-(B+C))\cup[((B-C)-A)\cup((C-B)-A)] \\
&= (A-(B+C))\cup(((B-C)\cup(C-B))-A) \\
&= (A-(B+C))\cup((B+C)-A) \\
&= A+(B+C)
\end{aligned}
$$

Entonces $+$ es asociativa.

Veamos que
$$A+\emptyset=(A-\emptyset)\cup(\emptyset-A)=A\cup\emptyset=A$$
Y similarmente $\emptyset+A=A$, por lo que $\emptyset$ es el elemento neutro de $+$.

Veamos ahora que
$$A+A=(A\setminus A)\cup(A\setminus A)=\emptyset\cup\emptyset=\emptyset$$
Por lo que, cada elemento de R es su propio inverso aditivo. Por tanto $(R,+)$ es un grupo.

Además
$$A+B=(A\setminus B)\cup(B\setminus A)=(B\setminus A)\cup(A\setminus B)=B+A$$
Por lo que $(R,+)$ es un grupo abeliano.

$$A\cdot(B\cdot C)=A\cdot(B\cap C)=A\cap(B\cap C)=(A\cap B)\cap C=(A\cdot B)\cdot C$$
Así que la multiplication es asociativa.

$$
\begin{aligned}
A\cdot(B+C) &= A\cap((B\setminus C)\cup(C\setminus B)) \\
&= (A\cap(B\setminus C))\cup(A\cap(C\setminus B)) \\
&= ((A\cap B)\setminus(A\cap C))\cup((A\cap B)\setminus(A\cap C)) \\
&= (A\cap B)+(A\cap C) \\
&= A\cdot B+A\cdot C;
\end{aligned}
$$

Así que la multiplication es distributiva sobre la addition. (La prueba por la derecha es similar.) ya que $\cap$ es conmutativo. Por lo tanto, R es un anillo.

2. Como $A\cdot B=A\cap B=B\cap A=B\cdot A$, entonces R es conmutativo.
   Como $A\cdot X=A\cap C=A$ y $X\cdot A=X\cap A=A$, entonces R tiene identidad.
   Además, para todo $A\in R$, $A\cdot A=A\cap A=A$, por lo que R es booleano.

$\square$

Problema 3 (25). *Sea I el anillo de los cuaterniones de Hamilton, y definimos*
$$N: I\to\mathbb{Z}\quad by\quad N(a+bi+cj+dk)=a^2+b^2+c^2+d^2$$
(La función N es llamada Norma*).*

1. *Pruebe that $N(\alpha)=\alpha\overline{\alpha}$ para todo $\alpha\in I$, donde si $\alpha=a+bi+cj+dk$, entonces $\overline{\alpha}=a-bi-cj-dk$.*

2. *Pruebe que $N(\alpha\beta) = N(\alpha)N(\beta)$ para todo $\alpha, \beta \in I$.*
3. *Pruebe que un elemento de I es una unidad si y solo si su norma $N(\alpha) = +1$. Muestre que I^* es isomorfo al grupo de cuaterniones de orden 8 [El inverso en el anillo de los cuaterniones racionales de un elemento diferente de cero α es $\frac{\overline{\alpha}}{N(\alpha)}$.]*

Demostración.

1.

$$\begin{aligned}
\alpha\overline{\alpha} &= (a + bi + cj + dk)(a - bi - cj - dk) \\
&= a^2 - abi - acj - adk + bai - b^2i^2 - bcij - bdik + caj \\
&\qquad - cbji - c^2j^2 - cdjk + dak - daki - dckj - d^2k^2 \\
&= a^2 + b^2 + c^2 + d^2 \\
&= N(\alpha)
\end{aligned}$$

2.

$$\begin{aligned}
N(\alpha\beta) &= N((a + bi + cj + dk)(x + yi + zj + wk)) \\
&= N((ax - by - cz - dw) + (ay + bx + cw - dz)i+ \\
&\qquad (az - bw + cx + dy)j + (aw + bz - cy + dx)k) \\
&= (ax - by - cz - dw)^2 + (ay + bx + cw - dz)^2 + \\
&\qquad (az - bw + cx + dy)^2 + (aw + bz - cy + dx)^2 \\
&= (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2) \\
&= N(\alpha)N(\beta)
\end{aligned}$$

3. Supongamos que α es una unidad, entonces $\alpha\beta = 1$ para algún β en el anillo de cuaterniones de Hamilton. Note que por la definición de N como una suma de cuadrados, entonces $N(\alpha) \geq 0$ para todo $\alpha \in I$. Ahora

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$$

y $N(\alpha)$ y $N(\beta)$ son ambos enteros, por lo tanto $N(\alpha) = 1$. Ahora, supongamos que $N(\alpha) = 1$. Entonces

$$\alpha\overline{\alpha} = N(\alpha) = 1$$

Y claramente $\overline{\alpha} \in I$, así que α es una unidad en I.

Supongamos que $\alpha \in I$ es una unidad, entonces

$$N(\alpha) = a^2 + b^2 + c^2 + d^3 = 1$$

si alguno de a, b, c, d es mayor que 2 en valor absoluto, tenemos una contradicción, así que cada uno de a, b, c, d es menor que 2 en valor absoluto. Por lo tanto son $1, 0$ o -1, Si más de uno es mayor que 1 en valor absoluto, tenemos otra contradicción; por lo tanto, a lo mucho uno de ellos puede set 1, si todos son cero, entonces $\alpha = 0$, por lo que no es una unidad, así que exactamente uno de ellos es 1, entonces $N(\alpha) = 1$, así que α es una unidad. Por lo tanto $|I^*| = 8$, ya que I^* es no abeliano y tiene seis elementos de orden 4, $I^* \cong Q_8$.

□

Problema 4 (30)**.** *Sea $A = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots$ el producto de contables copias de $\mathbb{Z}$. Sea A el anillo con adición y multiplicación componente a componente. Sea R el anillo de los homomorfismos de grupo de A en si mismo descrito en el ejercicio anterior. Es decir, con la adición y composición punto por punto. Sea φ el elemento de R definido por $\varphi(a_1, a_2, a_3, \ldots) = (a_2, a_3, a_4, \ldots)$. Sea ψ el elemento de R de definido por $\psi(a_1, a_2, a_3, \ldots) = (0, a_1, a_2, a_3, \ldots)$.*

1. *Probar que $\varphi\psi$ es la identidad de R pero $\psi\varphi$ no es la identidad de R.*
2. *exhibir infinitos inversor por derecha de φ en R.*
3. *Encontrar un elemento no cero π en R tal que $\varphi\pi = 0$ pero $\pi\varphi \neq 0$.*
4. *Probar que no hay un elemento distinto de cero $\lambda \in R$ tal que $\lambda\varphi = 0$*

Demostración.

1. Sea $(\prod a_i) \in A$. Note que
$$(\varphi \circ \psi)\left(\prod a_i\right) = \varphi\left(\prod b_i\right)$$
Donde $b_0 = 0$ y $b_{i+1} = a_i$. Ahora, $\varphi(\prod b_i) = \prod c_i$ donde $c_i = b_{i+1} = a_i$ para todo $i \in \mathbb{N}$; por lo tanto $(\varphi \circ \psi)(\prod a_i)$ y tenemos que $\varphi \circ \psi = 1$. Por otro lado, si $a_0 \neq 0$, entonces la cero-esima coordinada de (a_i) es no cero, mientras que la cero-esima coordinada de $(\psi \circ \triangleleft)(\prod a_i)$ es cero, por lo que $\psi \circ \varphi \neq 1$ $\square$