Corso di Laurea in Matematica
compito di Algebra I del 10 maggio 2012
SOLUZIONE

Esercizio 1. *Sia $A \neq \emptyset$ un insieme. Su $\Omega = A^A = \{f \mid f : A \to A\}$ si definisca la relazione $\sim$ ponendo, per ogni $f, g \in \Omega$,*

$$f \sim g \text{ se esiste una biezione } \phi : A \to A \text{ tale che } g = f \circ \phi.$$

(a) *Si provi che $\sim$ è un relazione d'equivalenza su Ω.*

- riflessività. Sia ι_A l'applicazione identica su A; allora ι_A è una biezione e $f = f \circ \iota_A = f$ per ogni $f \in \Omega$; quindi $f \sim f$ per ogni $g \in \Omega$.
- simmetria. Siano $f, g \in \Omega$ tali che $f \sim g$; allora esiste una biezione $\phi \in \Omega$ tale che $g = g \circ \phi$; ora, ϕ è invertibile, l'inversa ϕ^{-1} è una biezione, e si ha

$$f = f \circ \iota_A = f \circ (\phi \circ \phi^{-1}) = (f \circ \phi) \circ \phi^{-1}) = g \circ \phi^{-1},$$

da cui $g \sim f$.
- transitività. Siano $f, g, h \in \Omega$ tali che $f \sim g,\ g \sim h$; allora esistono biezioni $\phi, \psi \in \Omega$ tali che $g = f \circ \phi$ e $h = g \circ \psi$; allora anche $\phi \circ \psi$ è una biezione e si ha $f \circ (\phi \circ \psi) = (f \circ \phi) \circ \psi = g \circ \psi = h$, dunque $f \sim h$.

(b) *Sia $f : A \to A$ un'applicazione costante; si dica quanti elementi contiene la classe di equivalenza $[f]_\sim$.*

$f \in \Omega$ costante significa che esiste un elemento $a \in A$ tale che $f(x) = a$ per ogni $x \in A$. Sia $g \in [f]_\sim$; ciò significa che $f \sim g$, cioè esiste una biezione $\phi \in \Omega$ tale che $g = f \circ \phi$; dunque per ogni $x \in A$ si ha

$$g(x) = (f \circ \phi)(x) = f(\phi(x)) = a.$$

Quindi $g = f$ è la stessa costante. In conclusione $[f]_\sim = \{f\}$ contiene un solo elemento.

(c) *Siano $f, g \in \Omega$ applicazioni* **iniettive***; si provi che $f \sim g \ \Leftrightarrow\ Im(f) = Im(g)$.*

Siano $f, g \in \Omega$ con $f \sim g$; allora $g = f \circ \phi$ per qualche biezione $\phi \in \Omega$. Allora, per ogni $x \in A$, $g(x) = f(\phi(x)) \in f(A)$, quindi $g(A) \subseteq f(A)$. Per la simmetria si ha allo stesso modo $f(A) \subseteq g(A)$ e dunque $Im(f) = Im(g)$. Quindi l'implicazione

$$f \sim g \ \Rightarrow\ Im(f) = Im(g).$$

vale indipendentemente dall'ipotesi aggiuntiva che f e g siano iniettive.

Per il viceversa, assumiamo che f, g siano iniettive e tali che $f(A) = g(A)$ (cioè, $Im(f) = Im(g)$). Ora, per ogni $a \in A$, $g(a) \in g(A) = f(A)$ e dunque esiste un elemento $\bar{a} \in A$ tale che $g(a) = f(\bar{a})$. Ma poiché f è iniettiva, tale elemento $\bar{a}$ è unico (cioè dipende univocamente da a). Possiamo quindi definire un'applicazione $\phi : A \to A$ ponendo $\phi(a) = \bar{a}$ per ogni $a \in A$. Allora, per costruzione di ϕ si ha, per ogni $a \in A$,

$$(f \circ \phi)(a) = f(\phi(a)) = f(\bar{a}) = g(a)$$

dunque $g = f \circ \phi$. Avremo che $f \sim g$ se proviamo che ϕ è una biezione. L'iniettività è immediata: se $a, a_1 \in A$ sono tali che $\phi(a) = \phi(a_1)$, allora

$$g(a) = f(\phi(a)) = f(\phi(a_1)) = g(a_1),$$

dunque, poiché ϕ è iniettvia, $a = a_1$. Quindi ϕ è iniettiva.
Per la suriettività, sia $b \in A$; allora $f(b) \in f(A) = g(A)$ e quindi esiste $c \in A$ tale che $f(b) = g(c)$. Dunque $f(b) = (f \circ \phi)(c) = f(\phi(c)$. Poiché f è iniettiva, si deduce che $b = \phi(c)$. Questo vale per qualunque $b \in A$, così provando che ϕ è suriettiva.

(d) *Siano $f, g \in \Omega$ con $f \sim g$ e sia $\phi : A \to A$ una biezione tale che $g = f \circ \phi$; si provi che è ben definita l'applicazione*

$$\begin{array}{rccc} \Lambda : & A/\sim_f & \to & A/\sim_g \\ & [x]_{\sim_f} & \mapsto & [\phi^{-1}(x)]_{\sim_g} \end{array}.$$

Siano $x, y \in A$ tali che $[x]_{\sim_f} = [y]_{\sim_f}$. Ciò significa $x \sim_f y$, e per la definizione dell'equivalenza $\sim_f$ associata a f, si ha quindi $fx) = f(y)$. Allora, osservando che da $g = f \circ \phi$ segue $f = g \circ \phi^{-1}$,

$$g(\phi^{-1}(x)) = (g \circ \phi^{-1})(x) = f(x) = f(y) = (g \circ \phi^{-1})(y) = g(\phi^{-1}(y)),$$

dunque $\phi^{-1}(x) \sim_g \phi^{-1}(y)$. Di conseguenza $[\phi^{-1}(x)]_{\sim_g} = [\phi^{-1}(y)]_{\sim_g}$ e questo garantisce che Λ è ben definita.

Esercizio 2. *Si dica per quali $z \in \mathbb{Z}$ si ha*

$$z \cdot 5^{234567891} + 7^{345678912} - 8z \cdot 10^{9^{999}} \equiv 1 \pmod{11}.$$

L'idea è, come sempre, di utilizzare dove possibile il Teorema di Fermat.
Poiché $234567891 \equiv 1 \pmod{10}$, esiste $a \in \mathbb{Z}$ (che non occorre determinare) tale che $234567891 = 10 \cdot a + 1$; poiché 5 non è un multiplo di 11 (e 11 è un numero primo), il Teorema di Fermat assicura che

$$5^{234567891} = (5^{10})^a \cdot 5^1 \equiv 5 \pmod{11}. \tag{1}$$

Allo stesso modo, poiché 7 non è multiplo di 11 e $345678912 \equiv 2 \pmod{10}$,

$$7^{345678912} \equiv 7^2 \equiv 5 \pmod{11}. \tag{2}$$

Per trattare il terzo addendo del membro di sinistra, basta osservare che $10 \equiv -1 \pmod{11}$; quindi (dato che certamente 9^{999} è dispari),

$$10^{9^{999}} \equiv (-1)^{9^{999}} \equiv -1 \pmod{11}. \tag{3}$$

Sostituendo nella congruenza di partenza i termini trovati in (1), (2) e (3), si giunge alla congruenza equivalente

$$z \cdot 5 + 5 - 8z \cdot (-1) \equiv 1 \pmod{11},$$

ovvero

$$13z \ + 5 \equiv 1 \pmod{11},$$

che possiamo riscrivere come

$$2z \equiv 7 \pmod{11}$$

e le cui soluzioni sono tutti e soli i numeri $z \in \mathbb{Z}$ tali che

$$z \equiv 9 \pmod{11}.$$

Esercizio 3. *Per ogni $f \in \mathbb{R}^{\mathbb{R}}$ (cioè ogni applicazione $f : \mathbb{R} \to \mathbb{R}$), definiamo il* supporto *di f come*

$$supp(f) = \{a \in \mathbb{R} \mid f(a) \neq 0\}.$$

Lavoriamo ora nell'anello delle funzioni reali $\mathbb{R}^{\mathbb{R}}$.

(a) *Si provi che $A = \{f \in \mathbb{R}^{\mathbb{R}} \mid \exists n \in \mathbb{N} : \ |f(x)| \leq n$ per ogni $x \in \mathbb{R}\}$ è un sottoanello ma non un ideale di $\mathbb{R}^{\mathbb{R}}$.*

L'elemento identico dell'anello $\mathbb{R}^{\mathbb{R}}$ è la funzione costante $\underline{1}$, che appartiene a A (con $n = 1$): infatti $|\underline{1}(x)| = 1 \leq 1$ per ogni $x \in \mathbb{R}$. Se, per assurdo, A fosse un ideale, allora, poiché contiene lk'elenmento identico, $A = \mathbb{R}^{\mathbb{R}}$, il che è certamente assurdo, dato che esistono funzioni reali illimitate, come per esempio la funzione $x \mapsto x$. Dunque, A non è un ideale.
Per provare che A è un sottoanello, ed avendo già osservato che contiene l'elemento identico, consideriamo due elementi $f.g$ di A, e proviamo che $f - g$ e fg appartengono ad A. Poiché $f, g \in A$ esistono $n, m \in \mathbb{N}$ tali che

$$\forall x \in \mathbb{R} \ : \ |f(x)| \leq n \ \ e \ \ |g(x)| \leq m.$$

Allora, per ogni $x \in \mathbb{R}$ si ha

$$|(f-g)(x)| = |f(x) - g(x)| \leq |f(x)| + |-g(x)| = |f(x)| + |g(x)| \leq n + m$$

e

$$|(fg)(x)| = |f(x)g(x)| = |f(x)||g(x)| \leq nm.$$

Dunque $f - g \in A$ e $fg \in A$, per ogni $f, g \in A$. Questo prova che A è un sottoanello di $\mathbb{R}^{\mathbb{R}}$.

(b) *Si provi che* $B = \{f \in \mathbb{R}^{\mathbb{R}} \mid |supp(f)| < \infty\}$ *è un ideale di* $\mathbb{R}^{\mathbb{R}}$.

- Innanzi tutto, notiamo che la funzione costante $\underline{0}$ appartiene a B (infatti: $supp(\underline{0}) = \emptyset$) che quindi non è vuoto.
- Siano $f, g \in B$. Allora, per ogni $x \in \mathbb{R}$, da $f(x) = 0$ e $g(x) = 0$ segue $(f - g)(x) = 0$. Quindi

$$supp(f - g) \subseteq supp(f) \cup supp(g);$$

e poiché sia $supp(f)$ che $supp(g)$ sono finiti, si conc;ude che $supp(f - g)$ è finito, ovvero che $f - g \in B$.
- Per la proprietà di assorbimento, è conveniente osservare il seguente fatto: per ogni $f, g \in \mathbb{R}^{\mathbb{R}}$, si ha $supp(fg) = supp(f) \cap supp(g)$. Infatti, per $x \in \mathbb{R}$

$$0 \neq (fg)(x) = f(x)g(x) \;\Leftrightarrow\; \begin{cases} 0 \neq f(x) \\ 0 \neq g(x) \end{cases} \quad \Leftrightarrow \quad x \in supp(f) \cap supp(g).$$

Dunque, in particolare, per ogni $f \in B$ e ogni $h \in \mathbb{R}^{\mathbb{R}}$ si avrà

$$supp(fh) = supp(f) \cap supp(h) \subseteq supp(f)$$

che è finito. Quindi $fh \in B$. Pertanto, B è un ideale di $\mathbb{R}^{\mathbb{R}}$.

(c) *Si provi che l'ideale* B *non è principale.*

Supponiamo, per assurdo, che B sia principale; ovvero che esista $f \in B$ tale che

$$B = (f) = \{fh \mid h \in \mathbb{R}^{\mathbb{R}}\}.$$

Allora, per quanto osservato nella dimostrazione del punto precedente, si avrebbe

$$supp(g) \subseteq supp(f) \quad \text{per ogni} \;\; g \in B.$$

Il che è assurdo, dato che palesemente esistono funzioni il cui supporto è finito ma non è contenuto inell'insieme finito $supp(f)$. Per essere precisi; bastera considerare un qualsiasi elemento

$$r \in \mathbb{R} \setminus (supp(f))$$

(che certamente esiste dato che $supp(f)$ è finito; quindi considerare la funzione $h \in \mathbb{R}^{\mathbb{R}}$ definita da, per ogni $x \in \mathbb{R}$,

$$h(x) = \begin{cases} 0 & \text{se} \quad x \neq r \\ 1 & \text{se} \quad x = r \end{cases}$$

Allora, $h \in B$, dato che $supp(h) = \{r\}$ è finito, ma $h \notin (f)$ dato che, per costruzione, $supp(h) \not\subseteq supp(f)$.

Esercizio 4. *Per ogni numero primo $p \geq 1$ sia*

$$f_p = x^2 + 2(p+1)x + 4p + 1 \in \mathbb{Q}[x].$$

(a) *Si dica per quali primi p, l'anello quoziente $A_p = \mathbb{Q}[x]/(f_p)$ è un campo* [sugger.: si provi con la sostituzione $x \mapsto x - 1$].

Dal punto di vista rigoroso, la sostituzione proposta non è altro che l'unico isomorfismo $\phi : \mathbb{Q}[x] \to \mathbb{Q}[x]$ tale che $x \mapsto x - 1$ (e $a \mapsto a$ per ogni $a \in \mathbb{Q}$). In particolare $f \in \mathbb{Q}[x]$ è irriducibile se e soltanto se $\phi(f)$ è irriducibile. Nel nostro caso:

$$\phi(f_p) = (x-1)^2 + 2(p+1)(x-1) + 4p + 1 = x^2 + 2px + 2p.$$

Se $p \neq 2$, $\phi(f_p)$, e quindi f, è irriducibile per il criterio di Eisenstein.
Se $p = 2$, si ha $f_2 = x^2 + 6x + 9 = (x+3)^2$.
Ora, $A_p = \mathbb{Q}[x]/(f_p)$ è un campo se e soltanto se f_p è irriducibile. Dunque si conclude che *$A + p$ è un campo se e soltanto se $p \neq 2$*

(b) *Per ogni primo p, si descrivano gli ideali massimali di A_p.*

Nel casp $p \neq 2$, per quanto visto, A_p è un campo; dunque il suo unico ideale massimale è quello nullo, ovvero $\{(f_p)\}$.

Se $p = 2$, $f_2 = (x+3)^2$. Per il teorema di Corrispondenza, gli ideali massimali di A_2 sono tutti e soli quelli del tipo $I/)f_2)$ dove I è un ideale massimale di $\mathbb{Q}[x]$ che contiene (f_2). Sia I un tale ideale, allora, per i fatti noti di teoria, essendo $\mathbb{Q}[x]$ un dominio a ideali principali, $I = (g)$ dove
– g è irriducibile (perché I è massimale);
– g divide f_2 (perché $(f_2) \subseteq (g)$).
Quindi, a meno di associati, la sola possibilità è $g = x + 3$,Pertanto A_2 ha un unico ideale massimale, che è $(x+3)/(f_2)$.