SOLUZIONI ESAME DI ALGEBRA 1
APPELLO DEL 14/01/2008

Esercizio 1. In $\mathbb{R}$, $a\sigma b \iff \exists\, x \in \mathbb{R}$, $x \neq 0$ tale che $ax = b$

i) Propr. riflessiva: $a\sigma a \iff ax = a \iff x = 1 \in \mathbb{R}^*$.
ii) Propr. simmetrica: $a\sigma b \Longrightarrow b\sigma a$. Distinguiamo due casi:
   a) se $a = 0$: $a\sigma b \Longrightarrow a = b = 0 \Longrightarrow b\sigma a$;
   b) se $a \neq 0$, $b \neq 0$: $a\sigma b \iff \exists\, x = \frac{b}{a} \in \mathbb{R}^*$ tale che $ax = b$ $\Longrightarrow \exists\, x^{-1} = \frac{a}{b} \in \mathbb{R}^* \Longrightarrow b\sigma a$.
iii) Propr. transitiva: $a\sigma b$ e $b\sigma c$, si hanno due casi:
   a) $a = b = c = 0$ e allora $a\sigma c$;
   b) $a \neq 0, b \neq 0, c \neq 0$, per cui $\exists\, x = \frac{b}{a} \in \mathbb{R}^*$ e $\exists\, y = \frac{c}{b} \in \mathbb{R}^* \Longrightarrow$ $\exists\, xy = \frac{c}{a} \in \mathbb{R}^*$ poiché il prodotto di due numeri reali é reale $\Longrightarrow a\sigma c$.

Quindi tale relazione é di equivalenza.
Costruiamo l'insieme quoziente. Notiamo che $[0] = \{0\}$ e che $\forall a \in \mathbb{R}^*, [a] = [1]$ poiché $\exists\, x = \frac{1}{a}$ tale che $ax = 1$. Quindi $\mathbb{R}_{/\sigma} = \{[0], [1]\}$.

Esercizio 2. $f : \mathbb{Z}_{18} \to \mathbb{Z}_3$ tale che $f([x]_{18}) = [x]_3$.

i) Dobbiamo dimostrare che preso $[x]_{18} = [y]_{18}$ risulta $f([x]_{18}) = f([y]_{18})$ ossia $[x]_3 = [y]_3$.
   $[x]_{18} = [y]_{18} \iff x = y + 18k$ con $k \in \mathbb{Z} \Longrightarrow [x]_3 = [y + 18k]_3 = [y + 3(6k)]_3 = [y]_3$.
ii) $f([a]_{18} + [b]_{18}) = f([a + b]_{18}) = [a + b]_3 = [a]_3 + [b]_3 = f([a]_{18}) + f([b]_{18})$. Analogo per il prodotto.
iii) $\ker f = \{[a]_{18} \in \mathbb{Z}_{18} : f([a]_{18}) = [0]_3\} = \{[0]_{18}, [3]_{18}, [6]_{18}, [9]_{18}, [12]_{18}, [15]_{18}\}$.
   $\mathrm{Im} f = \mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ poiché $f([0]_{18}) = [0]_3$, $f([1]_{18}) = [1]_3$, $f([2]_{18}) = [2]_3$.
   Quindi f non é iniettiva perché $\ker f \neq \{[0]_{18}\}$, infatti $f([0]_{18}) = f([3]_{18}) = [0]_3$, ma $[0]_{18} \neq [3]_{18}$.
   f invece risulta suriettiva perché $\mathrm{Im} f = \mathbb{Z}_3$.
iv) $\mathbb{Z}_{18_{/\ker f}} = \{[0]_{18} + \ker f, [1]_{18} + \ker f, [2]_{18} + \ker f\}$. Per il teorema di isomorfismi di anelli risulta $\mathbb{Z}_{18_{/\ker f}}$ isomorfo a $\mathrm{Im} f = \mathbb{Z}_3$.

Esercizio 3. Risolviamo il sistema di congruenze dato:

$$\begin{cases} 7x \equiv 3 \mod 13 \\ x \equiv 2 \mod 15 \end{cases}$$

Riduciamo la prima congruenza in forma normale. Essa ammette soluzioni se e solo se $(7, 13) = 1 \mid 8$, per cui é risolubile. Ricaviamo

l'identitá di Bézout: $1 = (-1)13 + (2)7$, per cui $[7]_{13}^{-1} = [2]_{13}$ in $\mathbb{Z}_{13}$. La prima congruenza diventa

$$x \equiv 6 \mod 13$$

Il sistema da risolvere é ora in forma normale:

$$\begin{cases} x \equiv 6 \mod 13 \\ x \equiv 2 \mod 15 \end{cases}$$

Possiamo applicare il Teorema cinese dei resti in quanto $(13, 15) = 1$, ricaviamo allora l'identitá di Bézout per 13 e 15:

$$\begin{aligned} 15 = 13 \cdot 1 + 2 &\longrightarrow 1 = 13 + (-6)2 \\ 13 = 2 \cdot 6 + 1 &\longrightarrow 2 = 15 + 13(-1) \end{aligned}$$

Sostituendo la seconda uguaglianza nella prima si ottiene

$$1 = 13 + (-15 + 13)6 = 15(-6) + 13(7)$$

Moltiplichiamo ora ambo i membri di $1 = 15(-6) + 13(7)$ per $6 - 2$:

$$4 = 15(-18) + 13(14)$$

La soluzione finale é $x = 6 - 13(14) = 2 + 15(-16) = -358$, riducendola modulo $13 \cdot 15 = 195$ si ha $x \equiv 32 \mod 195$.

Esercizio 4. Consideriamo $p(x) = x^2 + x + 2$ in $\mathbb{Z}_3[x]$.

i) Dato che $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ verifichiamo se tali elementi sono radici di $p(x)$:

$$\begin{aligned} p(\overline{0}) &= \overline{2} \neq \overline{0} \\ p(\overline{1}) &= \overline{1} \neq \overline{0} \\ p(\overline{2}) &= \overline{2} \neq \overline{0} \end{aligned}$$

$p(x)$ non ha radici in $\mathbb{Z}_3$, quindi per il Teorema di Ruffini non ha fattori di grado 1, ed essendo di grado 2 risulta irriducibile in $\mathbb{Z}_3[x]$.

ii) Gli elementi di $\mathbb{Z}_3[x]_{/(x^2+x+2)}$ sono della forma $a(x) + I$, dove $I = (x^2 + x + 2)$, piú precisamente:

$$\begin{aligned} a(x) + I &= \{b(x) \in \mathbb{Z}_3[x] \ / \ b(x) - a(x) = q(x)(x^2 + x + 2), q(x) \in \mathbb{Z}_3[x]\} \\ &= \{b(x) \in \mathbb{Z}_3[x] \ / \ b(x) = a(x) + q(x)(x^2 + x + 2), q(x) \in \mathbb{Z}_3[x]\} \end{aligned}$$

Ogni polinomio $a(x)$ é in relazione con il resto $r(x)$ della divisione di $a(x)$ per $x^2 + x + 2$:

$$a(x) + I = r(x) + I, \ \deg(r(x)) < 2$$

Consideriamo tutti i possibili resti della divisione per $x^2 + x + 2$, quindi l'anello quoziente sará

$$\mathbb{Z}_3[x]_{/(x^2+x+2)} = \{a_0 + a_1 x + I \ / \ a_0, a_1 \in \mathbb{Z}_3\}$$

Si hanno 3 possibili scelte per il coefficiente a_0 e altre 3 possibilitá per a_1, quindi la cardinalitá dell'anello quoziente é $3 \cdot 3 = 9$.

iii) $\mathbb{Z}_3$ é un campo, $\mathbb{Z}_3[x]$ é un P.I.D., per cui $p(x) \in \mathbb{Z}_3[x]$ é irriducibile se e solo se $(p(x))$ é un ideale primo, se e solo se $(p(x))$ é un ideale massimale.
Inoltre si ha le seguente proprietá:
Dato A anello e I un suo ideale, $A_{/I}$ é campo se e solo se I é massimale.
Nel nostro caso $p(x) = x^2 + x + 2$ é irriducibile, per cui l'ideale $(p(x))$ é massimale, ne segue che l'anello quoziente $A_{/I}$ é un campo.
Si é trovato al punto precedente $n = 9$, $\mathbb{Z}_9$ non é un campo, poiché 9 non é primo. $\mathbb{Z}_3[x]_{/(x^2+x+2)}$ essendo un campo, non é isomorfo a $\mathbb{Z}_9$, che non é un campo.