TRENTO, A.A. 2015/16
CORSO DI ALGEBRA
FOGLIO DI ESERCIZI # 13

Esercizio 13.1. Siano A, B insiemi, e $f : A \to B$. Per $S \subseteq A$ si definisca $f(S) = \{ f(s) : s \in S \} \subseteq B$, e per $T \subseteq B$ si definisca $f^{-1}(T) = \{ a \in A : f(a) \in T \} \subseteq A$.

(1) Se $T \subseteq B$, si mostri che $f(f^{-1}(T)) = T \cap f(A)$.
   (a) Si mostri con un esempio che può ben essere $f(f^{-1}(T)) \neq T$.
   (b) Se ne deduca che se $S \subseteq A$ allora $f(f^{-1}(f(S))) = f(S)$.
   (c) Se ne deduca che se f è suriettiva, allora $f(f^{-1}(T)) = T$.

(2) Sia R la relazione di A data da xRy se e solo se $f(x) = f(y)$, e sia $[x]$ la classe di x rispetto a R. Si mostri che se $S \subseteq A$, allora

$$f^{-1}(f(S)) = \bigcup_{x \in S} [x],$$

   (a) Se ne deduca che $f^{-1}(f(S)) \supseteq S$. Si mostri con un esempio che l'inclusione può essere propria.
   (b) Se ne deduca che se f è iniettiva, allora $f^{-1}(f(S)) = S$.

(3) Si mostri che $f(S_1 \cup S_2) = f(S_1) \cup f(S_2)$, ma in generale vale solo $f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2)$. Si dia un esempio in cui non vale l'eguaglianza.

(4) Si mostri che $f^{-1}(T_1 \cup T_2) = f^{-1}(T_1) \cup f^{-1}(T_2)$ e $f^{-1}(T_1 \cap T_2) = f^{-1}(T_1) \cap f^{-1}(T_2)$.

Esercizio 13.2. Si enunci e si dimostri il terzo teorema di isomorfismo per i gruppi.

Esercizio 13.3. Si mostri che un gruppo ciclico $G = \langle a \rangle$ di ordine m ha uno e un solo sottogruppo di ordine n per ogni divisore n di m, e che questo sottogruppo è $\left\langle a^{m/n} \right\rangle$.

Si faccia sia la dimostrazione diretta, che quella attraverso il terzo teorema di isomorfismo per gruppi.

Esercizio 13.4. Si enunci il terzo teorema di isomorfismo per gli anelli.

Esercizio 13.5. Un polinomio non nullo $f \in \mathbf{Z}[x]$ si dice *primitivo* se il massimo comun divisore dei suoi coefficienti è 1.

(1) Si mostri che ogni $0 \neq f \in \mathbf{Z}[x]$ si può scrivere nella forma

$$f = cf_1,$$

ove $c \in \mathbf{Z}$, e f_1 è primitivo.

(2) Si mostri che se $0 \neq c, d \in \mathbf{Z}$, e $0 \neq f, g \in \mathbf{Z}[x]$ sono polinomi primitivi, e $cf = dg$, allora c e d sono associati in $\mathbf{Z}$, cioè $d = cu$, ove $u \in \mathbf{Z}$ è una unità. (Lo so che le unità in $\mathbf{Z}$ sono ± 1, ma ho scritto l'affermazione in modo che rimanga valida quando a $\mathbf{Z}$ sostituisco un UFD qualsiasi.) (SUGGERIMENTO: Se $h = cf = dg$, allora c e d sono due massimi comun divisori dei coefficienti di h, dunque. . .)

(3) Si mostri che ogni polinomio $0 \neq f \in \mathbf{Q}[x]$ si può scrivere come $f = \alpha f_1$, ove $\alpha \in \mathbf{Q}$, e $f_1 \in \mathbf{Z}[x]$ è primitivo.

(4) Si mostri che se $0 \neq f \in \mathbf{Q}[x]$, e
$$f = \alpha f_1 = \beta f_2$$
con $\alpha, \beta \in \mathbf{Q}$, e $f_1, f_2 \in \mathbf{Z}[x]$ primitivi, allora $\beta = \alpha u$, ove u è una unità di $\mathbf{Z}$.

(5) Si mostri che se $0 \neq f, g \in \mathbf{Z}[x]$ sono *primitivi* (avevo dimenticato questa condizione in una versione precedente) e associati in $\mathbf{Q}[x]$ (cioè esiste $\alpha \in \mathbf{Q}$ tali che $g = \alpha f$), allora sono associati anche in $\mathbf{Z}[x]$, cioè $\alpha \in \mathbf{Z}$ è una unità in $\mathbf{Z}$

(6) Si mostri che il prodotto di due polinomi primitivi è primitivo. (Questo è noto come *Lemma di Gauss*.)

(7) Si mostri che se $f \in \mathbf{Z}[x]$ ha grado positivo, ed è irriducibile in $\mathbf{Z}[x]$, allora è primitivo.
(SUGGERIMENTO: Per assurdo, se $f = df_1$, con $d > 1$ intero, allora questa è una decomposizione in cui nessuno dei due fattori è una unità, e dunque f non è irriducibile.)

(8) Si mostri che se $f \in \mathbf{Z}[x]$ ha grado positivo, ed è irriducibile in $\mathbf{Z}[x]$, allora è irriducibile in $\mathbf{Q}[x]$.
(SUGGERIMENTO: Intanto, f è primitivo. Se per assurdo $f = f_1 f_2$, con $f_1, f_2 \in \mathbf{Q}[x]$, ciascuno di grado positivo, si scriva $f_i = \alpha_i g_i$, con $\alpha_i \in \mathbf{Q}$, e $f_i \in \mathbf{Z}[x]$ primitivi. Allora
$$f = \alpha_1 \alpha_2 g_1 g_2 \tag{13.5.1}$$
ove, per il Lemma di Gauss, $g_1 g_2$ è primitivo. Allora $\alpha_1 \alpha_2$ è una unità in $\mathbf{Z}[x]$, e (13.5.1) mostra che f è riducibile in $\mathbf{Z}[x]$, dato che i gradi di g_1, g_2 sono positivi, dato che sono i gradi di f_1, f_2.)

Esercizio 13.6. Si mostri che l'ideale $(2, x) = \{\, 2u + xv : u, v \in \mathbf{Z}[x] \,\}$ di $\mathbf{Z}[x]$ non è un ideale principale.