ESERCIZI SU

ANELLI, CAMPI E DIVIBILITÀ

N.B.: il simbolo ⛑ *contrassegna gli esercizi (relativamente) più complessi.*

— ∗ —

1 — Sia p un primo in $\mathbb{Z}$, e $\mathbb{Z}_{(p)} := \left\{ a/b \in \mathbb{Q} \,\middle|\, a,b \in \mathbb{Z},\, \mathrm{MCD}(a,b) = 1,\, b \notin p\mathbb{Z} \right\}$, che è sottoanello di $\mathbb{Q}$ (e quindi è un dominio). Dimostrare che il campo dei quozienti $Q\big(\mathbb{Z}_{(p)}\big)$ di $\mathbb{Z}_{(p)}$ è (isomorfo a) il campo $\mathbb{Q}$ dei numeri razionali.

2 — Sia $d \in \mathbb{Z} \setminus \{0\}$, e sia $\mathbb{Z}_{\langle d \rangle} := \left\{ a/b \in \mathbb{Q} \,\middle|\, a,b \in \mathbb{Z},\, b \in \left\{d^n\right\}_{n\in\mathbb{N}} \right\}$, che è sottoanello di $\mathbb{Q}$ (e quindi è un dominio). Dimostrare che il campo dei quozienti $Q\big(\mathbb{Z}_{\langle d \rangle}\big)$ di $\mathbb{Z}_{\langle d \rangle}$ è (isomorfo a) il campo $\mathbb{Q}$ dei numeri razionali.

3 — Sia D un dominio, sia $Q(D)$ un suo campo dei quozienti, e sia D' un altro dominio tale che $D \leq D' \leq Q(D)$. Dimostrare che $Q(D)$ è anche campo dei quozienti di D'.

4 — Sia D un dominio, sia $Q(D)$ un suo campo dei quozienti, e sia S una *"parte moltiplicativa"* di D, cioè un sottoinsieme di $D \setminus \{0\}$ chiuso rispetto al prodotto. Sia poi $S^{-1}D$ il sottoinsieme di $Q(D)$ definito da $S^{-1}D := \left\{ n/d \,\middle|\, n \in D,\, d \in S \right\}$ (in breve, sono le frazioni in $Q(D)$ con denominatore in S).

(a) Dimostrare che per ogni parte moltiplicativa S di D, il sottoinsieme $S^{-1}D$ è un sottoanello del campo $\mathbb{Q}(D)$;

(b) dimostrare che per $S := D \setminus \{0\}$ si ha $S^{-1}D = \mathbb{Q}(D)$;

(c) dimostrare che per $S \neq \emptyset$ si ha $1_{Q(D)} \in S^{-1}D$;

(d) dimostrare che date due qualsiasi parti moltiplicative S_- e S_+ con $S_- \subseteq S_+$ si ha $S_-^{-1}D \leq S_+^{-1}D$;

(e) quando $S_-^{-1}D$ è unitario, si descriva esplicitamente (in termini di D e di S) l'insieme $U\big(S^{-1}D\big)$ degli elementi invertibili di $S^{-1}D$.

5 ⛑ — Sia k un campo, sia $k[[x_1,\dots,x_n]]$ il corrispondente anello delle serie formali nelle n variabili $x_1, \dots, x_n$ a coefficienti in k, e sia $k((x_1,\dots,x_n))$ il corrispondente campo delle serie di Laurent formali in $x_1, \dots, x_n$ a coefficienti in k. Dimostrare che il campo dei quozienti $Q\big(k[[x_1,\dots,x_n]]\big)$ di $k[[x_1,\dots,x_n]]$ è (isomorfo a) il campo $k((x_1,\dots,x_n))$.

Suggerimento: *Si consideri prima il caso $n = 1$ (la generalizzazione è immediata), e per questo si osservi che la situazione è del tutto analoga a quella dell' esercizio 1 qui sopra.*

6 — Sia D un dominio e $Q(D)$ un suo campo dei quozienti. Dimostrare che il campo dei quozienti $Q\big(D[x_1,\dots,x_n]\big)$ di $D[x_1,\dots,x_n]$ è (isomorfo a) il campo $Q(D)(x_1,\dots,x_n)$ delle funzioni razionali — in x_1 , … , x_n — a coefficienti in $Q(D)$.

Suggerimento : Si consideri prima il caso $n = 1$, poi la generalizzazione sarà immediata.

7 — Siano $\mathbb{Z}[\,i\,]$ e $\mathbb{Q}[\,i\,]$ i sottoinsiemi degli "interi di Gauss" e dei "razionali di Gauss" nel campo $\mathbb{C}$ dei numeri complessi così definiti:

$$\mathbb{Z}[\,i\,] \;:=\; \big\{\, z_0 + i\,z_1 \;\big|\; z_0, z_1 \in \mathbb{Z} \,\big\} \quad , \qquad \mathbb{Q}[\,i\,] \;:=\; \big\{\, q_0 + i\,q_1 \;\big|\; q_0, q_1 \in \mathbb{Q} \,\big\}$$

Dimostrare che:

(a) $\mathbb{Z}[\,i\,]$ e $\mathbb{Q}[\,i\,]$ sono sottoanelli del campo $\mathbb{C}$;

(b) $\mathbb{Z}[\,i\,]$ è il sottoanello di $\mathbb{C}$ generato dal sottoinsieme $\mathbb{Z} \cup \{i\}$;

(c) $\mathbb{Q}[\,i\,]$ è il sottoanello di $\mathbb{C}$ generato dal sottoinsieme $\mathbb{Q} \cup \{i\}$;

(d) $\mathbb{Q}[\,i\,]$ è un campo;

(e) $\mathbb{Q}[\,i\,]$ è campo dei quozienti di $\mathbb{Z}[\,i\,]$.

Suggerimento : I punti (a), (b) e (c) richiedono una semplice verifica diretta. Per il punto (d), per ogni $\kappa \in \mathbb{Q}[\,i\,] \setminus \{0\}$ si calcoli il suo inverso $\kappa^{-1} \in \mathbb{C}$ e dalla forma esplicita di quest'ultimo si verifichi che in effetti è $\kappa^{-1} \in \mathbb{Q}[\,i\,]$. Una volta acquisito il punto (d), il punto (e) è molto semplice.

8 — Sia $d \in \mathbb{Z}$, sia $\sqrt{d} \in \mathbb{C}$ una radice quadrata di d nel campo $\mathbb{C}$ dei numeri complessi, e siano $\mathbb{Z}\big[\sqrt{d}\,\big]$ e $\mathbb{Q}\big[\sqrt{d}\,\big]$ i sottoinsiemi di $\mathbb{C}$ così definiti:

$$\mathbb{Z}\big[\sqrt{d}\,\big] \;:=\; \big\{\, z_0 + z_1\sqrt{d} \;\big|\; z_0, z_1 \in \mathbb{Z} \,\big\} \quad , \qquad \mathbb{Q}\big[\sqrt{d}\,\big] \;:=\; \big\{\, q_0 + q_1\sqrt{d} \;\big|\; q_0, q_1 \in \mathbb{Q} \,\big\}$$

Dimostrare che:

(a) $\mathbb{Z}\big[\sqrt{d}\,\big]$ e $\mathbb{Q}\big[\sqrt{d}\,\big]$ sono sottoanelli del campo $\mathbb{C}$;

(b) $\mathbb{Z}\big[\sqrt{d}\,\big]$ è il sottoanello di $\mathbb{C}$ generato dal sottoinsieme $\mathbb{Z} \cup \big\{\sqrt{d}\,\big\}$;

(c) $\mathbb{Q}\big[\sqrt{d}\,\big]$ è il sottoanello di $\mathbb{C}$ generato dal sottoinsieme $\mathbb{Q} \cup \big\{\sqrt{d}\,\big\}$;

(d) $\mathbb{Q}\big[\sqrt{d}\,\big]$ è un campo;

(e) $\mathbb{Q}\big[\sqrt{d}\,\big]$ è campo dei quozienti di $\mathbb{Z}\big[\sqrt{d}\,\big]$.

Suggerimento : È la diretta generalizzazione dell'esercizio 7 qui sopra (che corrisponde al caso $d := -1$) e si risolve allo stesso modo.

9 — Siano D_1 e D_2 due dominî, e siano $Q(D_1)$ e $Q(D_2)$ campi dei quozienti dell'uno e dell'altro rispettivamente. Dimostrare che, se $D_1 \cong D_2$, allora $Q(D_1) \cong Q(D_2)$.

Suggerimento: *A partire da un isomorfismo (di anelli)* $\phi : D_1 \xhookrightarrow{\cong} D_2$, *si definisca una funzione* $\phi_{_Q} : Q(D_1) \longrightarrow Q(D_2)$ *tenendo conto che ogni elemento di* $Q(D_1)$ *si scrive nella forma* $n\,d^{-1}$ *con* $n, d \in D$, $d \neq 0$, *e imponendo le condizioni seguenti:*

(a) la restrizione di $\phi_{_Q}$ *a* D_1 *(che è contenuto in* $Q(D_1)$*...) coincida con* ϕ*;*

(b) $\phi_{_Q}$ *sia un morfismo (di anelli).*

Si verifichi poi che esiste una e una sola funzione $\phi_{_Q} : Q(D_1) \longrightarrow Q(D_2)$ *che soddisfi tali condizioni, e che tale* $\phi_{_Q}$ *è in effetti un isomorfismo.*

10 — Sia A un anello, S un sottoinsieme di A, e sia $(S)_s$, risp. $(S)_d$, risp. $(S)_b$, l'ideale sinistro, risp. destro, risp. bilatero di A generato dal sottoinsieme S. Sia $\phi : A \twoheadrightarrow B$ un epimorfismo di anelli. Dimostrare che $\phi\big((S)_s\big)$, risp. $\phi\big((S)_d\big)$, risp. $\phi\big((S)_b\big)$, è l'ideale sinistro, risp. destro, risp. bilatero di B generato dal sottoinsieme $\phi(S)$.

Suggerimento: *Si sfrutti il fatto che c'è una biiezione tra ideali sinistri, risp. destri, risp. bilateri, di* A *contenenti* $Ker(\phi)$ *e di* B *data da* $I \mapsto \phi(I)$, *con inversa* $J \mapsto \phi^{-1}(J)$, *e inoltre che tale biiezione — e la sua inversa — rispetta la relazione di inclusione, cioè* $I' \subseteq I'' \iff \phi(I') \subseteq \phi(I'')$ *— e* $J' \subseteq J'' \iff \phi^{-1}(J') \subseteq \phi^{-1}(J'')$ *per l'inversa.*

11 — Sia A un anello (commutativo) a ideali principali, e sia I un ideale di A. Dimostrare che l'anello (commutativo) quoziente A/I è anch'esso a ideali principali.

Suggerimento: *Sia* $\pi_I : A \twoheadrightarrow A/I$ *la proiezione canonica; l'enunciato segue allora dall'esercizio 10 qui sopra applicato a* $\phi := \pi_I$. *Più in dettaglio, siccome* π_I *è un epimorfismo, per ogni ideale* $\overline{J}$ *di* A/I *si ha che* $\overline{J} = \pi_I\big(\pi_I^{-1}\big(\overline{J}\,\big)\big)$, *dove* $\pi_I^{-1}\big(\overline{J}\,\big)$ *è un ideale di* A *e come tale è principale, per ipotesi. Si concluda allora che, se* y *è un qualsiasi generatore dell'ideale* $\pi_I^{-1}\big(\overline{J}\,\big)$, *allora* $\pi(y)$ *è un generatore dell'ideale* $\overline{J}$.

12 — Dimostrare che l'anello $\mathbb{Z}[x]$ non è a ideali principali.

Suggerimento: *Si dimostri che l'ideale* $I := \big(\{x, 3\}\big)$ *generato dal sottoinsieme* $\{x, 3\}$ *non è principale. Analogamente, più in generale non è principale ogni ideale del tipo* $I := \big(\{x, 3\}\big)$ *dove* p *sia un intero primo.*

13 — In un anello commutativo A, sia $\,\big|\,$ la relazione di divisibilità in A, e sia $\sim$ la relazione in A di "essere associato a", definita da $a \sim b \overset{\triangle}{\iff} \big(a|b \wedge b|a\big)$ per ogni $a, b \in A$. Se inoltre A è unitario, sia $\approx$ la relazione in A definita da $a \approx b \overset{\triangle}{\iff} \exists\, \varepsilon \in U(A) : b = \varepsilon\, a$ (per ogni $a, b \in A$). Dimostrare che:

(a) la relazione $\,\big|\,$ è transitiva;

(b) la relazione $\sim$ è simmetrica e transitiva;

(c) la relazione $\big|$ è "compatibile" con la relazione $\sim$, cioè
$\Big(a' \sim a'' \,,\, b' \sim b'' \Big) \implies \Big(a' \big| a'' \iff b' \big| b'' \Big)$ per ogni $a', a'', b', b'' \in A$;

(d) se l'anello A è unitario, allora la relazione $\big|$ è un preordine;

(e) se l'anello A è unitario, allora la relazione $\sim$ è un'equivalenza;

(f) se l'anello A è unitario, allora la relazione $\approx$ è un'equivalenza;

(g) se l'anello A è unitario, allora $\approx \subseteq \sim$, cioè $a \approx b \implies a \sim b$ (per ogni $a, b \in A$).

(h) se l'anello A è unitario e integro (cioè è un dominio unitario), allora $\approx = \sim$, cioè si ha $a \approx b \iff a \sim b$ (per ogni $a, b \in A$).

14 — In un anello commutativo unitario A, siano $\big|$ e $\sim$ le due relazioni (di preordine e di equivalenza, rispettivamente) definite nell'esercizio 13 qui sopra. Nell'insieme quoziente $A\Big/\!\sim$ si definisca la relazione $\Big\|$ così: $[a]_\sim \Big\| [b]_\sim \overset{\triangle}{\iff} a \big| b$ per ogni $[a]_\sim, [b]_\sim \in A\Big/\!\sim$.
Dimostrare che:

(a) la definizione della relazione $\Big\|$ è ben posta;

(b) la relazione $\Big\|$ è un *ordine* in $A\Big/\!\sim$;

(c) la classe $\big[1_A\big]_\sim$ è il *minimo* dell'insieme $A\Big/\!\sim$ per la relazione d'ordine $\Big\|$.

Suggerimento: *La parte (a) segue direttamente dalla proprietà (c) nell'esercizio 13 qui sopra; il resto discende dalla proprietà (c) — nell'esercizio 13 — e dalle definizioni...*

15 — Sia D un dominio unitario, e siano $q' \sim q''$ due elementi in D tra loro associati. Dimostrare che q' è *irriducibile* $\iff$ q'' è *irriducibile*.

16 — Sia A un anello commutativo, e siano $a, b \in A$, $d_1, d_2 \in A$. Dimostrare che
$$d_1 \underline{\in} d_2 \text{ sono } \mathrm{MCD}(a,b) \iff \Big(\big(d_1 \underline{\in} d_2 \text{ è } \mathrm{MCD}(a,b) \big) \;\&\; \big(d_1 \sim d_2 \big) \Big)$$

Suggerimento: *Si osservi che se $d_1 \sim d_2$, allora d_1 e d_2 hanno esattamente gli stessi divisori e gli stessi multipli...*

17 — Sia A un anello commutativo, e siano $a, b \in A$, $m_1, m_2 \in A$. Dimostrare che
$$m_1 \underline{\in} m_2 \text{ sono } \mathrm{mcm}(a,b) \iff \Big(\big(m_1 \underline{\in} m_2 \text{ è } \mathrm{mcm}(a,b) \big) \;\&\; \big(m_1 \sim m_2 \big) \Big)$$

Suggerimento: *È l'analogo dell'esercizio 16 qui sopra, e si dimostra allo stesso modo.*

18 — Sia A un anello commutativo, e siano $a, b, d \in A$. Indichiamo con (d) l'ideale principale (di A) generato da $\{d\}$, e con (a, b) l'ideale (di A) generato da $\{a, b\}$.

Dimostrare che

$$(a, b) = (d) \iff \Big(\big(d = \mathrm{MCD}(a, b) \big) \ \& \ \big(\exists\, r, s \in A : a\, r + b\, s = d \big) \Big)$$

cioè, esprimendosi a parole,

$$(a, b) = (d) \iff \Big(d \text{ è } \mathrm{MCD}(a, b) \text{ e esiste una } \textit{identità di Bézout} \text{ per esso} \Big)$$

19 — Sia D un dominio in cui esista $\mathrm{MCD}(a, b)$ per ogni coppia $a, b \in D$. Dimostrare che il MCD gode della "proprietà associativa", nel senso che per ogni a_1, a_2, $a_3 \in D$ si ha

$$\mathrm{MCD}\big(\mathrm{MCD}(a_1, a_2), a_3\big) \sim \mathrm{MCD}\big(a_1, \mathrm{MCD}(a_2, a_3)\big)$$

così che, più in generale, resta ben definito (a meno di invertibili) il $\mathrm{MCD}(a_1, a_2, \ldots, a_k)$ per ogni $a_1, a_2, \ldots, a_k \in D$.

20 — Sia D un *dominio di Bézout*, cioè un dominio unitario in cui, per ogni coppia $a, b \in D$, esista $\mathrm{MCD}(a, b)$ ed una identità di Bézout per esso. Dimostrare che ogni ideale finitamente generato di D è principale; in altre parole, per ogni ideale I per cui esistano $a_1, a_2, \ldots, a_k \in A$ (con $k \in \mathbb{N}$) tali che $I = \big(\{a_1, a_2, \ldots, a_k\}\big)$ si ha anche $I = (a)$ per un opportuno elemento $a \in I$. Si dimostri inoltre che l'ultima identità vale se e soltanto se $a = \mathrm{MCD}(a_1, a_2, \ldots, a_k)$.

Suggerimento: L'enunciato segue facilmente per induzione dagli esercizi 18 e 19 qui sopra; in particolare, l'esercizio 18 copre il caso $k = 2$, cioè quello di ideali I generati da due elementi.