Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"
Corso di Laurea Triennale in Matematica

Anelli commutativi senza identità

Relatore:
Prof. Alberto Facchini

Laurenda:
Jennifer Parolin
Matricola 2058699

Anno Accademico 2021-2022
24/02/2022

Indice

Capitolo 1

Richiami e primi risultati

In questa tesi evidenziamo alcune differenze di comportamento tra anelli commutativi con identità e anelli commutativi senza identità. Ricordiamo brevemente la definizione di anello.

Definizione 1.1. Un *anello* $(R, +, \cdot)$ è dato da un insieme R sul quale sono definite due operazioni binarie, addizione $+$ e moltiplicazione $\cdot$, con le seguenti proprietà:

1. $(R, +)$ è un gruppo abeliano con identità 0_R;
2. $(R, \cdot)$ è un semigruppo;
3. valgono le leggi di distributività a destra e a sinistra, ossia $x(y+z) = xy+xz$ e $(x + y)z = xz + yz$ per ogni $x, y, z \in R$.

Un anello si dice *commutativo* se $\cdot$ è commutativa. Un *anello con identità* (o *unitario*) è un anello in cui esiste l'elemento neutro 1_R per la moltiplicazione. □

Per semplificare la notazione chiamiamo "anello" l'insieme R in vece della terna $(R, +, \cdot)$.

Per completezza riportiamo anche le definizioni di dominio d'integrità e di campo.

Definizione 1.2. Un anello commutativo con identità non nullo è un *dominio d'integrità* (in breve *dominio*) se non ha divisori dello zero. □

Definizione 1.3. Un anello commutativo con identità non nullo è un *campo* se ogni elemento non nullo è invertibile. □

Tutti gli anelli di questo elaborato sono commutativi, mentre non richiederemo a priori l'esistenza dell'identità.

Richiamiamo la definizione di omomorfismo d'anelli, seguita da una proposizione che generalizza un noto risultato di Algebra.

Definizione 1.4. Siano R ed S due anelli. Un'applicazione $\varphi\colon R \to S$ è detta *omomorfismo d'anelli* se rispetta entrambe le operazioni degli stessi, ovvero se è omomorfismo di gruppi additivi e omomorfismo di semigruppi moltiplicativi. Se R ed S hanno identità, rispettivamente 1_R e 1_S, se vale $\varphi(1_R) = 1_S$ allora φ è detto *omomorfismo d'anelli con identità*. □

Proposizione 1.5. *Se R è un anello con identità 1_R allora esiste un unico omomorfismo d'anelli con identità $h\colon \mathbb{Z} \to R$, definito da $h(z) = z1_R$ per ogni $z \in \mathbb{Z}$. Se invece R non ha identità allora c'è una corrispondenza biunivoca:*

$$\{\, h\colon \mathbb{Z} \to R \mid h \text{ omomorfismo d'anelli senza identità} \,\} \rightleftarrows \{\, e \mid e \in R, e \text{ idempotente} \,\}$$
$$(h\colon \mathbb{Z} \to R) \mapsto h(1)$$
$$(h_e\colon \mathbb{Z} \to R, \quad h_e(z) = ze \quad \forall z \in \mathbb{Z}) \hookleftarrow e$$

□

Seguono le nozioni di ideale e di ideale generato da un sottoinsieme dell'anello: la prima rimane invariata; la seconda pure nella sostanza, ma richiede maggior dettaglio nella sua esemplificazione.

Definizione 1.6. Sia R un anello. Un suo sottoinsieme I si dice *ideale* di R, e si indica con $I \trianglelefteq R$, se verifica le seguenti proprietà:

1. I è un sottogruppo additivo di R;
2. $rx \in I$ per ogni $r \in R$, $x \in I$. □

Definizione 1.7. Siano R un anello e X un suo sottoinsieme. L'*ideale generato* da X, indicato con $\langle X \rangle$, è il più piccolo ideale di R che contiene X, ovvero è l'intersezione degli ideali di R che contengono X, ed è così descritto:
se c'è 1_R, $\langle X \rangle = \{\, \sum_{i=0}^{n} r_i x_i \mid n \geq 0 \text{ intero}, x_i \in X, r_i \in R \,\}$;
se non c'è 1_R, $\langle X \rangle = \left\{\, \sum_{i=0}^{n} r_i x_i + \sum_{j=0}^{m} z_i x'_i \mid n, m \geq 0 \text{ interi}, x_i, x'_j \in X, r_i \in R, z_j \in \mathbb{Z} \,\right\}$.
□

La prossima proposizione descrive la ben nota struttura reticolare dell'insieme degli ideali di un anello.

Proposizione 1.8. *Sia R un anello. L'insieme degli ideali di R, dotato della relazione di inclusione $\subseteq$, risulta essere un reticolo, in cui per ogni $I, J \trianglelefteq R$ estremo superiore ed estremo inferiore sono:*

- $I \vee J := \langle I \cup J \rangle = I + J = \{\, i + j \mid i \in I, j \in J \,\}$.
- $I \wedge J := I \cap J$. □

Un'altra operazione tra ideali è il prodotto:

Definizione 1.9. Sia R un anello e siano I e J due suoi ideali. L'*ideale prodotto* di I e J è l'ideale $IJ := \langle \{\, ij \mid i \in I, j \in J \,\} \rangle$. □

Se un anello R ha identità vale sempre $RR = R$, ovvero R è idempotente. Se R è privo di identità ciò può non valere: si prenda per esempio $R = 2\mathbb{Z}$, per il quale $RR = 4\mathbb{Z}$; oppure R un anello nullo con moltiplicazione nulla. È anche possibile che un anello non abbia identità ma sia idempotente, vedi $R = \bigoplus_{\infty} \mathbb{Z}/2\mathbb{Z}$ dove, in particolare, ogni elemento dell'anello è idempotente. Un secondo esempio è dato dall'anello $R = \{\, f \colon \mathbb{R} \to \mathbb{R} \mid f \text{ è a supporto compatto} \,\}$, sul quale addizione e moltiplicazione sono definite puntualmente (qui per ogni $f \in R$ esiste $g \in R$ tale che $f = fg$).

In vista del prossimo richiamo indichiamo con $\mathscr{L}_p(R) = \{\, I \mid I \trianglelefteq R, I \neq R \,\}$ l'insieme degli ideali propri di un anello R: tale insieme è parzialmente ordinato dall'inclusione.

Definizione 1.10. Sia R un anello. Un ideale I di R è *massimale* se è un elemento massimale di $(\mathscr{L}_p(R), \subseteq)$. Un ideale I di R è *primo* se è proprio e per ogni $a, b \in R$ tali che $ab \in I$ allora $a \in I$ oppure $b \in I$ (ovvero se è proprio e per ogni $K, J \trianglelefteq R$ tali che $KJ \subseteq I$ allora $K \subseteq I$ oppure $J \subseteq I$). □

Se un anello R ha identità allora, come sappiamo, ogni suo ideale massimale è primo. Altrimenti questo risultato non è più vero in generale: si vedano infatti i due esempi seguenti.

Esempio 1.11. Sia $R = \frac{2\mathbb{Z}}{8\mathbb{Z}} = \{\, \bar{0}, \bar{2}, \bar{4}, \bar{6} \,\}$ anello con quattro elementi. I suoi ideali sono: $\frac{2\mathbb{Z}}{8\mathbb{Z}} = R$, $\frac{8\mathbb{Z}}{8\mathbb{Z}} = \{\, \bar{0} \,\}$ e $I := \frac{4\mathbb{Z}}{8\mathbb{Z}} = \{\, \bar{4}, \bar{0} \,\}$. L'unico ideale massimale di R è I, ma I non è primo, infatti $\bar{2} \cdot \bar{2} = \bar{4} \in I$ con $\bar{2} \notin I$. □

Esempio 1.12. Si consideri l'anello $2\mathbb{Z}$ e si consideri il suo ideale $4\mathbb{Z}$: esso è massimale ma non primo ($2 \cdot 2 = 4 \in 4\mathbb{Z}$, ma $2 \notin 4\mathbb{Z}$). □

La prossima proposizione caratterizza quando un ideale massimale è primo.

Proposizione 1.13. *Un ideale massimale M di un anello R è primo se e solo se $RR \nsubseteq M$.*

Dimostrazione. ($\Rightarrow$) Sia M ideale massimale e primo di R e supponiamo per assurdo che $RR \subseteq M$, quindi $R \subseteq M$ poiché M è primo. Allora $R = M$, assurdo perché M è proprio. (Osserviamo che non abbiamo di fatto utilizzato l'ipotesi sulla massimalità di M).
($\Leftarrow$) Sia M ideale massimale non primo di R. Allora esistono $x, y \in R$ tali che $x \notin M$, $y \notin M$, $xy \in M$. Pertanto $\langle x, M\rangle = R$ e $\langle y, M\rangle = R$ per la massimalità di M, e $\langle x, M\rangle \langle y, M\rangle \subseteq M$. Dunque $RR \subseteq M$. □

La definizione che segue riguarda una tipologia di anelli, quelli abeliani, che si incontrano sovente quando non si dà per scontata la presenza dell'identità.

Definizione 1.14. Un anello R è *abeliano* se $xy = 0$ per ogni $x, y \in R$, ovvero $RR = 0$. □

Osserviamo che un tale genere di anello non ha identità, a meno che non si tratti dell'anello nullo. Inoltre, in base a quanto appena visto, i suoi ideali massimali, quando esistono, non sono mai primi. Più precisamente, non ha mai ideali primi (se $I \lhd R$ e $a \in R \setminus I$, allora $a^2 = 0 \in I$). Tutti i suoi sottogruppi additivi sono ideali.

Esplicitiamo che cosa intendiamo in questo luogo con "anello semplice":

Definizione 1.15. Un anello R è *semplice* se i suoi unici ideali sono quelli banali, ossia R e 0, ed essi sono distinti. □

Annotiamo che in tal caso per ogni $a \in R$, $a \neq 0$, si ha $\langle a\rangle = R$.

La seguente proposizione descrive più nel dettaglio gli anelli semplici.

Proposizione 1.16. *Sia R un anello semplice. Allora si verifica una e una sola delle seguenti due condizioni:*

1. *R è un campo;*
2. *R è un anello abeliano finito con gruppo additivo ciclico di ordine primo, ovvero $R \cong \mathbb{Z}/p\mathbb{Z}$ con p primo e la moltiplicazione nulla.*

Dimostrazione. Per ogni $a \in R$ si ha $aR = R$ oppure $aR = 0$ per ipotesi. Sia $J := \{ a \in R \mid aR = 0 \}$. Allora J risulta essere un ideale di R, detto l'*annullatore* di R, quindi nuovamente $J = 0$ oppure $J = R$. Se $J = R$ allora $RR = 0$, cioè R è abeliano. In questo caso, per quanto osservato ogni sottogruppo additivo di R è un ideale, quindi dovendo essere R semplice l'unica possibilità è che esso sia finito di ordine primo. Se invece $J = 0$ abbiamo che $\forall a \in R$ con $a \neq 0$ vale $aR = R$. Se $a \neq 0$ consideriamo $ann(a) := \{ x \in R \mid ax = 0 \}$ detto l'*annullatore* di a. L'annullatore di a è un ideale, per cui ancora una volta esso è R oppure 0, ma essendo ora $J = 0$ si ha $ann(a) = 0$. Abbiamo ottenuto che se $a \neq 0$ esso non è un divisore dello zero, quindi è cancellabile. Sia ora $z \in R$ tale che $z \neq 0$. Poiché $zR = R$ allora $\exists e \in R$ tale che $ze = z$. Se $a \in R$ si ha $zea = za$, quindi per cancellazione di z abbiamo $ea = a$, perciò e è identità di R. Infine siccome per ogni $a \neq 0$ $aR = R$ allora $\exists a^{-1} \in R$ tale che $aa^{-1} = e$, ovvero ogni elemento non nullo di R è invertibile, quindi R è un campo. □

Osserviamo che la distinzione dei casi nella proposizione precedente dipende dalla presenza o meno dell'identità nell'anello. Sempre alla luce della stessa proposizione abbiamo che se un anello R è senza identità, allora vale l'implicazione 'semplice $\Rightarrow$ abeliano', mentre se un anello senza identità R è abeliano esso può essere semplice, e allora è della forma descritta al punto 2 della Prop. 1.16, oppure no. Per esempio si prenda l'insieme $\mathbb{Z}$ dotato dell'addizione usuale e con moltiplicazione nulla.
In aggiunta, ricordando che un ideale M di un anello R è massimale se e solo se R/M è semplice (questo per il teorema di corrispondenza), possiamo continuare con 'se e solo se R/M è del tipo 1 o 2 nella Prop. 1.16'. Ciò chiarisce quale aspetto della catena di implicazioni 'se M è ideale massimale dell'anello unitario $R \Rightarrow R/M$ è campo $\Rightarrow R/M$ è dominio $\Rightarrow M$ è primo' viene a mancare se non chiediamo ad R di avere identità: si tratta infatti della prima implicazione, mentre tutte le altre rimangono vere (si veda l'Esempio 1.12 sopracitato nel quale $4\mathbb{Z}$ è ideale massimale di $2\mathbb{Z}$, però $2\mathbb{Z}/4\mathbb{Z}$ non è campo). Questa osservazione conduce immediatamente ad una seconda versione della Proposizione 1.13.

Proposizione 1.17. *Un ideale massimale M di un anello R è primo se e solo se R/M è campo.* □

Un'ulteriore considerazione può essere fatta ricordando che negli anelli non nulli con identità esistono sempre ideali massimali, i quali sono sempre primi,

quindi tali anelli hanno sempre ideali primi. D'altro canto se un anello non ha identità può capitare che esso non abbia ideali primi, vedi Esempio 1.11 oppure qualsiasi anello abeliano, così come può capitare che non abbia ideali massimali: quest'ultima situazione può essere senz'altro costruita artificiosamente a partire da un gruppo abeliano senza sottogruppi massimali al quale aggiungere la moltiplicazione nulla, vedi ad esempio ($\mathbb{Q}, +$ canonica, $\cdot$ nulla). Per maggiori dettagli, si veda il Capitolo 5. Come immediata conseguenza di questi ragionamenti, in un anello senza identità non sempre tutti gli ideali propri sono contenuti in qualche ideale massimale e/o primo.

Le definizioni sottostanti riguardano la caratteristica di un anello, a seconda che questo abbia identità o meno.

Definizione 1.18. Sia R un anello con identità. La sua *caratteristica*, indicata con $char(R)$, è il più piccolo intero $n > 0$ tale che $\underbrace{1_R + \cdots + 1_R}_{n \text{ volte}} = 0_R$ se un tale n esiste, altrimenti si pone $char(R) = 0$. □

Si osservi che $char(R) = 1$ se e solo se $1_R = 0_R$, ovvero $R = 0$. Si ottiene poi che il sottoanello fondamentale P di R è isomorfo a $\mathbb{Z}/n\mathbb{Z}$ se $char(R) > 0$, a $\mathbb{Z}$ se $char(R) = 0$ (in ambo i casi mediante l'unico omomorfismo $h\colon \mathbb{Z} \to R$ d'anelli con identità).

Definizione 1.19. Sia R un anello senza identità. La sua *caratteristica*, indicata con $char(R)$, è il più piccolo intero $n > 0$ tale che $nx = 0$ per ogni $x \in R$, se un tale n esiste. Altrimenti si pone $char(R) = 0$. □

Da notare che se R è finito $char(R)$ è nient'altro che l'esponente additivo di R, il quale divide la cardinalità di R ed è perciò finito $\neq 0$. Nell'Esempio 1.11, dove $|R| = 4$, si ha $char(R) = 4$, infatti tale R è additivamente ciclico.

Seguono due proposizioni che trattano di caratteristica e che prescindono dall'esistenza dell'identità.

Proposizione 1.20. *Se R è un anello senza divisori dello zero, allora la sua caratteristica è zero, oppure un primo, oppure uno.*

Dimostrazione. Per assurdo sia $char(R) = n \neq 0$ e $\neq 1$ con n non primo, quindi $n = mk$ con m e k interi tali che $0 < m, k < n$. Poiché né m né k sono $char(R)$ devono esistere $a, b \in R$ tali che $ma \neq 0$ e $kb \neq 0$, ma allora $0 = n(ab) = mk(ab) = (ma)(kb)$ e quindi R ha divisori dello zero. □

Proposizione 1.21. *Se R è anello senza divisori dello zero e $char(R) = n > 0$, allora tale n è per ogni $x \in R$ $x \neq 0$ il più piccolo intero positivo tale che $nx = 0$.*

Dimostrazione. Per assurdo $\exists y \in R$ $y \neq 0$ tale che $my = 0$ con m intero $0 < m < n$. Poiché m non è caratteristica di R deve $\exists x \in R$ $x \neq 0$ tale che $mx \neq 0$. Dunque $0 \neq (mx)y = mxy = x(my) = 0$ assurdo. □

Le seguenti proposizioni riportano un paio di risultati che non richiedono a priori l'esistenza dell'identità.

Proposizione 1.22. *Se R è un anello finito senza divisori dello zero, allora o è un campo oppure è l'anello nullo.*

Dimostrazione. Sia $a \in R$ tale che $a \neq 0$. Si consideri l'applicazione $\bar{a}\colon R \to R$ definita da $\bar{a}(x) := ax$ per ogni $x \in R$. Essa è iniettiva, infatti se $r, s \in R$ tali che $ar = as$ cioè $a(r - s) = 0$ allora $r = s$ perché in R non ci sono divisori dello zero. Quindi $\bar{a}$ è anche suriettiva perché R è finito. Ma allora $\exists x \in R$ tale che $ax = a$. Ora per ogni $b \in R$ $ba = bxa$, quindi per cancellazione di a otteniamo $b = bx$ cioè x è identità di R. Infine per ogni $a \in R$ $a \neq 0$ $\exists a^{-1} \in R$ tale che $aa^{-1} = x$, ossia ogni elemento di R non nullo è invertibile, cioè R è campo. □

Proposizione 1.23. *Se R è un anello senza divisori dello zero, allora gli unici elementi idempotenti sono lo zero e l'eventuale identità.*

Dimostrazione. Se $e \in R$ $e \neq 0$ $e^2 = e \Rightarrow$ per ogni $r \in R$ $e(er - r) = e^2r - er = er - er = 0 \Rightarrow er = r$ $\forall r \in R \Rightarrow e = 1_R$. □

Di conseguenza un anello R senza identità e senza divisori dello zero non può avere un sottoanello non nullo con una propria identità.

La prossima proposizione è particolarmente utile, assieme alla Proposizione 1.23, per dimostrare in modo alternativo la Proposizione 1.16.

Proposizione 1.24. *Se in un anello un ideale è principale e idempotente, allora è generato da un elemento idempotente dell'anello.*

Dimostrazione. Supponiamo, come primo caso, che R sia privo di identità. Sia $a \in R$ tale che $\langle a \rangle = \{\, ar + za \mid r \in R, z \in \mathbb{Z} \,\} = \langle a \rangle^2 = \langle a^2 \rangle$. In particolare $a = a^2\bar{r} + \bar{z}a^2$ per opportuni $\bar{r} \in R$ e $\bar{z} \in \mathbb{Z}$. Sia $e := a\bar{r} + \bar{z}a$. Allora e è idempotente. Infatti $ee = (a\bar{r} + \bar{z}a)(a\bar{r} + \bar{z}a) = a^2\bar{r}^2 + \bar{z}^2a^2 + 2\bar{z}\bar{r}a^2 = \bar{r}(a - \bar{z}a^2) + \bar{z}(a - a^2\bar{r}) + 2\bar{z}\bar{r}a^2 = a\bar{r} - \bar{z}\bar{r}a^2 + \bar{z}a - \bar{z}\bar{r}a^2 + 2\bar{z}\bar{r}a^2 = a\bar{r} + \bar{z}a = e$. Inoltre $\langle a \rangle = \langle e \rangle$,

in quanto $e = a\bar{r} + \bar{z}a \in \langle a \rangle \Rightarrow \langle e \rangle \subseteq \langle a \rangle$, poi $a = ea \Rightarrow a \in \langle e \rangle \Rightarrow \langle a \rangle \subseteq \langle e \rangle$. Se R ha identità la dimostrazione procede in maniera del tutto parallela con i dovuti aggiustamenti. □

Dimostrazione alternativa della Proposizione 1.16. Sappiamo che per ogni $a \in R$ $a \neq 0$ si ha $\langle a \rangle = R$. Se R ha identità allora $\langle a \rangle = aR = R$, quindi se $a \neq 0$, $\exists a^{-1} \in R$ tale che $aa^{-1} = 1$, ovvero ogni elemento non nullo di R è invertibile, quindi R è un campo. Se invece R non ha identità consideriamo l'ideale 0 che è massimale per ipotesi. Se esso non è primo allora per la Proposizione 1.13 abbiamo $RR \subseteq 0$, cioè R è abeliano. Ma ogni suo sottogruppo additivo è un ideale, quindi poiché R è semplice R è necessariamente finito di ordine primo. Se invece l'ideale 0 è primo, ovvero R non ha divisori dello zero, allora come ricordato poc'anzi $RR \nsubseteq 0$. Ma essendo R semplice, otteniamo $RR = R$, in particolare $\langle a \rangle^2 = \langle a \rangle$. Ma allora per la Proposizione 1.24 R contiene un elemento idempotente non nullo: assurdo in virtù della Proposizione 1.23. □

Capitolo 2

Estensioni

2.1 Aumentazione ed estensione di Dorroh

In questa sezione mostriamo come descrivere gli anelli senza identità mediante anelli con identità. Iniziamo con una serie di tre definizioni.

Definizione 2.1. Un *anello con identità con aumentazione* è una coppia (R, f) dove R è anello con identità e $f\colon R \to \mathbb{Z}$ è omomorfismo d'anelli con identità (f è detta *aumentazione*). □

Definizione 2.2. Siano (R, f) e (R', f') anelli con identità con aumentazione. Un'applicazione $\varphi\colon R \to R'$ è detta *omomorfismo d'anelli con identità con aumentazione* se è omomorfismo d'anelli con identità e rende commutativo il seguente diagramma:

$$\begin{array}{ccc} R & \xrightarrow{f} & \mathbb{Z} \\ {\scriptstyle\varphi}\downarrow & \nearrow_{f'} & \\ R' & & \end{array}$$

□

Definizione 2.3. Sia R un anello. L'*estensione di Dorroh* di R è un anello, indicato con R_+, dato dall'insieme $\mathbb{Z} \oplus R := \{\, (z, r) \mid z \in \mathbb{Z}, r \in R \,\}$ sul quale sono definite le seguenti operazioni, per ogni (z, r), (z', r') in $\mathbb{Z} \oplus R$:

- $(z, r) + (z' + r') = (z + z', r + r')$ ossia R_+ è, come gruppo additivo, la somma diretta di R e $\mathbb{Z}$;
- $(z, r) \cdot (z', r') = (zz', zr' + z'r + rr')$. □

Tale estensione prende il nome da J. L. Dorroh, che per primo la costruì in [3]. Risulta che $(1,0)$ è identità di R_+. L'insieme $\bar{R} := \{\, (0,r) \in R_+ \,\}$ è un ideale di R_+ ed ha una propria identità se e solo se R ce l'ha (in tal caso si tratta di $(0,1_R)$, sempre distinta dall'identità di R_+). L'anello di partenza R è naturalmente isomorfo a $\bar{R}$: l'applicazione $\bar{f}\colon R \to R_+$, definita da $\bar{f}(r) = (0,r)$ per ogni r in R, è omomorfismo d'anelli iniettivo e ha immagine $\bar{R}$. Abbiamo così provato la seguente proposizione:

Proposizione 2.4. *Ogni anello (senza identità) può essere immerso come ideale in un anello con identità.* □

A questo punto tutte le nozioni viste in questo capitolo vanno a sommarsi. Infatti, dato una anello R e la sua estensione di Dorroh R_+, si può affiancare ad R_+ un'aumentazione canonica f^+ ponendo, per ogni (z,r) in R_+, $f^+(z,r) = z$. Tale f^+ è suriettiva e il suo nucleo è $\bar{R}$. Dunque, per il primo teorema di omomorfismo per gli anelli, otteniamo $R_+/\bar{R} \cong \mathbb{Z}$. Infine, c'è la seguente corrispondenza biunivoca:

$$\begin{aligned} \{\text{ anelli }\} &\rightleftarrows \{\text{ anelli con identità con aumentazione }\} \\ R &\mapsto (R_+, f^+) \\ \ker g &\mapsfrom (S,g) \end{aligned}$$

In particolare, questo risultato ci consente di "pensare" gli anelli (senza identità) come ideali di opportuni anelli con identità con aumentazione. Osserviamo inoltre che la corrispondenza appena vista rispetta anche gli omomorfismi: se $h\colon R \to R'$ è omomorfismo d'anelli, allora $\iota_{\mathbb{Z}} \oplus h\colon R_+ \to R'_+$, definito da $(z,r) \mapsto (z, h(z))$ per ogni (z,r) in R_+, è omomorfismo d'anelli con identità con aumentazione; viceversa, se $\varphi\colon (S,f) \to (S',f')$ è omomorfismo d'anelli con identità con aumentazione, allora $\varphi|_{\ker f}^{\ker f'}\colon \ker f \to \ker f'$ è omomorfismo d'anelli. Riassumendo, c'è la corrispondenza biunivoca:

$$\begin{aligned} \{\text{ omomorfismi d'anelli }\} &\rightleftarrows \{\text{ omomorfismi d'anelli con identità con aumentazione }\} \\ \big(h\colon R \to R'\big) &\mapsto \iota_{\mathbb{Z}} \oplus h \\ \varphi|_{\ker f}^{\ker f'} &\mapsfrom \big(\varphi\colon (S,f) \to (S',f')\big) \end{aligned}$$

2.2 Altre estensioni

In questa sezione forniamo un'introduzione al tema delle estensioni d'anelli, adattato alle nostre esigenze. Iniziamo con la definizione di estensione:

Definizione 2.5. Sia R un anello. Un anello S è un'*estensione* di R se S è un anello con identità ed esiste un omomorfismo iniettivo d'anelli $f\colon R \to S$. □

In riferimento alla definizione appena data, nel caso dell'estensione di Dorroh abbiamo chiamato l'omomorfismo $\bar{f}$.

Oltre alla Dorroh, molte altre estensioni sono state studiate, spesso con lo scopo di preservare una determinata proprietà dell'anello di partenza, laddove a livello teorico non vi siamo impedimenti. Alcune estensioni sono varianti o generalizzazioni di estensioni già note. Altre richiedono una tecnica di costruzione inedita. Vediamo ora nel dettaglio altri esempi basilari di estensioni. Rimandiamo invece al Corollario 4.2, nel Capitolo 4, la trattazione della proprietà di noetherianità in un certo tipo di estensioni.

Estensione di Albert Riprendendo l'estensione di Dorroh, possiamo notare che essa ha sempre caratteristica nulla, indipendentemente dall'anello che estende. Quest'aspetto intrinseco viene ereditato da $\mathbb{Z}$, in base alla definizione dell'operazione + dell'estensione. Quindi se R è anello con $char(R) = 0$, allora la sua estensione di Dorroh R_+ ne rispetta la caratteristica. Se invece $char(R) = m \neq 0$ e cerchiamo un'estensione che abbia ancora caratteristica m, possiamo variare la Dorroh: sostituiamo $\mathbb{Z}/m\mathbb{Z}$ a $\mathbb{Z}$, avendo cura di aggiustare la definizione delle operazioni, ma mantenendo esattamente la stessa logica (allo stesso modo l'immersione di R nell'estensione è del tutto analoga alla precedente). Viene detta *estensione di Albert* di un anello R quella che, a seconda che R abbia caratteristica 0 oppure $m \neq 0$, è la Dorroh o la variazione appena proposta, rispettivamente. L'estensione di Albert rispetta quindi sempre la caratteristica di un anello. Tale estensione prende il nome da A. A. Albert, il quale la presentò in [1].

Estensione di Szendrei Un'altra proprietà che l'estensione di Dorroh non mantiene in generale è l'assenza di divisori dello zero (altrimenti detta *integrità*). Infatti se consideriamo l'anello degli interi pari $2\mathbb{Z}$, abbiamo che in $2\mathbb{Z}_+$ ci sono molti divisori dello zero, giacché vale per esempio $(2, -2)(0, 4) = (0, 0)$. Vediamo

ora come modificare l'estensione di Dorroh mantenendo l'integrità. Sia R un anello senza divisori dello zero non nullo (se $R = 0$ allora R stesso è l'estensione cercata, come mostra peraltro il metodo che stiamo per descrivere, con qualche piccola modifica). Consideriamo in R_+ l'insieme $I := \{\, x \in R_+ \mid xa = 0 \ \forall a \in \bar{R} \,\}$, che risulta essere un ideale di R_+ (si tratta dell'annullatore di $\bar{R}$). Osserviamo che vale $I \cap \bar{R} = 0$, per definizione di I e perché $\bar{R}$, esattamente come R, non ha divisori dello zero. Poi I è un ideale proprio di R_+, poiché per esempio $(1, 0) \notin I$. Inoltre I è primo. Infatti se per assurdo esistono $x, y \in R_+$ tali che $xy \in I$ (ovvero $xya = 0$ per ogni $a \in \bar{R}$), ma né x né $y \in I$, allora esistono $x_0, y_0 \in \bar{R}$ tali che $xx_0 \neq 0$ e $yy_0 \neq 0$, quindi $0 = (xy)(x_0y_0) = (xx_0)(yy_0) \neq 0$, assurdo perché $\bar{R}$ non ha divisori dello zero. Abbiamo pertanto ottenuto che il quoziente R_+/I è un dominio. Se indichiamo con π la proiezione canonica di R_+ su R_+/I, la sua restrizione ad $\bar{R}$ ha nucleo nullo (vedi quanto detto su $I \cap \bar{R}$), ovvero $\pi\big|_{\bar{R}} \colon \bar{R} \to R_+/I$ è omomorfismo d'anelli iniettivo. Dunque R_+/I è l'estensione cercata di R (qui l'omomorfismo iniettivo d'anelli di R in R_+/I è dato dalla composizione $\pi\big|_{\bar{R}} \circ \bar{f}$). Chiamiamo quest'estensione *di Szendrei*, come in [12], a partire dall'articolo di J. Szendrei [11] che la contiene. Anche in questa circostanza R è isomorfo ad un ideale dell'estensione, in quanto $R \cong \bar{R} \cong \pi\big|_{\bar{R}}(\bar{R}) = \pi(\bar{R}) = \frac{\bar{R}+I}{I} \trianglelefteq \frac{R_+}{I}$. Inoltre, questo tipo di estensione rispetta anche la caratteristica di R. Infatti, se $char(R) = 0$ e per assurdo $char(R_+/I) = n \neq 0$, allora per ogni $r \in R$ si ha che $n(0, r) \in I$, cioè $(0, nr) \in I$, ma $I \cap \bar{R} = 0$, quindi $nr = 0$ per ogni $r \in R$ assurdo. Se invece $char(R) = n \neq 0$ allora risulta che $nR_+ \subseteq I$. Perciò, per ogni $(z, r) + I \in R_+/I$ abbiamo che $n(z, r) + I = I$. Lo stesso non vale se usiamo $0 \neq m < n$, dunque $char(R_+/I) = n$.

Estensioni minimali La tipologia di estensioni trattata in questo paragrafo risulterà essere in relazione stretta con quelle finora incontrate. Sia R un anello e sia S una sua estensione, con $f \colon R \to S$ omomorfismo iniettivo d'anelli. Allora S contiene il sottoanello $S^* := f(R)+\mathbb{Z}1_S = \{\, f(r) + z1_S \mid r \in R, z \in \mathbb{Z} \,\}$, generato dall'immagine di f e dall'identità di S. Nell'anello S^* le operazioni sono definite in modo naturale, per ogni $f(r)+z1_S$, $f(r')+z'1_S$ in S^*: $(f(r)+z1_S)+(f(r')+z'1_S) = f(r+r')+(z+z')1_S$ e $(f(r)+z1_S)\cdot(f(r')+z'1_S) = f(rr'+z'r+zr')+zz'1_S$. Risulta che S^* è estensione di R (per la prova si consideri la corestrizione di f ad S^*). Diciamo che S è *estensione minimale* di R se $S = S^*$.

Osserviamo che l'estensione di Dorroh R_+ di R è effettivamente un'estensione minimale di R, infatti si verifica immediatamente che $R_+ = (R_+)^*$ (si ricordi

l'omomorfismo $\bar{f}$ definito in precedenza). Abbiamo così scoperto il motivo della natura delle operazioni dell'estensione di Dorroh: esse sostanzialmente mimano quelle di una qualsiasi estensione minimale, inserite in un apparato che ragiona per componenti.

È naturale chiedersi se anche l'estensione di Albert, nel caso di caratteristica positiva, sia un'estensione minimale. Vediamo ora il ragionamento che ci porta a rispondere affermativamente. Sia R un anello con $char(R) = n \neq 0$. Consideriamo l'insieme nR_+, che è un ideale di R_+. In particolare $nR_+ \cap \bar{R} = 0$. Risulta che R_+/nR_+ è un'estensione di R di caratteristica n (qui l'omomorfismo iniettivo d'anelli $f\colon R \to R_+/nR_+$ è dato da $f(r) = (0,r) + nR_+$ per ogni r in R). Naturalmente l'applicazione $\varphi\colon R_+/nR_+ \to \mathbb{Z}/n\mathbb{Z} \oplus R$, definita da $\varphi((z,r) + nR_+) = (\bar{z}, r)$ per ogni $(z,r) + nR_+$ in R_+/nR_+, è isomorfismo d'anelli con identità. Infine $(\mathbb{Z}/n\mathbb{Z} \oplus R)^* = \varphi(f(R)) + \mathbb{Z}((\bar{1},0)) = \{\, (\bar{0},r) + z(\bar{1},0) \mid r \in R, z \in \mathbb{Z} \,\} = \{\, (\bar{z},r) \mid r \in R, z \in \mathbb{Z} \,\} = \mathbb{Z}/n\mathbb{Z} \oplus R$.

Prima di trattare lo stesso quesito anche a proposito dell'estensione di Szendrei, ci soffermiamo sulla caratterizzazione delle estensioni minimali. Se $R_1 \subseteq R_2$ sono anelli, diciamo che un ideale A_2 di R_2 *giace sopra* un ideale A_1 di R_1 se $A_2 \cap R_1 = A_1$. Ora sia R un anello e sia S un'estensione minimale di R, con $f\colon R \to S$ omomorfismo iniettivo d'anelli. Consideriamo l'applicazione $g\colon R_+ \to S$ definita da $g(z,r) = f(r) + z1_S$. Allora g è omomorfismo d'anelli, è suriettivo (quindi $S \cong R_+/\ker g$) e il suo nucleo è un ideale di R_+ che giace sopra 0 in $\bar{R}$. Viceversa, se C è un ideale di R_+ che giace sopra 0 in $\bar{R}$, allora R_+/C è estensione minimale di R. Riassumendo, c'è la corrispondenza biunivoca:

$$\{\, C \mid C \trianglelefteq R_+ \text{ che giace sopra 0 in } \bar{R} \,\} \rightleftarrows \{\, S \mid S \text{ estensione minimale di } R \,\}$$

Ovvero le estensioni minimali di R sono isomorfe a R_+/C, per qualche C ideale di R_+ che giace sopra 0 in $\bar{R}$.

Se riprendiamo ora in esame l'estensione di Szendrei, possiamo subito concludere che essa è minimale. Infatti si tratta proprio di R_+/I, con $I \cap \bar{R} = 0$.

Capitolo 3

Il contributo di Gilmer

Nell'introduzione all'articolo [2] l'autore, D. D. Anderson, afferma che circa trenta articoli di Robert Gilmer coinvolgono gli anelli senza identità. In questo capitolo ci occuperemo in particolare di uno di questi, ovvero [4]. Seguiremo abbastanza fedelmente la struttura dei risultati che vi compaiono, ai quali aggiungeremo, dove lo riterremo utile, dimostrazioni e commenti.

Iniziamo col dare due definizioni delle quali faremo ampio uso.

Definizione 3.1. Sia R un anello e sia $I \trianglelefteq R$. Il *radicale* di I, indicato con $\sqrt{I}$, è l'ideale $\{ r \in R \mid r^n \in I, \exists n \in \mathbb{N}, n \geq 1 \}$. □

Osserviamo che vale sempre $I \subseteq \sqrt{I}$, così come $\sqrt{\sqrt{I}} = \sqrt{I}$. Inoltre, se I è primo allora $I = \sqrt{I}$.

Definizione 3.2. Sia R un anello. Un ideale Q di R è detto *primario* se è proprio e per ogni $x, y \in R$ tali che $xy \in Q$ allora $x \in Q$ oppure $y \in \sqrt{Q}$. □

Notiamo che se un ideale è primo allora è primario.

Proseguiamo col riportare un elenco di undici proprietà, o condizioni, che un anello R può verificare o meno, alcune delle quali sono già sorte nel primo capitolo. Come nell'articolo originale $R \neq 0$ e chiamiamo le proprietà con le lettere A-L, omettendo la lettera I.

***A*:** R ha identità.

***B*:** R è generato da elementi idempotenti, ossia se $r \in R$ allora $r = r_1e_1 + \cdots + r_ne_n + z_1e_1 + \cdots + z_ne_n$, dove per ogni $i = 1, \ldots, n$ $r_i \in R$, $e_i \in R$ idempotenti, $z_i \in \mathbb{Z}$.

***C*:** Se A è un ideale non nullo di R tale che $\sqrt{A} \neq R$, allora R/A ha identità.

***D*:** Se $x \in R$ allora esiste $y \in R$ tale che $x = xy$.

***E*:** Se A è un ideale proprio di R allora $\sqrt{A} \neq R$.

***F*:** R è idempotente.

***G*:** Gli ideali massimali di R sono primi.

***H*:** Se P è un ideale primo non nullo di R, allora R/P ha identità.

***J*:** Un ideale A di R tale che $\sqrt{A}$ è massimale è primario.

***K*:** Ogni ideale proprio di R è contenuto in un ideale massimale.

***L*:** Se A e B sono ideali comassimali propri di R, allora $AB = A \cap B$.

Un anello che soddisfa E è detto *u-ring*. È facile verificare che tutte queste proprietà si preservano per passaggio a quoziente. Il nostro scopo è studiare le relazioni che intercorrono tra le varie condizioni. Il primo passo consiste nel dimostrare che A implica tutte le altre: in alcuni casi il risultato è immediato (proprietà B,C,D,F,H), in altri è sufficiente una traccia, in altri ancora riportiamo una dimostrazione completa.

A*⇒*E Si compongono i seguenti due fatti: il primo, in un anello con identità un ideale è proprio se e solo se non contiene l'identità; il secondo, un elemento idempotente di un anello appartiene ad un ideale se solo se appartiene al suo radicale.

A*⇒*G Si usa la sequenza di implicazioni nominata in precedenza: se A è un ideale massimale di un anello unitario $R \Rightarrow R/A$ è campo $\Rightarrow R/A$ è dominio $\Rightarrow A$ è primo.

A*⇒*J Sia R anello con identità e sia A un suo ideale tale che $\sqrt{A}$ è massimale. Dobbiamo provare che A è primario. Per ipotesi A è proprio. Poi siano $x, y \in R$ tali che $xy \in A$ e $y \notin \sqrt{A}$. Allora $\sqrt{A} + \langle y \rangle = R$. Quindi esistono $m \in \sqrt{A}$ e $r \in R$ tali che $m + ry = 1$. In particolare esiste $n \in \mathbb{N}$, $n \geq 1$, tale che $m^n \in A$. Elevando la precedente identità alla n otteniamo $1 = 1^n = (m + ry)^n = m^n + sy$, con $s \in R$. Infine moltiplicando ambo i membri per x abbiamo $x = xm^n + sxy$, quindi $x \in A$. Perciò A è primario.

A*⇒*K Sia R anello con identità e sia A un suo ideale proprio. Si applica il lemma di Zorn all'insieme degli ideali propri che contengono A, insieme parzialmente ordinato dall'inclusione. Questo argomento fornisce l'esistenza di un ideale massimale di R che contiene A.

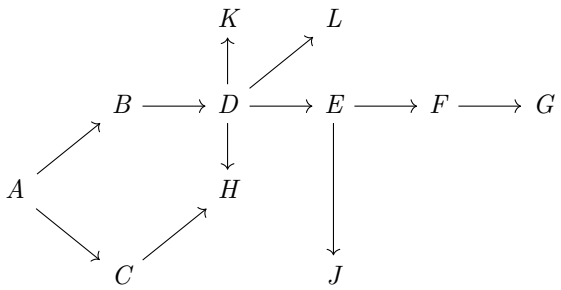
A*⇒*L Sia R anello con identità e siano A e B due suoi ideali propri e comassimali. Dimostriamo, tramite doppia inclusione, che $AB = A \cap B$. Poiché ogni generatore di AB, ovvero un elemento di tipo ab con $a \in A$ e $b \in B$, appartiene sia ad A che a B, allora $AB \subseteq A \cap B$. Viceversa, sia $c \in A \cap B$. Per ipotesi $A + B = R$, quindi esistono $a \in A$ e $b \in B$ tali che $a + b = 1$. Moltiplichiamo l'identità per c e otteniamo $c = ca + cb$. Dunque $c \in AB$. Ovvero $A \cap B \subseteq AB$.

In tutte le implicazioni appena viste l'identità gioca, in qualche modo, un ruolo fondamentale. Ciò suggerisce che se un anello non è unitario, ossia non soddisfa A, allora le rimanenti dieci condizioni potrebbero non valere. Prendiamo in considerazione, per esempio, l'anello $2\mathbb{Z}$. In precedenza abbiamo già osservato come, in questo caso, F e G non siano vere ($2\mathbb{Z} \cdot 2\mathbb{Z} = 4\mathbb{Z} \neq 2\mathbb{Z}$, l'ideale $4\mathbb{Z}$ è massimale ma non primo). Inoltre, siccome $2\mathbb{Z}$ non ha divisori dello zero, l'unico elemento idempotente è lo zero (vedi Prop. 1.23), che genera l'ideale nullo: per questo, B non vale. Sempre lo zero ci porta alla medesima conclusione riguardo D: infatti è l'unico elemento che la verifica. L'ideale $4\mathbb{Z}$ permette di negare anche E: il suo radicale è proprio $2\mathbb{Z}$. Per quanto concerne L, abbiamo che gli ideali $4\mathbb{Z}$ e $6\mathbb{Z}$ sono propri e comassimali, tuttavia $24\mathbb{Z} = 4\mathbb{Z} \cdot 6\mathbb{Z} \neq 4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$. Infine, l'ideale $12\mathbb{Z}$ ha radicale $6\mathbb{Z}$, che è massimale, però $2\mathbb{Z}/12\mathbb{Z}$ non ha identità (per la verifica sono sufficienti i prodotti $\bar{2} \cdot \bar{4} = \bar{8}$, $\bar{6} \cdot \bar{8} = \bar{0}$, $\bar{10} \cdot \bar{2} = \bar{8}$): di conseguenza, C è falsa. Esattamente la stessa motivazione smentisce J: si applica il Lemma 3.19, che vedremo più avanti (in alternativa, qui, $12\mathbb{Z}$ non è primario perché $6 \cdot 2 = 12 \in 12\mathbb{Z}$, $6 \notin 12\mathbb{Z}$ ma $2 \notin 6\mathbb{Z}$). Le uniche condizioni che $2\mathbb{Z}$ realizza sono H e K: le ragioni risiedono nella struttura del reticolo di ideali dell'anello. Si può dimostrare, infatti, che tra gli ideali di $2\mathbb{Z}$, i quali sono tutti della forma $2n\mathbb{Z}$ con n naturale, sono massimali quelli del tipo $2p\mathbb{Z}$ con p primo; mentre sono primi, oltre all'ideale nullo, tutti i massimali eccetto $4\mathbb{Z}$.

Un anello senza identità che falsifica K è $\mathbb{Q}$ abeliano, poiché, come già detto, non ha ideali massimali. Più in generale, un anello abeliano (non nullo per ipotesi), non ha mai le seguenti proprietà: B, giacché 0 è l'unico idempotente; D, vera solo per 0; E, in quanto tutti gli ideali hanno per radicale l'intero anello; F, per

definizione di anello abeliano. Le condizioni C, H e J, invece, sono sempre vere a vuoto. Volendo contraddire le restanti G ed L con un anello abeliano, scegliamo $2\mathbb{Z}$ abeliano: vi sono ideali massimali, cioè quelli appena identificati con $2\mathbb{Z}$ canonico, ma nessuno è primo; gli ideali $4\mathbb{Z}$ e $6\mathbb{Z}$ sono propri e comassimali, la loro intersezione è $12\mathbb{Z}$, il loro prodotto è l'ideale nullo.
Resta da indicare un anello non unitario per il quale H sia falsa: per questo specifico caso utilizziamo l'anello $R = 2\mathbb{Z} \times 2\mathbb{Z}$. In esso l'ideale $P := 0 \times 2\mathbb{Z}$ è primo e non nullo, però R/P non ha identità.

Alla ricerca di relazioni tra le undici proprietà, finora abbiamo dimostrato che A implica tutte le altre. Il prossimo passo prevede di studiare in toto le implicazioni semplici esistenti tra le condizioni B-L. Il diagramma sottostante descrive quello che sarà il risultato finale del nostro lavoro.



La sezione 4 di [4] contiene una serie di esempi per mostrare che nessun'altra implicazione può essere aggiunta al diagramma (che quindi non contiene equivalenze). Analizzando quest'ultimo, facciamo alcune riflessioni. La prima: dato un anello senza identità, il suo comportamento rispetto alle proprietà B-L non può essere del tutto arbitrario, infatti è vincolato a rispettare le relazioni che sussistono tra di esse; per questo motivo, il diagramma può essere considerato una valida guida per chi si approccia agli anelli non unitari. La seconda: prendendo in prestito la terminologia dei grafi, il diagramma è un'unica componente connessa, quindi spesso è facile stabilire quali proprietà siano più forti di altre. La terza e ultima: il diagramma mette in luce come quasi tutte le implicazioni $A \Rightarrow B$-L, provate in precedenza, siano ulteriormente scomponibili, ovvero, per ottenere le tesi, quasi sempre non è necessaria la presenza dell'identità, piuttosto è sufficiente una qualche sua conseguenza (vedi ad esempio $A \Rightarrow L$, in cui basta disporre di D per provare la seconda inclusione, omettendo il passaggio, l'unico, che usa direttamente l'unità).

Per poter dimostrare tutte le implicazioni del diagramma, dobbiamo prima

vedere una serie risultati utili a tale scopo, iniziando da un paio di teoremi, ai quali seguiranno quattro corollari (un ulteriore corollario, il 4.2, si trova nel capitolo successivo). Da qui fino alla fine del capitolo, se S è estensione minimale di R, sottintenderemo, senza perdere di generalità, che R è sottoanello di S e che l'omomorfismo iniettivo d'anelli di R in S è l'inclusione.

Teorema 3.3. *Siano R ed S due anelli tali che S è estensione minimale di R. Allora:*
a) un sottoinsieme A di R è un ideale di R se e solo se è un ideale di S;
b) se A è un ideale di S tale che $A \cap R$ è un ideale finitamente generato di R, allora A è un ideale finitamente generato di S.

Dimostrazione. Sia e l'identità di S, quindi per ipotesi

$$S = R[e] = \{\, v + ze \mid v \in R, z \in \mathbb{Z} \,\}$$

a) Sia $A \subseteq R$. Se $A \trianglelefteq S$ allora è immediato che $A \trianglelefteq R$. Viceversa, se $A \trianglelefteq R$ allora $\emptyset \neq A \subseteq S$, $a - b \in A$ per ogni $a, b \in A$, $a(v + ze) = av + za \in A$ per ogni $v + ze \in S$: dunque $A \trianglelefteq S$.
b) Innanzitutto, $A \trianglelefteq S$ per ipotesi, $R \trianglelefteq S$ per il punto a), quindi $A \cap R$ è un ideale di S ed è un sottoinsieme di R, allora, di nuovo per il punto a), $(A \cap R) \trianglelefteq R$. Poi, sia $\{\, a_1, \ldots, a_k \,\}$ un insieme di generatori per l'ideale $A \cap R$ in R. Sia $G := \{\, m \in \mathbb{Z} \mid v + me \in A, \exists v \in R \,\}$. Risulta che G è un sottogruppo del gruppo additivo degli interi. Infatti, G non è vuoto poiché 0 vi appartiene. Inoltre, se $m, n \in G$, ovvero esistono $v, w \in R$ tali che $v + me = a \in A, w + ne = b \in A$, allora $v - w + (m - n)e = v - w + a - v - b + w = a - b \in A$, quindi $m - n \in G$. In particolare, G è ciclico, ovvero esiste $q \in \mathbb{Z}$ tale che $G = q\mathbb{Z}$. Sia $v \in R$ tale che $v + qe = a \in A$. Dimostreremo che $\{\, a_1, \ldots, a_k, a \,\}$ è un insieme di generatori per A in S. Sia $a' = u + se \in A$, quindi $s = mq$ con $m \in \mathbb{Z}$. Abbiamo che $a' - ma = u + mqe - mv - mqe = u - mv \in A \cap R$. Dunque, per ipotesi, $a' - ma = \sum_{i=0}^{k} r_i a_i + \sum_{j=0}^{k} z_j a_j$, con $r_i \in R$ per ogni i, $z_j \in \mathbb{Z}$ per ogni j. Isolando a' nell'ultima identità otteniamo la tesi. □

Teorema 3.4. *Siano A, B, C ideali di un anello R tali che A è generato da $\{\, a_1, \ldots, a_k \,\}$ e $AB = AC$. Allora, dato $b \in B^k$ esiste $c_b \in C$ tale che $ab = ac_b$ per ogni $a \in A$.*

Dimostrazione. Per la tesi è sufficiente provare il seguente asserto: se v è un generico generatore di B^k, ossia $v = b_1 \cdots b_k$ con $b_i \in B$ per ogni i, allora

esiste $c_v \in C$ tale che $a_i v = a_i c_v$ per ogni $i = 0, \ldots, k$. Questo sarà il nostro obiettivo. Per ipotesi, vale $BA = \sum_{j=1}^{k} Ba_j = CA = \sum_{j=1}^{k} Ca_j$. Quindi, per ogni $i = 0, \ldots, k$, $b_i a_i = \sum_{j=1}^{k} c_{ij} a_j$, per qualche $c_{ij} \in C$. Abbiamo ottenuto il sistema omogeneo

$$\sum_{j=1}^{k} (\delta_{ij} b_i - c_{ij}) a_j = 0$$

di k equazioni, lineare in $a_1, \ldots, a_k$, a coefficienti in R. Indichiamo con M la matrice dei coefficienti del sistema, con $\bar{a}$ il vettore dei generatori di A e con $\bar{0}$ il vettore nullo lungo k. Allora il sistema si scrive in forma compatta come $M\bar{a} = \bar{0}$. Moltiplichiamo ambo i membri per M^c, la matrice dei complementi algebrici di M, giungendo a $M^c M\bar{a} = M^c\bar{0} = \bar{0}$, cioè $(\det M)(\mathbb{1}_k)\bar{a} = \bar{0}$ (si noti che l'uso di 1 serve solo per semplificare la notazione). Perciò, abbiamo che $\det M a_i = 0$ per ogni $i = 0, \ldots, k$. Inoltre, un calcolo mostra che $\det M = v - c_v$ per qualche $c_v \in C$. Di conseguenza $a_i v = a_i c_v$. □

Corollario 3.5. *Siano A e B ideali di un anello R tali che A è finitamente generato e $AB = A$. Allora esiste $b \in B$ tale che $ab = a$ per ogni $a \in A$.*

Dimostrazione. Sia S un'estensione minimale di R con identità e (almeno una tale estensione esiste sempre, per esempio l'estensione di Dorroh). In virtù del Teorema 3.3 le ipotesi date valgono anche in S. Poiché S è unitario, vale $A = AS$. Quindi abbiamo $AB = AS$. Supponiamo che A sia generato da k elementi in S. Allora, per il Teorema 3.4, preso $e \in S^k$ esiste $b \in B$ tale che $ab = ae = a$, per ogni $a \in A$. □

Corollario 3.6. *Se R è un anello idempotente e finitamente generato, allora ha identità.*

Dimostrazione. Per ipotesi $RR = R$, quindi per il Corollario 3.5 esiste $e \in R$ tale che $re = r$ per ogni $r \in R$, ovvero e è identità di R. □

Corollario 3.7. *Sia R un anello. Se B è un ideale di R finitamente generato e idempotente, allora B è principale ed è generato da un elemento idempotente.*

Dimostrazione. Per ipotesi $BB = B$, dunque per il Corollario 3.5 esiste $b \in B$ tale che $xb = x$ per ogni $x \in B$. Per cui $B = \langle b \rangle$ e $bb = b$. □

Corollario 3.8. *Sia $\{ x_1, \ldots, x_n, y_1, \ldots, y_n \}$ una collezione di elementi di un anello R tale che $x_i y_i = x_i$ per ogni i. Allora esiste $y \in R$ tale che $x_i y = x_i$ per ogni i.*

Dimostrazione. Siano A e B gli ideali di R generati rispettivamente da $\{ x_1, \ldots, x_n \}$ e da $\{ y_1, \ldots, y_n \}$. Risulta che $AB = A$: infatti, i generatori ab di AB appartengono ad A, mentre per ipotesi i generatori x_i di A appartengono ad AB. Per il Corollario 3.5 esiste $y \in B$ tale che $x_i y = x_i$ per ogni i. □

Osserviamo che l'enunciato del Corollario 3.7 generalizza quello della Proposizione 1.24, ma la dimostrazione, questa volta, è sicuramente più immediata, grazie al bagaglio di conoscenze acquisito nel frattempo. Parimenti, il Corollario 3.6 può semplificare ulteriormente la dimostrazione della Proposizione 1.16.

Le proposizioni che seguono forniscono una formulazione equivalente per alcune delle undici proprietà: si tratta di *D*, *E*, *H* e *J*. Tali proposizioni facilitano alcune dimostrazioni delle implicazioni del diagramma; al contempo, procurano un differente punto di vista su un anello che possiede qualcuna di queste proprietà.

Proposizione 3.9. D *è equivalente a ciascuna delle seguenti condizioni:*
***D'**: Per ogni $x \in R$ si ha $\langle x \rangle = Rx$.*
***D''**: Per ogni ideale A di R si ha $RA = A$.*
***D'''**: Se $\{ x_1, \ldots, x_n \}$ è un insieme finito di elementi di R, allora esiste $y \in R$ tale che $x_i y = x_i$ per ogni i.*
***D''''**: Se A e B sono ideali comassimali di R, allora $A \cap B = AB$.*

Dimostrazione. *D'*⇒*D*: Sia $x \in R$. Per ipotesi $x \in Rx$, quindi esiste $y \in R$ tale che $x = xy$.
D⇒*D''*: Per ipotesi esistono $y_i \in R$ tali che $x_i y_i = x_i$ per ogni i. La tesi si ottiene applicando il Corollario 3.8.
D''⇒*D''*: Dimostriamo che vale $A \subseteq RA$ (essendo il viceversa sempre vero). Sia $a \in A$ e utilizziamo l'ipotesi sull'insieme $\{ a \}$, per cui esiste $y \in R$ tale che $a = ya$, quindi $a \in RA$.
D''⇒*D'''*: Abbiamo già visto che vale sempre $AB \subseteq A \cap B$. Dedichiamoci all'inclusione inversa. Per ipotesi, vale $A \cap B = R(A \cap B) = (A + B)(A \cap B)$. Ora usiamo il fatto che il prodotto tra ideali distribuisce rispetto alla loro somma. Dunque $A \cap B = A(A \cap B) + B(A \cap B)$. Infine, poiché $A \cap B$ è incluso sia in A che in B, allora $A(A \cap B) \subseteq AB$ e $B(A \cap B) \subseteq AB$. Pertanto, $A \cap B \subseteq AB$.
D'''⇒*D'*: Sia $x \in R$. Gli ideali $\langle x \rangle$ ed R sono comassimali. Utilizzando l'ipotesi otteniamo $\langle x \rangle = \langle x \rangle \cap R = R \langle x \rangle = Rx$. □

Proposizione 3.10. *E è equivalente ad E':*
***E'**: Ogni ideale proprio di R è contenuto in un ideale primo.*

Per la dimostrazione di questa proposizione sono necessari un paio di lemmi, tratti nell'ordine da [10, p. 827] e da [10, p. 826], ed una proposizione.

Lemma 3.11. *Sia R un anello e sia A un suo ideale. Allora A e $\sqrt{A}$ sono contenuti in esattamente gli stessi ideali primi.*

Dimostrazione. Se esiste P ideale primo di R tale che $\sqrt{A} \subseteq P$, allora, poiché $A \subseteq \sqrt{A}$, otteniamo che $A \subseteq P$. D'altro canto, se esiste P ideale primo di R tale che $A \subseteq P$, dobbiamo provare che $\sqrt{A} \subseteq P$. Sia $x \in \sqrt{A}$. Allora esiste $n \in \mathbb{N}$ $n \geq 1$ tale che $x^n \in A$. Siccome $A \subseteq P$, ne consegue che $x^n \in P$, dunque $x \in P$ perché P è primo. □

Lemma 3.12. *Sia R un anello e siano $P, B \trianglelefteq R$ con P primo. Se $P \cap B \neq B$, cioè $B \nsubseteq P$, allora $P \cap B$ è un ideale primo di B.*

Dimostrazione. L'insieme $P \cap B$ è un ideale di B, per ipotesi un ideale proprio. Siano $x, y \in B$ tali che $xy \in P \cap B$. Quindi, giacché P è primo, x o $y \in P$. Inoltre, entrambi gli elementi appartengono per ipotesi a B. Perciò, x o $y \in P \cap B$. □

Proposizione 3.13. *Sia R un anello con identità e sia I ideale proprio di R. Allora $\sqrt{I}$ è l'intersezione degli ideali primi che contengono I.*

Posponiamo la dimostrazione di questa proposizione, assieme ad alcune considerazioni, a quella della Prop. 3.10.

Dimostrazione della Prop. 3.10. *E'⇒E*: Sia A un ideale proprio di R. Dunque, per *E'*, esiste P ideale primo tale che $A \subseteq P$. Per il Lemma 3.11, $\sqrt{A} \subseteq P$. Di conseguenza, $\sqrt{A}$ è proprio.
E⇒E': Sia $A \trianglelefteq R$ con $A \neq R$. Per E abbiamo che $\sqrt{A}_R \neq R$, dove $\sqrt{A}_R$ è il radicale di A in R. Sia ora S un'estensione minimale di R. Per il Teorema 3.3, $A, R \trianglelefteq S$. Essendo poi $A \neq S$, per E vale $\sqrt{A}_S \neq S$, dove $\sqrt{A}_S$ è il radicale di A in S. Naturalmente, $\sqrt{A}_R \subseteq \sqrt{A}_S$. Affermiamo che in S esiste un ideale primo P tale che $A \subseteq P$ ed $R \nsubseteq P$. Infatti, A è contenuto in qualche ideale massimale di S, perché S ha identità, e, per lo stesso motivo, quest'ideale massimale è primo. Se per assurdo R fosse incluso in tutti gli ideali primi di S contenenti A, allora, per la Prop 3.13, R sarebbe sottoinsieme anche della loro intersezione, cioè di $\sqrt{A}_S$, pertanto, si avrebbe $R = \sqrt{A}_R$: assurdo per ipotesi. A questo punto, in S vi sono gli ideali R e P tali che P è primo e $P \cap R \neq R$: per il Lemma 3.12 otteniamo che $P \cap R$ è ideale primo di R. Infine, da $A \subseteq R$ e $A \subseteq P$, segue che $A \subseteq R \cap P$. □

Dimostrazione della Prop. 3.13. ($\subseteq$) Innanzitutto, in R c'è qualche ideale primo che contiene I. Infatti, I è proprio, quindi esiste un ideale massimale di R che lo contiene. In più, tutti gli ideali massimali di R sono primi. Ora, presi tutti i primi P contenenti I, per il Lemma 3.11 questi contengono anche $\sqrt{I}$, ossia la loro intersezione contiene I.
($\supseteq$) Sia $r \in R \setminus \sqrt{I}$. Tale r esiste poiché per ipotesi I è proprio, per cui anche $\sqrt{I}$ lo è. Sia $S := \{ r^n \mid n \in \mathbb{N} \}$. Quest'insieme è moltiplicativamente chiuso ed è disgiunto da I, cioè $I \cap S = \emptyset$. Sia Ω l'insieme di tutti gli ideali di R che contengono I e sono disgiunti da S. Allora $(\Omega, \subseteq)$ è un insieme parzialmente ordinato ed è non vuoto, giacché I vi appartiene. Sia $C := \{ J_\lambda \}_{\lambda \in \Lambda}$ una catena non vuota di Ω. Risulta che $\bigcup J_\lambda$ è un ideale di R, $I \subseteq \bigcup J_\lambda$, $(\bigcup J_\lambda) \bigcap S = \emptyset$, $J_\lambda \subseteq \bigcup J_\lambda$ per ogni λ: perciò, $\bigcup J_\lambda$ è un maggiorante di C. Quindi, in base al Lemma di Zorn, Ω ha un elemento massimale. Sia esso J. Proviamo che J è primo, essenzialmente come in [8, pp. 1–2]. Per iniziare, J è proprio, essendo disgiunto da S che è non vuoto. Siano poi $a, b \in R \setminus J$. Allora gli ideali $J + \langle a \rangle$ e $J + \langle b \rangle$ non appartengono ad Ω, per non contraddire la massimalità di J. Siccome entrambi contengono I, devono necessariamente intersecare S. Siano tali intersezioni, rispettivamente, $s_1 = j_1 + xa$ e $s_2 = j_2 + yb$, con $j_1, j_2 \in J$, $x, y \in R$. Moltiplicando s_1 con s_2 troviamo $s_1 s_2 = j_1 j_2 + j_1 yb + j_2 xa + xyab \in S$. Notiamo che i primi tre termini del prodotto appartengono a J. Se per assurdo $ab \in J$ allora avremmo $s_1 s_2 \in J \cap S = \emptyset$, assurdo. Di conseguenza, $ab \notin J$, ovvero J è primo. Infine, $r \in S$, ma allora $r \notin J$. Per questo, r non appartiene all'intersezione degli ideali primi contenenti I. □

Analizziamo adesso, in dettaglio, la dimostrazione appena proposta. Notiamo che la presenza dell'identità non è, in realtà, del tutto necessaria. È sufficiente, per esempio, che R sia uno u-ring, come evidenziano i primi passi di entrambe le inclusioni (ora sappiamo che $E \Leftrightarrow E'$). Naturalmente, se utilizziamo quest'ipotesi più debole sull'anello, dobbiamo specificare nella definizione dell'insieme S che $n \geq 1$. Così come dobbiamo modificare la scrittura degli elementi s_1 e s_2, per rispettare la definizione di 'ideale generato' data nel Capitolo 1. Tuttavia, il risultato non ne risente. Come conseguenza di questa prima nota, rileviamo che una seconda prova di $E \Rightarrow E'$ è contenuta nella dimostrazione in analisi, in particolare all'interno della seconda inclusione. Riassumiamo il risultato chiave da utilizzare, tratto da [8, p. 2], nella seguente proposizione.

Proposizione 3.14. *Sia R un anello. Siano I ideale proprio di R ed S sottoin-*

sieme moltiplicativamente chiuso non vuoto di R tale che $I \cap S = \emptyset$. Allora esiste un ideale J massimale rispetto a $J \cap S = \emptyset$ e a $J \supseteq I$. Inoltre J è primo. □

Proposizione 3.15. *H è equivalente ad H':*
***H'**: Se Q è un ideale primario non nullo tale che $\sqrt{Q} \neq R$, allora R/Q ha identità.*

Anche stavolta, prima della dimostrazione, vediamo alcuni lemmi, il secondo dei quali proviene da [5, p. 75].

Lemma 3.16. *Sia R un anello e sia Q ideale primario di R tale che $\sqrt{Q} \neq R$. Allora $\sqrt{Q}$ è primo.*

Dimostrazione. L'ideale $\sqrt{Q}$ è proprio per ipotesi. Poi, siano $x, y \in R$ tali che $xy \in \sqrt{Q}$, cioè esiste $n \in \mathbb{N}$ tale che $(xy)^n = x^n y^n \in Q$. Sia $x \notin \sqrt{Q}$, ossia $x^m \notin Q$ per ogni $m \in \mathbb{N}$. Ma allora, siccome Q è primario, $y^n \in \sqrt{Q}$, ovvero esiste $t \in \mathbb{N}$ tale che $(y^n)^t = y^{nt} \in Q$. Quindi $y \in \sqrt{Q}$. □

Lemma 3.17. *Sia R un anello e sia P ideale primo di R tale che R/P ha identità. Se Q è un ideale di R primario per P (ossia Q è primario e $\sqrt{Q} = P$), allora R/Q ha identità.*

Dimostrazione. Sia $t + P$ identità di R/P, cioè, per ogni $x + P \in R/P$, vale $tx + P = (t + P)(x + P) = x + P$, ovvero $tx - x \in P$. Sia $z \notin P$ un fissato elemento di R. Poiché $P = \sqrt{Q}$, esiste un intero dispari k tale che $(tz - z)^k \in Q$. Se ora x è un generico elemento di R, si ha che $(tz-z)^k x = (ux-x)z^k \in Q$, dove $u \in R$ è indipendente da x. Giacché Q è primario e $z^k \notin \sqrt{Q}$, allora $ux - x \in Q$ per ogni $x \in R$. Quindi, in base a quanto visto inizialmente, $u + Q$ è identità di R/Q. □

Dimostrazione della Prop 3.15. *H⇒H'*: Sia $Q \neq 0$ ideale primario di R tale che $\sqrt{Q} \neq R$. Per il Lemma 3.16, $\sqrt{Q}$ è primo. Applicando H a $\sqrt{Q}$ otteniamo che $R/\sqrt{Q}$ ha identità. Per il Lemma 3.17, R/Q ha identità.
H'⇒H: Sia $P \neq 0$ ideale primo di R. Quindi P è primario e $\sqrt{P} = P$. In particolare, $\sqrt{P} \neq R$. Ma allora, per H', R/P ha identità. □

Proposizione 3.18. *J è equivalente a J':*
***J'**: Se A è ideale di R tale che $\sqrt{A}$ è massimale, allora R/A ha identità.*

L'equivalenza appena descritta è giustificata dal seguente lemma. Esso caratterizza quando, nella situazione ipotizzata da J, l'ideale A è primario.

Lemma 3.19. *Sia R un anello e sia $A \trianglelefteq R$ tale che $\sqrt{A}$ è massimale. Allora A è primario se e solo se R/A ha identità.*

Dimostrazione. $\Rightarrow$) Sia A primario. Allora abbiamo che $\sqrt{A}$ è sia massimale (per ipotesi) sia primo (per il Lemma 3.16). Ma allora, in virtù della Prop. 1.17, $R/\sqrt{A}$ è un campo. Per il Lemma 3.17, R/A ha identità.
$\Leftarrow$) Sia R/A anello con identità. Consideriamo l'omomorfismo d'anelli canonico che proietta R sul quoziente R/A. Applicando ad esso il teorema di corrispondenza per anelli, l'ideale $\sqrt{A}/A = \sqrt{A/A}$ è massimale in R/A. Dunque, poiché R/A ha identità, A/A è primario. Utilizzando di nuovo il teorema di corrispondenza sopracitato, A è primario. □

Procediamo ora col dimostrare in blocco quasi tutte le implicazioni del diagramma, tenendo presente che '$A \Rightarrow B$' e '$A \Rightarrow C$' sono già state viste. Tratteremo a parte, invece, '$E \Rightarrow J$', che necessita di un percorso più articolato.

C*⇒*H Immediata ricordando che il radicale di un ideale primo è l'ideale stesso.

E*⇒*F Per assurdo sia $RR \neq R$. Ma allora, utilizzando E, abbiamo $R = \sqrt{RR} \neq R$, assurdo. Quindi R è idempotente.

F*⇒*G Immediata per la Prop. 1.13.

B*⇒*D Sia $r \in R$. Per B, vale $r = r_1e_1 + \cdots + r_ne_n + z_1e_1 + \cdots + z_ne_n$, dove, per ogni $i = 1 \ldots n$, $r_i \in R$, $e_i \in R$ idempotenti, $z_i \in \mathbb{Z}$. Usiamo il Corollario 3.8 sugli elementi $e_1, \ldots, e_n$, ottenendo che esiste $y \in R$ tale che $e_iy = e_i$ per ogni i. Sostituiamo queste identità nella precedente: $r = r_1e_1y + \cdots + r_ne_ny + z_1e_1y + \cdots + z_ne_ny = y(r_1e_1 + \cdots + r_ne_n + z_1e_1 + \cdots + z_ne_n) = yr$.

D*⇒*L Immediata in base alla Prop. 3.9.

D*⇒*E Sia A ideale proprio di R. Allora esiste $x \in R \setminus A$. Per D, esiste $y \in R$ tale che $x = xy$. Dunque, $x = xy^n$ per ogni $n \in \mathbb{N}$. Di conseguenza, $y^n \notin A$ (altrimenti $x \in A$), ossia $y \in R \setminus \sqrt{A}$.

D*⇒*H Per la dimostrazione abbiamo bisogno della seguente proposizione.

Proposizione 3.20. *Se R è un anello senza divisori dello zero in cui vale D, allora R ha identità.*

Dimostrazione. Sia $0 \neq x \in R$. Associamo ad x la funzione $f\colon R \to R$ definita da $f(r) := xr$, per ogni $r \in R$. Poiché per ipotesi x non è un

divisore dello zero, f risulta essere iniettiva. Per D, esiste $y \in R$ tale che $x = xy$. Quindi, per ogni $r \in R$, abbiamo che $f(r) = xyr = f(yr)$. Dunque, per l'iniettività di f, vale $r = yr$ per ogni $r \in R$, cioè y è identità di R. (Da notare che è sufficiente che R abbia un solo elemento x che non divide lo zero e tale che $x = xy$ per qualche y in R). □

Sia $0 \neq P$ ideale primo di R primo, pertanto R/P non ha divisori dello zero. La proprietà D, vera per ipotesi su R, viene ereditata da R/P. La Prop. 3.20, applicata a R/P, porta alla tesi.

D*⇒*K Sia $W \neq 0$ ideale di R. Allora esiste un ideale primo P tale che $W \subseteq P$, perché $D \Rightarrow E \Leftrightarrow E'$. Ma D implica anche H, quindi R/P ha identità. Dunque, l'ideale P/P è contenuto in un ideale massimale M/P di R/P. Perciò, $W \subseteq P \subseteq M$, con M ideale massimale di R. Sia ora $W = 0$. Come sopra, vale E'. Se esiste un primo $P \neq 0$ tale che $W \subseteq P$, allora ci conclude allo stesso modo. Altrimenti, 0 è l'unico primo. Di conseguenza, in base a E, 0 è anche l'unico ideale proprio, quindi è massimale. (Osserviamo che, invero, abbiamo dimostrato che $E+H \Rightarrow K$)

Vediamo ora la dimostrazione dell'ultima implicazione rimasta, preceduta da alcuni risultati preparatori.

Lemma 3.21. *Sia V un ideale proprio di un anello R. Sia P un ideale minimale primo di V tale che R/P ha identità. Se $W := \{ x \in R \mid tx - x \in V, \text{esiste } t \in R \}$, allora W è un ideale di R e $V \subseteq W \nsubseteq P$.*

Dimostrazione. Proviamo, per prima cosa, che W è ideale di R. W non è vuoto perché 0 gli appartiene. Poi, siano $x_1, x_2 \in W$, cioè esistono $e_1, e_2 \in R$ tali che $e_1x_1 - x_1 \in V$ ed $e_2x_2 - x_2 \in V$. Consideriamo l'elemento $t := e_1 + e_2 - e_1e_2$. Allora, $tx_1 - x_1 = (e_1 + e_2 - e_1e_2)x_1 - x_1 = (e_1x_1 - x_1) - e_2(e_1x_1 - x_1) \in V$. Parimenti, $tx_2 - x_2 \in V$. Quindi, $t(x_1 - x_2) - (x_1 - x_2) \in V$, ossia $x_1 - x_2 \in W$. Inoltre, se $r \in R$, allora $e_1rx_1 - rx_1 = r(e_1x_1 - x_1) \in V$, dunque $rx_1 \in W$. Pertanto, $W \trianglelefteq R$. Certamente, $V \subseteq W$. Notiamo che, fino a questo punto, non abbiamo utilizzato né le ipotesi su P, né il fatto che V è proprio. Localizziamo ora l'anello R all'ideale primo P, ottenendo l'anello R_P. Questo è un anello unitario: infatti l'identità è s/s, con s un elemento qualsiasi di $R \setminus P$. Esiste un omomorfismo d'anelli canonico $f\colon R \to R_P$ definito da $f(r) := (rs)/s$, per ogni $r \in R$ e con s elemento qualunque di $R \setminus P$. Risulta che R_P è un anello

locale, il cui unico ideale massimale è P^e, l'estensione di P ad R_P. Indichiamo con Q la contrazione di V^e a R, quindi $Q = \{ r \in R \mid sr \in V, \text{esiste } s \in R \setminus P \}$. Ma allora, in R, la situazione è la seguente: $V \subseteq Q \subseteq \sqrt{Q} \subseteq P$, dove per inserire $\sqrt{Q}$ abbiamo usato il Lemma 3.11. Nell'anello R_P l'unico ideale primo contenente V^e è il massimale P^e: altrimenti, contraendo ad R, contraddiremmo l'ipotesi sulla minimalità di P come ideale primo contenente V. Dunque, per la Prop. 3.13, $\sqrt{V^e} = P^e$. Poiché R_P ha identità, vale J, perciò V^e è primario. Pertanto, essendo Q proprio, anche Q è primario. Per il Lemma 3.16, $\sqrt{Q}$ è primo. Quindi, per evitare la contraddizione sopracitata, $\sqrt{Q} = P$. In base al Lemma 3.17, R/Q ha identità. Sia essa $s + Q$. Se $y \in R$, allora $sy - y \in Q$. Di conseguenza, esiste $v_y \in R \setminus P$ tale che $(sy - y)v_y = s(yv_y) - (yv_y) \in V$. Per cui $yv_y \in W$. In particolare, se $y \notin P$, allora $yv_y \in W \setminus P$. □

Proposizione 3.22. ***D*⇔*E*+*H*.**

Dimostrazione. Dobbiamo provare solamente che se R è uno u-ring in cui vale H, allora vale anche D. Giacché $E \Rightarrow F$, abbiamo che $R = R^2 \neq 0$. Dunque, esiste $x \in R$ tale che $Rx \neq 0$. Sia $W_1 := \{ y \in R \mid yt - y \in Rx, \text{esiste } t \in R \}$ e sia $W_2 := \{ z \in R \mid zs - z \in W_1, \text{esiste } s \in R \}$. Per il lemma 3.21, W_1 e W_2 sono ideali di R tali che $W_1 \subseteq W_2$. Vale anche l'inclusione inversa. Infatti, sia $z \in W_2$, ovvero $zs - z \in W_1$, con $s \in R$. Quindi, per qualche $t \in R$, $(zs - z)t - (zs - z) = (st - t - s)z + z \in Rx$, pertanto $z \in W_1$. Finora abbiamo provato che $0 \neq Rx \subseteq W_1 = W_2$. Per assurdo, sia $W_1 \neq R$. Per E, esiste un primo P tale che $W_1 \subseteq P$. Per il Lemma di Zorn, esiste P' ideale minimale primo di W_1. Per H, R/P' ha identità. Applicando il Lemma 3.21, otteniamo che $W_1 = W_2 \nsubseteq P'$: assurdo perché $W_1 \subseteq P'$. Perciò, $W_1 = R$. In particolare, $x \in W_1$, quindi esiste $t \in R$ tale che $tx - x \in Rx$, ma allora $x \in Rx$. Sia ora $V_1 := \{ v \in R \mid tv = v, \text{esiste } t \in R \}$. Per quanto appena visto, $0 \neq \langle x \rangle \subseteq V_1$. Sia $V_2 := \{ w \in R \mid sw - w \in V_1, \text{esiste } s \in R \}$. Ripetendo i ragionamenti precedenti, concludiamo che $V_1 = V_2 = R$, ovvero in R vale D. □

Proposizione 3.23. *Un ideale massimale M di un anello R è primo se e solo se $\sqrt{M} \neq R$.*

Dimostrazione. ⇒) Se M è primo allora $\sqrt{M} = M \neq R$. (Osserviamo che qui la massimalità di M è un'ipotesi sovrabbondante).
⇐) Se $\sqrt{M} \neq R$ allora, in base alla dimostrazione della Prop. 3.13, esiste

un ideale primo J che contiene M. Dunque $J = M$, per non contraddire la massimalità di M. Quindi M è primo. □

Corollario 3.24. *Sia A ideale di un anello R. Se $\sqrt{A}$ è massimale, allora è primo.*

Dimostrazione. È sufficiente ricordare che la radicalizzazione di un ideale è un operazione idempotente. □

E*⇒*J Sia A ideale di R tale che $\sqrt{A}$ è massimale. Siano $x, y \in R$ tali che $xy \in A$ e $y \notin \sqrt{A}$. Pertanto, $\sqrt{A} + \langle y \rangle = R$. Se $q \in R$, esistono $m \in \sqrt{A}$, $v \in R$, $\alpha \in \mathbb{Z}$ tali che $q = m + vy + \alpha y$. In particolare, esiste $t \in \mathbb{Z}$ tale che $m^t \in A$. Elevando q alla t otteniamo $q^t = m^t + v'y + \alpha' y$, con $v' \in R$ e $\alpha' \in \mathbb{Z}$. Moltiplichiamo ora per x la precedente identità: $xq^t = m^t x + v'xy + \alpha' xy \in A$. Abbiamo provato che $\sqrt{A : x} = R$. Ma per ipotesi R è uno u-ring, pertanto $A : x = R$, ossia $Rx \subseteq A$. La medesima ipotesi implica che anche R/A è uno u-ring. Inoltre, nell'anello R/A vale la proprietà H. Infatti, per il Corollario 3.24, $\sqrt{A}$ è primo, quindi $\sqrt{A}/A$ è primo in R/A. In virtù del terzo teorema d'omomorfismo per anelli, $(R/A)/(\sqrt{A}/A) \cong R/\sqrt{A}$ e quest'ultimo, per la Prop. 1.17, è un campo, dunque ha identità. Se poi P/A è un generico ideale primo di R/A, allora P è ideale primo di R e $A \subseteq P$. Per il Lemma 3.11, $\sqrt{A} \subseteq P$, per cui $P = \sqrt{A}$ per non contraddire la massimalità di $\sqrt{A}$. Perciò l'ideale $\sqrt{A}/A$ è l'unico primo di R/A. Ora, poiché R/A verifica sia E sia H, per la Prop. 3.22 vale anche D. Allora esiste $z+A \in R/A$ tale che $x+A = (x+A)(z+A) = xz+A$. Dunque $x - xz \in A$, ma sappiamo che $xz \in A$ perché $Rx \subseteq A$. Allora $x \in A$, cioè A è primario.

Concludiamo questo capitolo con una nota: l'articolo originale [4] di Gilmer contiene un piccolo errore, in quanto non è vero in generale che C⇒J. Ovvero, se un anello non nullo R ha la proprietà C e A è un ideale di R tale che $\sqrt{A}$ è massimale, allora non necessariamente A è primario. Certamente, come afferma lo stesso autore, è opportuno utilizzare il Lemma 3.19 per cercare di ottenere la tesi, cioè che A è primario. Tuttavia, la combinazione di questo lemma con la condizione C è possibile solo quando $A \neq 0$. Ciò conduce al seguente controesempio (considerazioni ausiliarie mostrano che se $0 = \sqrt{0}$ allora la tesi è vera, così come se R contiene almeno un non divisore dello zero non nullo).

Esempio 3.25. Sia $R := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}'$, dove con $\mathbb{Z}/2\mathbb{Z}'$ indichiamo l'anello abeliano che ha lo stesso gruppo additivo di $\mathbb{Z}/2\mathbb{Z}$. Allora R è un anello non nullo senza identità ($\mathbb{Z}/2\mathbb{Z}'$ non ha identità). R ha quattro elementi: $(\bar{0}, \bar{0})$, $(\bar{0}, \bar{1})$, $(\bar{1}, \bar{0})$ e $(\bar{1}, \bar{1})$. Il gruppo additivo di R è il gruppo di Klein, infatti i tre elementi non nulli di R hanno tutti ordine additivo 2. Quindi i sottogruppi di $(R, +)$ sono: 0, R e i tre sottogruppi ciclici di ordine 2 generati rispettivamente dai tre elementi sopramenzionati. Di questi sottogruppi, tutti sono ideali eccetto il sottogruppo $\langle(\bar{1}, \bar{1})\rangle$, poiché $(\bar{1}, \bar{1})(\bar{1}, \bar{1}) = (\bar{1}, \bar{0}) \notin \langle(\bar{1}, \bar{1})\rangle$. Complessivamente, gli ideali di R sono: 0, R, $P := \langle(\bar{0}, \bar{1})\rangle$ e $\langle(\bar{1}, \bar{0})\rangle = RR$. Gli ideali massimali sono P e RR. In base alla Prop. 1.13, P è primo e RR non lo è. L'ideale nullo non è primo, anzi, osserviamo che tutti gli elementi non nulli di R sono divisori dello zero. I radicali degli ideali propri sono: $\sqrt{P} = P$, $\sqrt{RR} = R$, $\sqrt{0} = P$ (vedi Prop. 5.4). Dunque, R ha la proprietà C, dato che R/P è un campo per la Prop. 1.17, per cui R/P ha identità. Invece, R non verifica la condizione J: il radicale di 0 è massimale ma 0, in virtù del Lemma 3.19, non è primario.

Capitolo 4

Noetherianità e anelli di polinomi

In questo capitolo ci occupiamo di anelli noetheriani. In particolare, mettiamo in luce qualche aspetto che lega questa proprietà con la presenza dell'identità in un anello. Iniziamo con la definizione di anello noetheriano.

Definizione 4.1. Un anello R si dice *noetheriano* se soddisfa una delle seguenti condizioni equivalenti:

1. ogni ideale di R è finitamente generato;
2. ogni catena ascendente di ideali di R è stazionaria (cioè se $I_1 \subseteq I_2 \subseteq \dots$ è una sequenza di ideali di R, allora esiste $n \in \mathbb{N}$ tale che $I_n = I_{n+1} = \dots$);
3. ogni famiglia di ideali di R non vuota e parzialmente ordinata dall'inclusione ammette almeno un elemento massimale.

Dimostrazione dell'equivalenza delle condizioni. 1⇒2) Sia $I_1 \subseteq I_2 \subseteq \dots$ una catena ascendente di ideali di R. Sia $I := \bigcup I_j$. Allora I è un ideale di R. Quindi, per ipotesi, è finitamente generato. Sia $\{ a_1, \dots, a_n \}$ un insieme di generatori di I. Dunque, per ogni a_i, esiste un ideale I_{a_i} della catena tale che $a_i \in I_{a_i}$. Sia I_{a_k} il più grande di tutti. Ma allora $a_i \in I_{a_k}$ per ogni i. Perciò $I \subseteq I_{a_k}$. Di conseguenza, $I_{a_k} = I$, ovvero la catena si stabilizza a partire da I_{a_k}. 2⇒3) Per assurdo, sia S un insieme non vuoto di ideali di R che non ammette elementi massimali (si intende, come ordine parziale, l'inclusione). Sia $I_1 \in S$. Poiché I_1, per ipotesi, non è massimale, esiste $I_2 \in S$ tale che $I_1 \subsetneq I_2$. Lo stesso

vale per I_2, per cui esiste $I_3 \in S$ tale che $I_1 \subsetneq I_2 \subsetneq I_3$. Iterando la procedura, riusciamo a costruire una catena di ideali di R strettamente ascendente: assurdo.
3⇒1) Sia I un ideale di R. Sia S l'insieme di tutti gli ideali finitamente generati di R contenuti in I. Allora S è non vuoto, perché contiene 0, ed è parzialmente ordinato dall'inclusione. Per ipotesi, S ha un elemento massimale. Sia esso J. Se per assurdo $J \neq I$, allora esiste $a \in I \setminus J$. L'ideale $\langle J, a\rangle$ è finitamente generato e contenuto in I: dunque è un elemento di S. Tuttavia $J \subsetneq \langle J, a\rangle$: assurdo per la massimalità di J. Perciò $J = I$, ovvero I è finitamente generato. □

Il seguente corollario, tratto da [4], è un'interessante conseguenza del Teorema 3.3.

Corollario 4.2. *Siano R ed S due anelli tali che S è estensione minimale di R. Allora R è noetheriano se e solo se S è noetheriano.*

Dimostrazione. ⇒) Sia A ideale di S. Per il punto a) del teorema, $A \cap R$ è un ideale di R. Quindi, per ipotesi, è finitamente generato in R. Per il punto b) del teorema, A è ideale finitamente generato di S.
⇐) Sia A ideale di R. Utilizzando nuovamente il punto a) del teorema, A è un ideale di S. Ma allora, per ipotesi, è finitamente generato come ideale di S. Di conseguenza, a maggior ragione, è un ideale finitamente generato di R. □

In base al corollario appena visto, possiamo affermare che tutte le estensioni incontrate nel Capitolo 2 preservano la noetherianità.

Riprendendo le notazioni del Capitolo 3, osserviamo che ogni anello noetheriano ha la proprietà K, ovvero ogni suo ideale proprio è contenuto in un ideale massimale. Vediamo ora un'altra proposizione di [4].

Proposizione 4.3. *Sia R un anello noetheriano che verifica G. Allora R ha identità.*

Dimostrazione. Sia W ideale proprio di R. Per quanto osservato poc'anzi, esiste un ideale massimale M che lo contiene. Poiché vale G, l'ideale M è primo. Quindi, R è uno u-ring, perché vale E'. Dunque vale anche F, cioè R è idempotente. Poi, per ipotesi, R è finitamente generato. Per il Corollario 3.6, R ha identità. □

Notiamo che la proposizione precedente vale anche nel caso più generale in cui R è finitamente generato.

Volgiamo ora l'attenzione agli anelli di polinomi. Per prima cosa, consideriamo il seguente teorema.

Teorema 4.4 (della base di Hilbert)**.** *Se R è anello con identità noetheriano, allora $R[X]$ è noetheriano.*

Dimostrazione. Per assurdo, sia $R[X]$ non noetheriano, ovvero esiste $I \trianglelefteq R[X]$ non finitamente generato. Costruiamo una successione di polinomi di $R[X]$ nel modo seguente:
- p_0 è un elemento di I di grado minimo (tra gli elementi di I),
- p_n è un elemento di $I \setminus \langle p_0, \dots, p_{n-1} \rangle$ di grado minimo (tra gli elementi di $I \setminus \langle p_0, \dots, p_{n-1} \rangle$).

Da notare che la costruzione è possibile poiché I non è finitamente generato. Inoltre, i gradi dei p_i sono non decrescenti. Siano a_i e d_i, rispettivamente, i coefficienti direttori e i gradi dei p_i. Sia J l'ideale di R generato dagli a_i. Per ipotesi, J è finitamente generato, ossia esiste $N \in \mathbb{N}$ tale che J è generato da $a_0, \dots, a_{N-1}$. Ma allora $a_N = \sum_{i=0}^{N-1} e_i a_i$, con $e_i \in R$. Consideriamo il polinomio $q := \sum_{i=0}^{N-1} e_i X^{d_N - d_i} p_i$. Per costruzione, $q \in \langle p_0, \dots, p_{N-1} \rangle$. Il grado di q è d_N, mentre il coefficiente direttore è a_N. Quindi il polinomio $q - p_N$, che appartiene a $I \setminus \langle p_0, \dots, p_{N-1} \rangle$, ha grado minore o uguale di d_{N-1}: assurdo per la minimalità di p_N. Perciò I è finitamente generato. □

Cerchiamo adesso di capire dove, nella dimostrazione appena data, abbiamo usato l'identità di R, per meglio comprendere quanto è necessaria. Per procedere, allora, supponiamo che R non abbia identità e ripercorriamo la dimostrazione. Il primo punto in cui dobbiamo apportare un cambiamento è dato dalla scrittura di a_N, che diviene, in accordo con la Definizione 1.7, $a_N = \sum_{i=0}^{N-1} e_i a_i + \sum_{j=0}^{N-1} z_j a_j$, con $e_i \in R$ e $z_j \in \mathbb{Z}$. Di conseguenza, proviamo a modificare anche il polinomio q, ottenendo $q := \sum_{i=0}^{N-1} e_i X^{d_N - d_i} p_i + \text{"} \sum_{j=0}^{N-1} z_j X^{d_N - d_i} p_j \text{"}$. Osserviamo che la sommatoria virgolettata, scritta in questi termini, non ha interpretazione in $R[X]$, proprio perché non abbiamo a disposizione l'identità. Ciò nonostante, il polinomio che stiamo cercando di indicare con tale notazione esiste in $R[X]$; però, non è necessariamente combinazione dei p_j. Per questo, non siamo poi in grado di concludere con l'assurdo. In effetti, non esiste modo di fare a meno dell'identità: lo stesso Gilmer, in [6], dimostra che vale il viceversa del Teorema della base di Hilbert. Questo riportiamo (utilizzando le notazioni del Capitolo 3), preceduto da un lemma e da un corollario.

Lemma 4.5. *Se R è un anello noetheriano e I è ideale di R, allora R/I è noetheriano.*

Dimostrazione. Immediata applicando il teorema di corrispondenza per anelli alla proiezione canonica di R su R/I. □

Corollario 4.6. *Se R ed S sono anelli, R è noetheriano ed $f\colon R \to S$ è omomorfismo d'anelli, allora $f(R)$ è noetheriano.*

Dimostrazione. Per il lemma, $R/\ker f$ è noetheriano. Per il primo teorema d'omomorfismo per anelli, $f(R) \cong R/\ker f$. Quindi $f(R)$ è noetheriano. □

Teorema 4.7. *Se R è un anello tale che $R[X]$ è noetheriano, allora R è noetheriano e ha identità.*

Dimostrazione. Sia $\varphi\colon R[X] \to R$ l'applicazione definita da $\varphi(g(X)) := g(0)$, per ogni $g(X) \in R[X]$. Essa risulta essere un omomorfismo suriettivo d'anelli. Per il Corollario 4.6, R è noetheriano. Resta da provare che R ha identità. Sia $r \in R$. Consideriamo in $R[X]$ la catena ascendente di ideali $\langle r\rangle \subseteq \langle r, rX\rangle \subseteq \langle r, rX, rX^2\rangle \subseteq \dots$. Per ipotesi, questa si stabilizza. Diciamo che ciò avviene dopo aver aggiunto l'elemento rX^n. Dunque, $rX^{n+1} \in \langle r, rX, \dots, rX^n\rangle$. Ovvero $rX^{n+1} = \sum_{i=0}^{n} f_i(X)\cdot rX^i + \sum_{i=0}^{n} n_i rX^i$, con $f_i \in R[X]$ e $n_i \in \mathbb{Z}$. In particolare, $f_i(X) = \sum_{j=0}^{m_i} f_j^{(i)} \cdot X^j$, con $f_j^{(i)} \in R$. Notiamo che nelle precedenti sommatorie stiamo commettendo un abuso di notazione: infatti, in assenza di identità le potenze con esponente 0 non sono definite. Ciò che intendiamo qui, per esempio, con rX^0, è r. Eguagliando i coefficienti di X^{n+1} nella penultima identità, otteniamo $r = \sum_{i=0}^{n} f_{n+1-i}^{(i)} \cdot r = gr$, con $g := \sum_{i=0}^{n} f_{n+1-i}^{(i)} \in R$. Abbiamo provato che in R vale D. Infine, per il Corollario 3.6, R ha identità. □

Dunque, in base al teorema, pur essendo $2\mathbb{Z}$ noetheriano, $2\mathbb{Z}[X]$ non lo è.

Capitolo 5

Esistenza di ideali primi e di ideali massimali

Nei capitoli precedenti abbiamo evidenziato che un anello non unitario non ha necessariamente ideali primi e ideali massimali. Lo scopo di questo capitolo è fare più luce su questo tema. Per facilitarne la trattazione, introduciamo due definizioni.

Definizione 5.1. Sia R un anello. L'ideale $\sqrt{0}$ è detto *nilradicale* di R e viene anche indicato con $\mathscr{N}(R)$. Esso consiste esattamente di tutti gli elementi nilpotenti di R. □

Definizione 5.2. Sia R un anello. Un ideale I di R è detto *nil ideal* se ogni suo elemento è nilpotente. Ovvero I è un nil ideal se e solo se $I \subseteq \mathscr{N}(R)$. Se l'anello R è un nil ideal, cioè $R = \mathscr{N}(R)$, allora viene detto *nil ring*. □

Come già osservato per gli anelli abeliani, i nil rings possono occorrere se non diamo per scontata la presenza dell'identità in un anello. Infatti, ogni nil ring non nullo non ha identità. Inoltre, se un anello è abeliano allora è un nil ring.

Vediamo adesso una proposizione, tratta da [9, p. 14], che caratterizza l'assenza di ideali primi in un anello.

Proposizione 5.3. *Un anello R non ha ideali primi se e solo se $\mathscr{N}(R) = R$.*

Dimostrazione. Se $R = 0$ l'enunciato è immediatamente verificato. Sia ora $R \neq 0$.
⇐) Se R è un nil ring allora non può avere alcun ideale primo P, altrimenti si

avrebbe $\mathscr{N}(R) \subseteq P$, contro il fatto che P è proprio. Infatti se $0 \neq x \in \mathscr{N}(R)$, allora esiste $n \in \mathbb{N}$ $n \geq 1$ tale che $x^n = 0$. Quindi $0 = x^n \in P$, per cui $x \in P$.
$\Rightarrow$) Se $\mathscr{N}(R) \neq R$, allora i ragionamenti contenuti nella dimostrazione della Prop. 3.13 (commentata) fanno vedere che R ha almeno un ideale primo J. □

Questa proposizione trova conferma, oltre che nelle note ricordate sugli anelli abeliani, anche nell'Esempio 1.11. In esso l'anello $2\mathbb{Z}/8\mathbb{Z}$, pur non essendo abeliano, non ha ideali primi. Infatti i suoi elementi sono tutti nilpotenti: $\bar{2}^3 = \bar{4}^2 = \bar{6}^3 = \bar{0}$.

La prossima proposizione completa il quadro sugli ideali primi.

Proposizione 5.4. *Sia R un anello. Allora $\mathscr{N}(R)$ è l'intersezione degli ideali primi di R.*

Dimostrazione. È sufficiente utilizzare la Prop. 5.3 e lo schema della dimostrazione della Prop. 3.13. □

Volgiamo ora l'attenzione agli ideali massimali. Seguiremo abbastanza fedelmente il materiale contenuto in [7]. Anche questa volta partiamo da una definizione.

Definizione 5.5. Sia R un anello. Il *radicale di Jacobson* di R, denotato con $\mathscr{J}(R)$, è l'intersezione degli ideali di R che sono sia massimali sia primi, se questi esistono. Altrimenti si pone $\mathscr{J}(R) = R$ e in tal caso R è detto *radical ring.*

Osserviamo che un radical ring non nullo non ha identità. Inoltre, ogni nil ring è un radical ring. Più in generale, se R è un anello, vale $\mathscr{N}(R) \subseteq \mathscr{J}(R)$.

La proposizione che segue caratterizza l'assenza di ideali massimali in un anello. Per abbreviare la notazione, indicheremo con $\mathbb{Z}/p\mathbb{Z}'$ l'anello abeliano che ha come gruppo additivo lo stesso di $\mathbb{Z}/p\mathbb{Z}$.

Proposizione 5.6. *Un anello R non ha ideali massimali se e solo se valgono entrambe le seguenti condizioni:*
a) R è un radical ring;
b) $R^2 + pR = R$ per ogni primo p.

Dimostrazione. $\Leftarrow$) Dobbiamo provare che R non ha ideali massimali. Poiché a) è soddisfatta, R non ha ideali che sono sia massimali sia primi. Per assurdo sia M ideale massimale non primo di R. Quindi esiste ψ isomorfismo di R/M in $\mathbb{Z}/p\mathbb{Z}'$

per qualche primo p. Sia π la proiezione canonica di R su R/M. Chiamiamo φ la composizione di ψ dopo π. Dunque φ è omomorfismo suriettivo d'anelli e ha nucleo M. Per ogni $a, b \in R$ si ha che $\varphi(ab) = \varphi(a)\varphi(b) = 0$, perciò $R^2 \subseteq M$. Analogamente, per ogni $a \in R$ vale $\varphi(pa) = p\varphi(a) = 0$, per cui $pR \subseteq M$. Ma allora, utilizzando b), abbiamo che $R = R^2 + pR \subseteq M$, assurdo perché M è proprio. Di conseguenza R non ha nemmeno ideali massimali non primi. Perciò R non ha ideali massimali.
$\Rightarrow$) Per ipotesi R non ha ideali massimali, pertanto non ha ideali che sono sia massimali sia primi, ossia è un radical ring. Per assurdo b) non vale, ovvero esiste un primo p tale che $I := R^2 + pR \neq R$. Sia π la proiezione canonica di R su R/I. Sappiamo che è suriettiva e che ha nucleo I. Il quoziente R/I è abeliano. Infatti, se $x, y \in R/I$, cioè esistono $a, b \in R$ tali che $x = \pi(a)$ e $y = \pi(b)$, allora $xy = \pi(a)\pi(b) = \pi(ab)$. Ma $ab \in R^2 \subseteq I = \ker \pi$, quindi $xy = \pi(ab) = 0$. Poi R/I ha caratteristica p. Infatti, se $x \in R/I$, con $a \in R$ tale che $x = \pi(a)$, allora $px = p\pi(a) = \pi(pa)$. Ma, come in precedenza, $pa \in pR \subseteq I$, per cui $px = \pi(pa) = 0$. Perciò R/I è spazio vettoriale sul campo $\mathbb{Z}/p\mathbb{Z}$. Poiché $I \neq R$ abbiamo che $R/I \neq 0$. Dunque, per il teorema di struttura degli spazi vettoriali, R/I ha una base. Sia $\{ x_\lambda \}_{\lambda \in \Lambda}$ una base di R/I. Ogni elemento di R/I si scrive in modo unico come combinazione lineare finita di elementi della base. Fissiamo $\lambda_0 \in \Lambda$. Sia $\psi_0 \colon R/I \to \mathbb{Z}/p\mathbb{Z}'$ l'applicazione che mappa ogni elemento di R/I nella sua coordinata rispetto a x_0. Risulta che ψ_0 è omomorfismo d'anelli suriettivo. La composizione $\psi_0 \circ \pi$ è omomorfismo suriettivo di R in $\mathbb{Z}/p\mathbb{Z}'$. Quindi, per il primo teorema d'omomorfismo per anelli, $R/\ker(\psi_0 \circ \pi) \cong \mathbb{Z}/p\mathbb{Z}'$. Ma allora $\ker(\psi_0 \circ \pi)$ è ideale massimale di R: assurdo. □

Abbiamo già visto un esempio di anello che non ha ideali massimali: un anello R abeliano il cui gruppo additivo non ha sottogruppi massimali. Confrontando la descrizione di questo anello con la caratterizzazione della Prop. 5.6, deduciamo che deve essere $pR = R$ per ogni primo p. Questo passo conduce alle prossime definizioni.

Definizione 5.7. Sia G un gruppo abeliano e sia p un primo. Allora G è detto *p-divisibile* se $pG = G$. □

Definizione 5.8. Un gruppo abeliano G è detto *divisibile* se $nG = G$ per ogni $n \in \mathbb{N}$ $n \geq 1$. □

La proposizione che segue fornisce una prima caratterizzazione dei gruppi abeliani divisibili. La dimostrazione, immediata, fa uso del teorema fondamentale dell'aritmetica.

Proposizione 5.9. *Un gruppo abeliano è divisibile se e solo se è p-divisibile per ogni primo p.* □

Vediamo ora una seconda caratterizzazione.

Proposizione 5.10. *Sia G un gruppo abeliano. Le seguenti affermazioni sono equivalenti:*
1. G è divisibile;
2. G non ha sottogruppi massimali;
3. G non ha quozienti finiti non nulli.

Dimostrazione. 1⇒2) Per assurdo sia M sottogruppo massimale di G. Perciò $G/M \cong C_p$ per qualche primo p (con C_p intendiamo il gruppo ciclico di ordine p). Di conseguenza $pG \leq M$, ma per ipotesi $pG = G$, quindi $G \leq M$, assurdo.
2⇒3) Per assurdo sia $H \leq G$ tale che $G/H \neq 0$ è finito. Dunque G/H ha un sottogruppo massimale M/H. Ma allora, per il teorema di corrispondenza, M è sottogruppo massimale di G, assurdo.
3⇒1) Per assurdo sia G non divisibile, ossia esiste un primo p tale che $pG \neq G$. Il quoziente G/pG è non nullo e ha esponente p, infatti $p(G/pG) = (pG/pG) = 0$. Ma allora G/pG è spazio vettoriale sul campo $\mathbb{Z}/p\mathbb{Z}$. Sia $\{ x_\lambda \}_{\lambda \in \Lambda}$ base di G/pG. Fissiamo $\lambda_0 \in \Lambda$. Sia $\psi_0 \colon G/pG \to \mathbb{Z}/p\mathbb{Z}$ l'applicazione che mappa ogni elemento di G/pG nella sua coordinata rispetto a x_0. Risulta che ψ_0 è omomorfismo suriettivo di gruppi. Quindi, per il primo teorema d'omomorfismo per gruppi, $(G/pG)/\ker\psi_0 \cong \mathbb{Z}/p\mathbb{Z}$. Ma $\ker\psi_0 = H/pG$ con H un sottogruppo di G che contiene pG. Pertanto, in virtù del terzo teorema d'omomorfismo per gruppi, $G/H \cong (G/pG)/(H/pG) \cong \mathbb{Z}/p\mathbb{Z}$, ovvero G ha un quoziente finito non nullo, assurdo. □

A questo punto possiamo (ri)affermare che un anello abeliano il cui gruppo additivo è divisibile non ha ideali massimali. Invero, non tutti gli anelli privi di ideali massimali sono necessariamente abeliani o hanno divisori dello zero. Il prossimo esempio, preceduto da un paio di risultati utili, ne è la prova.

Proposizione 5.11. *Sia R un anello. Allora $\mathscr{J}(R)$ è un radical ring.*

Dimostrazione. Per assurdo sia M ideale massimale e primo di $\mathscr{J}(R)$, per cui, per la Prop. 1.17, $\mathscr{J}(R)/M$ è un campo. Sia 1 l'identità di $\mathscr{J}(R)/M$. Sia π la proiezione canonica di $\mathscr{J}(R)$ su $\mathscr{J}(R)/M$. Come ben sappiamo essa è suriettiva. Sia $e \in \mathscr{J}(R)$ tale che $\pi(e) = 1$. Sia $\varphi\colon R \to \mathscr{J}(R)/M$ applicazione definita da $\varphi(a) = \pi(ae)$ per ogni $a \in R$. Allora φ è omomorfismo d'anelli. Infatti, se $a, b \in R$, si ha che $\varphi(a+b) = \pi((a+b)e) = \pi(ae+be) = \pi(ae) + \pi(be) = \varphi(a) + \varphi(b)$; mentre $\varphi(ab) = \pi(abe) = \pi(abe) \cdot 1 = \pi(abe)\pi(e) = \pi(aebe) = \pi(ae)\pi(be) = \varphi(a)\varphi(b)$. Inoltre φ è suriettivo. Infatti, se $j + M \in \mathscr{J}(R)/M$, allora $\varphi(j) = \pi(je) = \pi(j)\pi(e) = (j+M) \cdot 1 = j + M$. Di conseguenza, per il primo teorema d'omomorfismo per anelli, $R/\ker\varphi \cong \mathscr{J}(R)/M$. Per cui $\ker\varphi$ è ideale massimale e primo di R. Quindi $\mathscr{J}(R) \subseteq \ker\varphi$. Però $e \in \mathscr{J}(R)$ e $\varphi(e) = 1$, assurdo. Dunque $\mathscr{J}(R)$ è un radical ring. □

Corollario 5.12 (della Prop. 5.6)**.** *Sia S un anello con identità che ha un unico ideale massimale R. Se $R^2 + pR = R$ per ogni primo p, allora R non ha ideali massimali. In particolare, se il gruppo additivo di S è divisibile, allora R non ha ideali massimali.*

Dimostrazione. Giacché per ipotesi S ha identità allora l'unico ideale massimale R è anche primo, perciò $\mathscr{J}(S) = R$. Per la Prop. 5.11, R è un radical ring. Se $R^2 + pR = R$ per ogni primo p, allora, in base alle Prop 5.6, R non ha ideali massimali. In particolare, se S ha gruppo additivo divisibile, allora ogni ideale I di S ha gruppo additivo divisibile. Infatti, sia X un insieme di generatori di I. L'insieme $S^{\{(X)\}} := \{\, f\colon X \to S \mid f(x) = 0 \text{ per quasi tutti gli } x \in X \,\}$ è un gruppo abeliano rispetto all'operazione di addizione tra funzioni definita puntualmente. Risulta che $S^{\{(X)\}}$ è divisibile ($S^{\{(X)\}}$ è la somma diretta di una famiglia di gruppi tutti uguali a S e indiciata in X). C'è un omomorfismo suriettivo di gruppi $v\colon S^{\{(X)\}} \to I$ definito da $v(f) = \sum_{x\in X} f(x)x$, per ogni $f \in S^{\{(X)\}}$ (la somma in realtà è finita, dato che $f(x) = 0$ per quasi tutti gli $x \in X$). Poiché $S^{\{(X)\}}$ è divisibile allora ogni suo quoziente lo è. Dunque, utilizzando il primo teorema d'omomorfismo per i gruppi, I ha gruppo additivo divisibile. Ora, in base a quanto detto, l'ideale R ha gruppo additivo divisibile, ovvero $pR = R$ per ogni primo p. Ma allora lo stesso vale anche per R/R^2. Quindi $R/R^2 = p(R/R^2) = (pR + R^2)/R^2$ per ogni primo p. Di conseguenza, $pR + R^2 = R$ per ogni primo p. La tesi segue come nella prima parte della dimostrazione. □

Esempio 5.13. Sia F un campo. Indichiamo con $F(X)$ il campo dei quozienti di $F[X]$. Sia $S(F) := \{\, h(X) = f(X)/g(X) \in F(X) \mid g(0) \neq 0 \,\}$. Risulta che $S(F)$ è un dominio con unico ideale massimale $R(F) := XS(F)$. Se F ha caratteristica 0 allora, per il Corollario 5.12, $R(F)$ non ha ideali massimali. □

Ulteriori esempi si possono trovare in [7, p. 504] e in [9, p. 31].

Bibliografia

[1] A. Adrian Albert. *Modern higher algebra.* XIV + 319 p. Chicago, The University of Chicago Press (The University of Chicago Science Series). Cambridge, University Press (1937). 1937.

[2] D. D. Anderson. «Commutative rngs». In: *Multiplicative ideal theory in commutative algebra. A tribute to the work of Robert Gilmer.* New York, NY: Springer, 2006, pp. 1–20. ISBN: 978-0-387-24600-0.

[3] J. L. Dorroh. «Concerning adjunctions to algebras». In: *Bull. Am. Math. Soc.* 38 (1932), pp. 85–88. ISSN: 0002-9904. DOI: 10.1090/S0002-9904-1932-05333-2.

[4] R. W. jun. Gilmer. «Eleven nonequivalent conditions on a commutative ring». In: *Nagoya Math. J.* 26 (1966), pp. 183–194. ISSN: 0027-7630. DOI: 10.1017/S0027763000011739.

[5] R. W. jun. Gilmer. «Extension of results concerning rings in which semi-primary ideals are primary». In: *Duke Math. J.* 31 (1964), pp. 73–78. ISSN: 0012-7094. DOI: 10.1215/S0012-7094-64-03106-0.

[6] R. W. jun. Gilmer. «If $R[X]$ is Noetherian, R contains an identity». In: *Am. Math. Mon.* 74 (1967), p. 700. ISSN: 0002-9890. DOI: 10.2307/2314264.

[7] Melvin Henriksen. «A simple characterization of commutative rings without maximal ideals». In: *Am. Math. Mon.* 82 (1975), pp. 502–505. ISSN: 0002-9890. DOI: 10.2307/2319747.

[8] Irving Kaplansky. *Commutative rings. 2nd revised ed.* Chicago-London: The University of Chicago Press. VIII, 182 p. 1974.

[9] Tomáš Kepka e Petr Němec. «Commutative radical rings. I». In: *Acta Univ. Carol., Math. Phys.* 48.1 (2007), pp. 11–41. ISSN: 0001-7140.

[10] Neal H. McCoy. «Prime ideals in general rings». In: *Am. J. Math.* 71 (1949), pp. 823–833. ISSN: 0002-9327. DOI: 10.2307/2372366.

[11] J. Szendrei. «On the extension of rings without divisors of zero». In: *Acta Sci. Math.* 13 (1950), pp. 231–234. ISSN: 0001-6969.

[12] Anne Vakarietis. *Preserving Properties in Extensions to Rings with Identity.* 2011-01-01. ISBN: 978-1-124-72391-4.