

Il teorema di Eakin-Nagata per gli anelli noetheriani

Dispense per i corsi di Algebra Commutativa – a.a. 2015/2016

Stefania Gabelli

Dipartimento di Matematica, Università degli Studi Roma Tre

Gli anelli noetheriani prendono il nome da Emmy Noether, per i fondamentali contributi di questa grande matematica alla Teoria degli Ideali in questo tipo di anelli (*Idealtheorie in Ringbereichen*, 1921). Lo studio degli anelli noetheriani ha avuto origine nell'ambito della Geometria Algebrica dallo studio delle k -algebre finitamente generate (quozienti di anelli di polinomi in un numero finito di indeterminate a coefficienti in un campo k).

In questi appunti daremo una dimostrazione dettagliata del ben noto Teorema di Eakin-Nagata, dimostrato nel 1968 [2, 4], il quale asserisce che, data un'estensione di anelli $R \subseteq T$ tale che T sia un R -modulo finito, se T è un anello noetheriano anche R è un anello noetheriano. (È facile dimostrare che anche il viceversa è vero.) Seguiremo il procedimento indicato da Kaplansky [3, pag. 54] e ripreso da Nagata [5].

Tutti gli anelli considerati saranno commutativi e unitari. Per le nozioni e le tecniche di base della Teoria dei Moduli e dell'Algebra Commutativa si può consultare [1, 6].

1 Preliminari

Sia R un anello commutativo unitario. Un R -modulo M si dice un *modulo noetheriano* se ogni sotto R -modulo di M è finitamente generato. Inoltre R si dice un *anello noetheriano* se è noetheriano come R -modulo.

Poiché i sotto R -moduli di un anello commutativo unitario R sono precisamente gli ideali di R , possiamo anche definire un *anello noetheriano* come un anello commutativo unitario i cui ideali sono finitamente generati.

Proposizione 1.1 *Sia R un anello commutativo unitario e M un R -modulo. Le seguenti condizioni sono equivalenti:*

- (i) M (rispettivamente R) è noetheriano;
- (ii) (Principio del massimo) Ogni insieme non vuoto di sotto R -moduli di M (rispettivamente di ideali di R) ha un elemento massimale rispetto all'inclusione;
- (iii) (Condizione della catena ascendente) Ogni catena ascendente di sotto R -moduli di M (rispettivamente di ideali di R)

$$N_0 \subseteq N_1 \subseteq \dots \subseteq N_k \subseteq \dots$$

è stazionaria, cioè esiste un (minimo) intero $h \geq 0$ tale che $N_h = N_k$ per $k \geq h$.

Dimostrazione: (i) \Rightarrow (iii) Sia $\{N_k\}_{k \geq 0}$ una catena di sotto R -moduli di M e sia $N = \bigcup_{k \geq 0} N_k$ la loro unione. Poiché $N = \alpha_1 R + \dots + \alpha_t R$ è finitamente generato, esiste un (minimo) intero $h \geq 0$ tale che $\alpha_i \in N_h$ per $i = 1, \dots, t$. Allora $N_h = N_k = N$ per ogni $k \geq h$.

(iii) \Rightarrow (ii) Sia \mathcal{S} un insieme non vuoto di sotto R -moduli di M e supponiamo che \mathcal{S} non abbia elementi massimali rispetto all'inclusione. Allora dato $N_0 \in \mathcal{S}$, esiste $N_1 \in \mathcal{S}$ tale che $N_0 \subsetneq N_1$. Poiché N_1 non è massimale in \mathcal{S} , esiste $N_2 \in \mathcal{S}$ tale che $N_0 \subsetneq N_1 \subsetneq N_2$. Così procedendo, si ottiene una catena ascendente di sotto R -moduli di M

$$N_0 \subseteq N_1 \subseteq \dots \subseteq N_k \subseteq \dots$$

che non è stazionaria.

(ii) \Rightarrow (i) Supponiamo che $N \subseteq M$ sia un sotto R -modulo che non è finitamente generato e sia \mathcal{S} l'insieme dei sotto R -moduli di M contenuti in N che sono finitamente generati. Poiché il modulo nullo appartiene ad \mathcal{S} , \mathcal{S} è non vuoto e quindi per ipotesi ha un elemento massimale L . Se $L \subsetneq N$, dato $x \in N \setminus L$, il sotto R -modulo $L' := L + xR$ di M è ancora finitamente generato e contenuto in N . Ma $L \subsetneq L'$, contro la massimalità di L . \square

Il seguente teorema è un caposaldo della teoria.

Teorema 1.2 (Teorema della Base, D. Hilbert, 1888) *Se R è un anello noetheriano e X_1, \dots, X_n , $n \geq 1$, sono indeterminate indipendenti su R , l'anello di polinomi $R[X_1, \dots, X_n]$ è un anello noetheriano. In particolare, gli anelli di polinomi $\mathbb{Z}[X_1, \dots, X_n]$ e $k[X_1, \dots, X_n]$, dove k è un campo, sono noetheriani.*

Dimostrazione: Per induzione sul numero delle indeterminate, basta dimostrare che, se R è noetheriano, lo è anche $R[X]$. Useremo le condizioni equivalenti date nella Proposizione 1.1.

Per ogni ideale non nullo I di $R[X]$ e per ogni $n \geq 0$, consideriamo il sottoinsieme $C_n(I)$ di R formato dai coefficienti direttori di tutti i polinomi di grado n appartenenti ad I e dallo zero. Si verifica facilmente che $C_n(I)$ è un ideale di R e che, se $I_1 \subseteq I_2$, si ha $C_n(I_1) \subseteq C_n(I_2)$. Inoltre

$$C_0(I) \subseteq C_1(I) \subseteq \dots \subseteq C_j(I) \subseteq \dots$$

Infatti, se $f(X) \in I$, anche $Xf(X) \in I$. Allora, data una catena di ideali di $R[X]$

$$I_0 \subseteq I_1 \subseteq \dots \subseteq I_k \subseteq \dots$$

per ogni $k, j \geq 0$, si hanno le catene di ideali di R

$$C_0(I_k) \subseteq C_1(I_k) \subseteq \dots \subseteq C_j(I_k) \subseteq C_{j+1}(I_k) \subseteq \dots$$

$$C_j(I_0) \subseteq C_j(I_1) \subseteq \dots \subseteq C_j(I_k) \subseteq C_j(I_{k+1}) \subseteq \dots$$

Poiché R è noetheriano, l'insieme di ideali $S := \{C_j(I_k)\}_{j,k \geq 0}$ ha un elemento massimale $C_p(I_q)$. Quindi in particolare $C_p(I_k) = C_p(I_q)$ per ogni $k \geq q$. D'altra parte, le catene di ideali

$$\{C_0(I_k)\}_{k \geq 0}; \quad \{C_1(I_k)\}_{k \geq 0}; \quad \dots; \quad \{C_{p-1}(I_k)\}_{k \geq 0}$$

stazionano. Quindi esiste un intero $q' \geq 0$ tale che $C_j(I_k) = C_j(I_{q'})$ per $j = 1, \dots, p-1$ e $k \geq q'$. In definitiva, se $m := \max(q, q')$, si ha

$$C_j(I_k) = C_j(I_m) \quad \text{per ogni } j \geq 0, k \geq m.$$

Per finire, mostriamo che questo implica che $I_k = I_m$ per $k \geq m$ e quindi che la catena di ideali $\{I_j\}_{j \geq 0}$ di $R[X]$ staziona. Supponiamo che $I_m \subsetneq I_k$ e sia $f(X) := a_n X^n + \dots + a_0$, $a_n \neq 0$, un polinomio di grado minimo in $I_k \setminus I_m$. Poiché $a_n \in C_n(I_k) = C_n(I_m)$, esiste un polinomio $g(X) \in I_m$ di grado n e coefficiente direttore a_n . Ma allora il polinomio $f(X) - g(X)$ ha grado strettamente minore di n e $f(X) - g(X) \in I_k \setminus I_m$, contro la minimalità di n . \square

Osservazione 1.3 Se R è noetheriano, un anello di polinomi $R[\mathbf{X}]$ in infinite indeterminate $\mathbf{X} := \{X_\lambda\}$ su R non è noetheriano, perché l'ideale $\langle \mathbf{X} \rangle$ generato da tutte le indeterminate non è finitamente generato.

Proposizione 1.4 Sia M un R -modulo e sia N un sotto modulo di M . Allora M è noetheriano se e soltanto se N è noetheriano ed il modulo quoziente M/N è noetheriano.

Inoltre, se R è un anello noetheriano e $I \subseteq R$ è un ideale, l'anello quoziente R/I è noetheriano.

Dimostrazione: Supponiamo che M sia noetheriano. Ogni sotto modulo di N è anche un sotto modulo di M . Quindi è finitamente generato su R . Inoltre, ogni sotto modulo di M/N è del tipo L/N , dove L è un sotto modulo di M contenente N . Allora se L è finitamente generato, anche L/N lo è.

Se poi R è un anello noetheriano, ogni ideale di R/I è finitamente generato come R -modulo e quindi anche come R/I -modulo.

Viceversa, sia L un sottomodulo di M . Per ipotesi $L \cap N$ e $(L + N)/N$ sono finitamente generati. Per l'isomorfismo canonico $L/(L \cap N) \cong (L + N)/N$, L è finitamente generato modulo l'ideale $L \cap N$ e quindi è finitamente generato. \square

Corollario 1.5 Siano M_1, \dots, M_n R -moduli. Allora la somma diretta $M_1 \oplus \dots \oplus M_n$ è un R -modulo noetheriano se e soltanto se M_1, \dots, M_n sono noetheriani.

In particolare, se R è un anello noetheriano, R^n è un R -modulo noetheriano.

Dimostrazione: Per induzione su n , basta dimostrare il caso $n = 2$. Sia $M := M_1 \oplus M_2$. Allora M_1 si immerge canonicamente in M tramite l'isomorfismo $M_1 \cong M_1 \oplus \{0\}$ e M_2 è canonicamente isomorfo a $M/(M_1 \oplus \{0\})$. Quindi basta applicare la Proposizione 1.4. \square

Corollario 1.6 Sia R un anello noetheriano. Allora:

- (1) Ogni R -modulo finitamente generato $M := x_1R + \cdots + x_nR$ è noetheriano.
- (2) Ogni R -algebra finitamente generata $T := R[x_1, \dots, x_n]$ è un anello noetheriano.

Dimostrazione: (1) L'applicazione

$$R^n \longrightarrow M; \quad (c_1, \dots, c_n) \mapsto x_1c_1 + \cdots + x_nc_n$$

è un omomorfismo R -lineare suriettivo. Allora M è R -isomorfo ad un quoziente di R^n ed in quanto tale è un R -modulo noetheriano (Proposizioni 1.5 e 1.4).

(2) L'anello di polinomi $R[X_1, \dots, X_n]$ è noetheriano (Teorema 1.2). Poiché l'applicazione

$$R[X_1, \dots, X_n] \longrightarrow T; \quad X_i \mapsto x_i$$

è un omomorfismo suriettivo, T è un quoziente di $R[X_1, \dots, X_n]$ ed in quanto tale è noetheriano (Proposizione 1.4) \square

2 Il Teorema di Eakin-Nagata

Se $R \subseteq T$ è un'estensione di anelli, T ha una struttura naturale di R -algebra (e dunque anche di R -modulo). Se T è un R -modulo noetheriano, allora anche R , essendo un suo sotto R -modulo è un anello noetheriano. Tuttavia in generale se T è un anello noetheriano, non è detto che T sia noetheriano come R -modulo ed infatti R può non essere noetheriano.

Ad esempio, se $R := \mathbb{Z} + X\mathbb{Q}[X]$ e $T := \mathbb{Q}[X]$, allora T è certamente un anello noetheriano, ma R non lo è, perché si può dimostrare che il suo ideale primo $X\mathbb{Q}[X]$ non è finitamente generato su R .

Il Teorema di Eakin-Nagata afferma che, nell'ipotesi aggiuntiva che T sia finitamente generato come R -modulo, se T è un anello noetheriano lo è anche R . Viceversa, ricordiamo che se R è noetheriano, anche T è un anello noetheriano per il Corollario 1.6.

La dimostrazione si svolge in vari passi. Cominciamo col ricordare alcuni fatti preliminari.

Sia M un R -modulo. L'annullatore di M in R è l'ideale $Ann_RM := (0 :_R M) \subseteq R$.

- (a) Se I è un ideale di R tale che $I \subseteq Ann_RM := (M :_R 0)$, allora M è anche un R/I -modulo, con la moltiplicazione scalare definita da $(r + I)m = rm$, per ogni $r \in R$ e $m \in M$. Quindi la struttura di M come R/I -modulo è la stessa di quella come R -modulo. In

particolare $N \subseteq M$ è un sotto R -modulo se e soltanto se è un sotto R/I -modulo e dunque M è un R -modulo noetheriano se e soltanto se è un R/I -modulo noetheriano.

Se $J \subseteq R$ è un ideale, prendendo $M := R/J$, si ha che $J \subseteq (0 :_R M)$ e dunque R/J è un R -modulo noetheriano se e soltanto se è un anello noetheriano.

- (b) Se $M = mR$ è un R -modulo ciclico, allora si ha un isomorfismo R -lineare $R/Ann_R M \rightarrow mR$.

Basta osservare che $Ann_R M = (0 :_R m)$ è il nucleo dell'omomorfismo suriettivo $R \rightarrow M = mR$, $r \mapsto mr$.

Sia $R \subseteq T$ un'estensione di anelli.

- (c) T è un R -modulo finito se e soltanto se T è una R -algebra finitamente generata e T è intero su R .

- (d) Sia $J \subseteq T$ un ideale. Se T/J è un R -modulo noetheriano allora $R/(J \cap R)$ è un R -modulo noetheriano e anche un anello noetheriano.

Basta considerare l'immersione naturale $R/(J \cap R) \subseteq T/J$ e notare che essendo $J \cap R \subseteq J \subseteq Ann_R(T/J)$, T/J ha la stessa struttura sia come R -modulo che come $R/(J \cap R)$ -modulo.

- (e) Se R/I è un anello noetheriano per ogni ideale non nullo $I \subseteq R$, allora R è un anello noetheriano.

Ogni una catena di ideali $(0) \neq I_0 \subseteq I_1 \subseteq \dots \subseteq I_k \subseteq \dots$ di R staziona, perché staziona la catena di ideali $I_1/I_0 \subseteq \dots \subseteq I_k/I_0 \subseteq \dots$ di R/I_0 .

Data un'estensione di anelli, $R \subseteq T$, consideriamo la proprietà:

- (*) Ogni ideale non nullo $I \subseteq R$ contiene un ideale contratto non nullo $J \cap R$, dove J è un ideale di T .

È immediato verificare che questa proprietà è transitiva, cioè, date estensioni di anelli $R \subseteq S \subseteq T$, se $R \subseteq S$ e $S \subseteq T$ soddisfano (*), anche $R \subseteq T$ soddisfa (*). Inoltre, se $R \subseteq T$ soddisfa (*), anche $R \subseteq S$ soddisfa (*).

Lemma 2.1 *Sia $R \subseteq T$ un'estensione di anelli. Se T/J è un R -modulo noetheriano per ogni ideale non nullo $J \subseteq T$ ed è verificata la proprietà (*), allora R è un anello noetheriano.*

Dimostrazione: Per la proprietà (*), ogni ideale non nullo $I \subseteq R$ contiene un ideale contratto non nullo $J \cap R$, con J ideale (non nullo) di T .

Poiché T/J è un R -modulo noetheriano, $R/(J \cap R)$ è un anello noetheriano (punto (d)). Ne segue che $R/I = \frac{R/(J \cap R)}{I/(J \cap R)}$ è un anello noetheriano, per ogni ideale non nullo I (Proposizione 1.4 (1)). In conclusione R è noetheriano (punto (e)). \square

Lemma 2.2 *Sia $R \subseteq T$ un'estensione di anelli. Se $C := (R :_R T) \neq (0)$, la proprietà (*) è verificata.*

Dimostrazione: Se $I \subseteq R$ è un ideale non nullo, allora IC è un ideale non nullo comune a R e T e $IC \subseteq I$. \square

Lemma 2.3 *Sia $R \subseteq T$ un'estensione di domini e supponiamo che T sia un R -modulo finitamente generato. Allora la proprietà (*) è verificata.*

Dimostrazione: Per transitività, procedendo per induzione sul numero dei generatori di T come R -algebra, possiamo supporre che $T = R[u]$, dove $u \in T$ è intero su R (punto (c)). Sia K il campo dei quozienti di R .

Caso (i) Supponiamo $R = K \cap T$. Allora, per ogni $r \in R \setminus 0$, si ha $rR = r(T \cap K) = rT \cap R$. Dunque (*) è verificata.

Caso (ii) Supponiamo che $R \subseteq T \subseteq K$. Allora $C := (R :_R T) \neq (0)$ e (*) è verificata per il Lemma 2.2.

Caso generale Sia $T = R[u]$ con u intero su R e sia $f(X) \in R[X]$ un polinomio monico tale che $f(u) = 0$. Sia poi $m(X) := a_0 + a_1X + \dots + a_nX^n \in K[X]$ il polinomio minimo di u su K . Tale polinomio divide $f(X)$ in $K[X]$ e quindi le sue radici sono elementi interi su R . Ne segue che i coefficienti a_i , essendo funzioni simmetriche di queste radici, sono elementi di K interi su R . Sia $S := R[a_0, \dots, a_n]$. Poiché S è una R -algebra finitamente generata intera su R , S è un R -modulo finitamente generato (punto (c)). Allora, essendo $R \subseteq S \subseteq K$, l'estensione $R \subseteq S$ verifica (*) per il Caso (ii).

Sia ora $U := S[u]$, essendo u intero di grado n su S , U è un S -modulo libero su S , con base $\{1, u, \dots, u^{n-1}\}$. Quindi $S = U \cap K$ e l'estensione $S \subseteq U$ verifica (*) per il Caso (i).

Poiché $R \subseteq S \subseteq U$, per transitività l'estensione $R \subseteq U$ verifica (*). Poiché poi $R \subseteq T = R[u] \subseteq U = S[u]$, anche l'estensione $R \subseteq T$ verifica (*). \square

Proposizione 2.4 *Sia $R \subseteq T$ un'estensione di anelli e supponiamo che:*

- (1) *T sia un R -modulo finitamente generato;*
 - (2) *T/J sia un R -modulo noetheriano per ogni ideale non nullo $J \subseteq T$.*
- Allora R è un anello noetheriano.*

Dimostrazione: Se T è un dominio, (1) implica che l'estensione $R \subseteq T$ verifica la proprietà (*) (Lemma 2.3). Ne segue che R è noetheriano per il Lemma 2.1.

Supponiamo che T non sia un dominio e sia $z \in T$ uno zerodivisore non nullo. Allora per ipotesi T/zT è un R -modulo noetheriano e dunque, per l'inclusione naturale $R/(zT \cap R) \subseteq T/zT$ anche il modulo quoziente $R/(zT \cap R)$ è noetheriano.

Se $zT \cap R = (0)$, otteniamo che R è noetheriano. Altrimenti, notiamo che $\text{Ann}_T(zT) \neq (0)$ e dunque per ipotesi $zT \cong T/\text{Ann}_T(zT)$ è un R -modulo noetheriano. Ne segue che il suo sottomodulo non nullo $zT \cap R$ è noetheriano. Poiché anche $R/(zT \cap R)$ è noetheriano, concludiamo che R è noetheriano (Proposizione 1.4). \square

Osservazione 2.5 Nella dimostrazione della proposizione precedente, se T non è un dominio, l'ipotesi che T sia un R -modulo finitamente generato non è necessaria.

Teorema 2.6 (*Eakin-Nagata, 1968*) *Sia $R \subseteq T$ un'estensione di anelli. Se T è un anello noetheriano finitamente generato come R -modulo, allora R è un anello noetheriano.*

Dimostrazione: Se T/J è un R -modulo noetheriano per ogni ideale non nullo $J \subseteq T$, allora R è un anello noetheriano per la Proposizione 2.4. Altrimenti, essendo T un anello noetheriano, l'insieme (non vuoto per ipotesi) degli ideali non nulli $J \subseteq T$ tali che T/J non è un R -modulo noetheriano ammette un elemento massimale L . L'estensione di anelli $R/(L \cap R) \subseteq T/L$ soddisfa le ipotesi della Proposizione 2.4, quindi, $R/(L \cap R)$ è un anello noetheriano ed anche un R -modulo noetheriano (punto (a)).

Facciamo vedere che R è un anello noetheriano. Per l'isomorfismo naturale di moduli $R/(L \cap R) \cong (R+L)/L$, si ha che $(R+L)/L$ è un R -modulo noetheriano. Sia I un ideale di R , allora $(I+L)/L$ è finitamente generato come sottomodulo di $(R+L)/L$. D'altra parte, poiché T è finitamente generato su R ed è un anello noetheriano, ogni suo ideale, in particolare L , è un R -modulo finitamente generato. Concludiamo che I è finitamente generato su R , e quindi R è noetheriano. \square

Osservazione 2.7 Si può dimostrare che l'ideale L di T considerato nella dimostrazione del Teorema di Eakin-Nagata è primo. Quindi, nelle ipotesi del teorema, se esiste qualche ideale non nullo $J \subseteq T$ tale che T/J non sia un R -modulo noetheriano, ci si può ridurre al caso in cui $R \subseteq T$ sia un'estensione di domini.

Per vedere questo, ci occorre ricordare che se M è un R -modulo noetheriano, allora $R/\text{Ann}_R M$ è un anello noetheriano.

Infatti, poiché M è noetheriano, esso è un R -modulo finitamente generato. Sia $M = m_1R + \dots + m_kR$. Allora

$$\text{Ann}_R M = (0 :_R M) = \bigcap_{i=1, \dots, k} (0 :_R m_i) = \bigcap_{i=1, \dots, k} \text{Ann}_R m_i R$$

e, per il punto (b), si ha un isomorfismo $R/\text{Ann}_R m_i R \cong m_i R$.

Ogni modulo ciclico $m_i R$ è noetheriano, come sotto modulo di M , e dunque lo è anche il modulo $m_1 R \oplus \dots \oplus m_k R$ (Proposizione 1.5). Poiché si

ha un omomorfismo di moduli

$$R \longrightarrow m_1R \oplus \cdots \oplus m_kR, \quad r \mapsto (m_1r, \dots, m_kr)$$

il cui nucleo è $\bigcap_{i=1, \dots, k} \text{Ann}_R m_iR \cong \text{Ann}_R M$, allora $R/\text{Ann}_R M$ è isomorfo ad un sotto R -modulo di $m_1R \oplus \cdots \oplus m_kR$ e dunque è noetheriano.

Allora, sia L massimale tra gli ideali J di T tali che T/J non sia un R -modulo noetheriano. Supponiamo per assurdo che L non sia primo, cioè esistano $a, b \in T \setminus L$ tali che $ab \in L$. Otterremo una contraddizione facendo vedere che in questo caso T/L è un R -modulo noetheriano.

Si ha un isomorfismo $T/(L + aT) \cong \frac{T/L}{(L+aT)/L}$. Per la massimalità di L , $T/(L + aT)$ è un R -modulo noetheriano. Per concludere che T/L è un R -modulo noetheriano, basta far vedere che anche $(L + aT)/L$ è un R -modulo noetheriano (Proposizione 1.4).

Notiamo che $(L + aT)/L = (a + L)T$ è un T -modulo ciclico. Poiché $(L + bT) \subseteq \text{Ann}_T((L + aT)/L)$, $(L + aT)/L$ è un modulo ciclico anche su $T/(L + bT)$ (punto (a)). D'altra parte, anche $T/(L + bT)$ è un R -modulo noetheriano e $\text{Ann}_R(T/(L + bT)) = (L + aT) \cap R =: A$. Perciò, come visto sopra, R/A è un anello noetheriano. Inoltre, essendo $T/(L + bT)$ finitamente generato su R/A (perché lo è T su R), otteniamo che $(L + aT)/L$ è finitamente generato su R/A . Ne segue che $(L + aT)/L$ è un R/A -modulo noetheriano e anche un R -modulo noetheriano.

Riferimenti bibliografici

- [1] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.
- [2] P. M. Eakin, *The converse to a well-known theorem on Noetherian ring*, Math. Annalen 177, 278-282, 1968.
- [3] I. Kaplansky, *Commutative rings*. Revised edition. The University of Chicago Press, Chicago, Ill.-London, 1974.
- [4] M. Nagata, *A type of subring of a Noetherian ring*, J. Math. Kyoto Univ., 465-467, 1968.
- [5] M. Nagata, *A Proof of the Theorem of Eakin-Nagata*, Proc. Japan Acad., 67, Ser. A, 238-239, 1991.
- [6] R.Y. Sharp, *Steps in Commutative Algebra*, London Math. Soc. Student Texts 51, 1990.