MATH 902 LECTURE NOTES, SPRING 2022

Contents

Lecture of January 19, 2022

In this class, all rings are assumed to be commutative, with associative multiplication and containing 1.

1. Finiteness conditions

1.1. Finitely generated algebras.

We start by recalling a definition from last semester, specialized to the setting of commutative rings.

Definition 1.1 (Algebra)**.** Given a ring A, an A-*algebra* is a ring R equipped with a ring homomorphism $\phi : A \to R$. This defines an A-module structure on R given by restriction of scalars, that is, for $a \in A$ and $r \in R$, $ar := \phi(a)r$ that is compatible with the internal multiplication of R i.e.,

$$a(rs) = (ar)s = r(as) \text{ for all } a \in A, rs \in R.$$

We will call ϕ the *structure homomorphism* of the A-algebra R.

Example 1.2.

- If A is a ring and $x_1, \dots, x_n$ are indeterminates, the inclusion map $A \hookrightarrow A[x_1, \dots, x_n]$ makes the polynomial ring into an A-algebra.
- When $A \subseteq R$ the inclusion map makes R an A-algebra. In this case the A-module multiplication ar coincides with the internal (ring) multiplication on R.
- Any ring comes with a unique structure as a $\mathbb{Z}$-algebra.

The collection of A-algebras forms a category where the morphisms are ring homomorphisms $f : R \to S$ such that the following diagram commutes

$$\begin{tikzcd} & A \arrow[dl, "\phi"'] \arrow[dr, "\psi"] & \\ R \arrow[rr, "f"'] & & S \end{tikzcd}$$

for structural homomorphisms $\varphi : A \to R$ and $\psi : A \to S$.

Definition 1.3 (Algebra generation)**.** Let R be an A-algebra and let $\Lambda \subseteq R$ be a set. The A-*algebra generated by* a subset Λ of R, denoted $A[\Lambda]$, is the smallest (w.r.t containment) subring of R containing Λ and $\varphi(A)$.

A set of elements $\Lambda \subseteq R$ *generates* R as an A-algebra if $R = A[\Lambda]$.

Note that there are two different meanings for the notation $A[S]$ for a ring A and set S: one calls for a polynomial ring, and the other calls for a subring of something.

This can be unpackaged more concretely in a number of equivalent ways:

Lemma 1.4. *The following are equivalent*

(1) Λ *generates R as an A-algebra.*
(2) *Every element in R admits a polynomial expression in Λ with coefficients in $\phi(A)$, i.e.*
$$R = \left\{ \sum_{\text{finite}} \phi(a)\lambda_1^{i_1}\cdots\lambda_n^{i_n} \mid a \in A, \lambda_j \in \Lambda, i_j \in \mathbb{N} \right\}.$$
(3) *The A-algebra homomorphism $\psi : A[X] \to R$, where $A[X]$ is a polynomial ring on a set of indeterminates X in bijection with Λ and $\psi(x_i) = \lambda_i$, is surjective.*

Proof. Let $S = \left\{\sum_{\text{finite}} \phi(a)\lambda_1^{i_1}\cdots\lambda_n^{i_n} \mid a \in A, \lambda_j \in \Lambda, i_j \in \mathbb{N}\right\}$. For the equivalence between (2) and (3) we note that S is the image of ψ. In particular, S is a subring of R. It then follows from the definition that (1) implies (2). Conversely, any subring of R containing $\phi(A)$ and Λ certainly must contain S, so (2) implies (1). $\square$

Example 1.5. We may have also seen these brackets used in $\mathbb{Z}[\sqrt{d}]$ for some $d \in \mathbb{Z}$ to describe the ring
$$\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$
In fact, this is a special instance of generating: the $\mathbb{Z}$-algebra generated by $\sqrt{d}$ in the most natural place, the algebraic closure of $\mathbb{Q}$, is exactly the set above. The point is that for any power $(\sqrt{2})^n$, write $n = 2q + r$ with $r \in \{0, 1\}$, so $(\sqrt{2})^n = 2^d(\sqrt{2})^r$. Similarly, the ring $\mathbb{Z}[\sqrt[3]{d}]$ can be written as
$$\{a + b\sqrt[3]{d} + c\sqrt[3]{d^2} \mid a, b, c \in \mathbb{Z}\}.$$

Note that the homomorphism ψ in part (3) need not be injective.

- If the homomorphism ψ is injective (so an isomorphism) we say that A is a *free* algebra.
- the set $\ker(\psi)$ measures how far R is from being a free A-algebra and is called the set of *relations* on Λ.

Definition 1.6 (Algebra-finite)**.** We say that $\varphi : A \to R$ is *algebra-finite*, or R is a *finitely generated A-algebra*, if there exists a finite set of elements $f_1, \dots, f_d$ that generates R as an A-algebra. We write $R = A[f_1, \dots, f_d]$ to denote this.

The term *finite-type* is also used to mean this.

Remark 1.7. Note that, by the lemma on generating sets, an A-algebra is finitely generated if and only if it is isomorphic to a quotient of a polynomial ring over A in finitely many variables. The choice of an isomorphism with a quotient of a polynomial ring is equivalent to a choice of generating set.

Lecture of January 21, 2022

Example 1.8. Let K be a field, and $B = K[x, xy, xy^2, xy^3, \dots] \subseteq C = K[x, y]$, where x and y are indeterminates. Let A be a finitely generated subalgebra of B, and write $A = K[f_1, \dots, f_d]$. Since each f_i is a (finite) polynomial expression in the monomials $\{xy^i \mid i \in \mathbb{N}\}$, it involves only finitely many of these monomials. Thus, there is an m such that $\{f_1, \dots, f_d\} \subset K[x, xy, \dots, xy^m]$, and hence $A \subseteq K[x, xy, \dots, xy^m]$.

But, every element of $K[x, xy, \dots, xy^m]$ is a K-linear combination of monomials with the property that the y exponent is no more than m times the x exponent, so this ring does not contain xy^{m+1}. Thus, B is not a finitely generated K-algebra.

Optional Exercise 1.9. Let $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ be ring homomorphisms (so B is an A-algebra via ϕ, C is a B-algebra via ψ, and C is an A-algebra via $\psi \circ \phi$). Then

- If $A \xrightarrow{\phi} B$ and $B \xrightarrow{\psi} C$ are algebra-finite, then $A \xrightarrow{\psi\phi} C$ is algebra-finite. (Take the union of the generating sets.)
- If $A \xrightarrow{\psi\phi} C$ is algebra-finite, then $B \xrightarrow{\psi} C$ is algebra-finite. (Use the same generating set.)
- If $A \xrightarrow{\psi\phi} C$ is algebra-finite, then $A \xrightarrow{\phi} B$ may *not* be algebra-finite. (Use the previous example.)

Remark 1.10. Any surjective φ is algebra-finite: the target is generated by 1. Since any homomorphism $\phi : A \to R$ can be factored as $\phi = \psi \circ \varphi$ where φ is the surjection $\varphi : A \to A/\ker(\varphi)$ and ψ is the inclusion $\psi : A/\ker(\varphi) \hookrightarrow R$, to understand algebra-finiteness, it suffices to restrict our attention to injective homomorphisms by the last bullet point of the previous exercise.

There are many basic questions about algebra generators that are surprisingly difficult. Let $R = \mathbb{C}[x_1, \dots, x_n]$ and $f_1, \dots, f_n \in R$. When do $f_1, \dots, f_n$ generate R over $\mathbb{C}$? It is not too hard to show that the Jacobian determinant

$$\det \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_n} \end{bmatrix}$$

must be a nonzero constant. It is a big open question whether this is in fact a sufficient condition!

1.2. **Finitely generated modules.** We will also find it quite useful to consider a stronger finiteness property for maps.

Definition 1.11. (Module generation) Let M be an A-module and let $\Gamma \subseteq M$ be a set. The A-*submodule* of M *generated by* Γ, denoted $\sum_{\gamma \in \Gamma} A\gamma$, is the smallest (w.r.t containment) submodule of M containing Γ.

A set of elements $\Gamma \subseteq M$ *generates* M as an A-module if the submodule of M generated by Γ is M itself, i.e. $M = \sum_{\gamma \in \Gamma} A\gamma$.

This also has some equivalent realizations:

Lemma 1.12. *The following are equivalent:*

(1) Γ *generates* M *as an* A*-module.*
(2) *Every element of* M *admits a linear combination expression in the elements of* Γ *with coefficients in* A*.*
(3) *The homomorphism* $\theta : A^{\oplus Y} \to M$*, where* $A^{\oplus Y}$ *is a free* A*-module with basis* Y *in bijection with* Γ *via* $\theta(y_i) = \gamma_i$*, is surjective.*

Optional Exercise 1.13. Prove the previous lemma.

Definition 1.14 (Module-finite)**.** We say that a ring homomorphism $\varphi : A \to R$ is *module-finite* if R is a finitely-generated A-module, that is, there is a *finite* set $m_1, \dots, m_n \in M$ so that $M = \sum_{i=1}^n Am_i$.

As with algebra-finiteness, surjective maps are always module-finite in a trivial way. The notion of module-finite is much stronger than algebra-finite, since a linear combination is a very special type of polynomial expression. To be specific:

Lemma 1.15 (Module-finite $\Rightarrow$ algebra-finite)**.** *If $\varphi : A \to R$ is module-finite then it is algebra-finite.*

The converse is not true.

Example 1.16.
(1) If $K \subseteq L$ are fields, L is module-finite over K just means that L is a finite field extension of K.
(2) The Gaussian integers $\mathbb{Z}[i]$ satisfy the well-known property (or definition, depending on your source) that any element $z \in \mathbb{Z}[i]$ admits a unique expression $z = a + bi$ with $a, b \in \mathbb{Z}$. That is, $\mathbb{Z}[i]$ is generated as a $\mathbb{Z}$-module by $\{1, i\}$; moreover, they form a free module basis!
(3) If R is a ring and x an indeterminate, $R \subseteq R[x]$ is not module-finite. Indeed, $R[x]$ is a free R-module on the basis $\{1, x, x^2, x^3, \dots\}$. It is however algebra-finite.
(4) Another map that is *not* module-finite is the inclusion of $K[x] \subseteq K[x, 1/x]$. Note that any element of $K[x, 1/x]$ can be written in the form $f(x)/x^n$ for some $f(x) \in K[x]$ and $n \in \mathbb{N}$. Then, any finitely generated $K[x]$-submodule M of $K[x, 1/x]$ is of the form $M = \sum_i \frac{f_i(x)}{x^{n_i}} \cdot K[x]$; taking $N = \max\{n_i \mid i\}$, we find that $M \subseteq 1/x^N \cdot K[x] \neq K[x, 1/x]$.

Optional Exercise 1.17. Let $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ be ring homomorphisms. Then

- If $A \xrightarrow{\phi} B$ and $B \xrightarrow{\psi} C$ are module-finite, then $A \xrightarrow{\psi\phi} C$ is module-finite.
- If $A \xrightarrow{\psi\phi} C$ is module-finite, then $B \xrightarrow{\psi} C$ is module-finite.

We will see that $A \xrightarrow{\psi\phi} C$ is module-finite does not imply $A \xrightarrow{\phi} B$ is module-finite soon.

1.3. **Integral extensions.** In field theory, there is a close relationship between (vector space-)finite field extensions and algebraic equations. The situation for rings is similar.

Definition 1.18 (Integral element/extension)**.** Let $\phi : A \to R$ be a ring homomorphism (for which we will denote $\phi(a)$ by a) and $r \in R$. The element r is *integral* if there are elements $a_0, \dots, a_{n-1} \in A$ such that

$$r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0;$$

i.e., r satisfies a *equation of integral dependence* over A. The homomorphism ϕ is *integral* if every element of R is integral over A.

Example 1.19. Let $A = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. The element $t = \sqrt{2} \in A$ is integral over $\mathbb{Z}$, since $t^2 - 2 = 0$. Likewise, $s = 1 + \sqrt{2}$ is integral over $\mathbb{Z}$, as $s^2 = 3 + 2\sqrt{2}$, so $s^2 - 2s - 1 = 0$.

On the other hand, $\frac{1}{2} \in \mathbb{Q}$ is not integral over $\mathbb{Z}$: if

$$\left(\frac{1}{2}\right)^n + a_{n-1}\left(\frac{1}{2}\right)^{n-1} + \cdots + a_0 = 0$$

with $a_i \in \mathbb{Z}$, multiply through by 2^n to get $1 + 2a_{n-1} + 2^2 a_{n-2} + \cdots + 2^n a_0 = 0$, which is impossible.

Lecture of January 24, 2022

Proposition 1.20. *Let $A \subseteq R$ be rings.*
(1) *If $r \in R$ is integral over A then $A[r]$ is module-finite over A.*
(2) *If $r_1, \dots, r_t \in R$ are integral over A then $A[r_1, \dots, r_t]$ is module-finite over A.*

Proof. (1) Suppose r is integral over A, satisfying the equation $r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0$. Then $A[r] = \sum_{i=0}^{n-1} Ar^i$. Indeed, $s \in A[r]$ with a polynomial expression $s = p(r) = \sum c_j r^j$ of degree $m \geqslant n$, we can use the equation above to rewrite the leading term $a^m r^m$ as $-a_m r^{m-n}(a_{n-1}r^{n-1} + \cdots + a_1 r + a_0)$, and decrease the degree in r.

(2) Write $A_0 := A \subseteq A_1 := A[r_1] \subseteq A_2 := A[r_1, r_2] \subseteq \cdots \subseteq A_t := A[r_1, \dots, r_t]$. Note that r_i is integral over A_{i-1}: use the same monic equation of r_i over A. Then, the inclusion $A \subseteq A[r_1, \dots, r_t]$ is a composition of module-finite maps, hence is module-finite. $\square$

We recall that the *classical adjoint* of an $n \times n$ matrix A is the $n \times n$ matrix whose (i,j)-entry is $(-1)^{i+j}$ times the determimant of the matrix obtained from A by removing the ith column and the jth row.

Lemma 1.21 (Determinantal trick)**.** *Let R be a ring, $B \in M_{n\times n}(R)$, $v \in R^{\oplus n}$, and $r \in R$.*

(1) $\operatorname{adj}(B)B = \det(B)I_{n\times n}$.
(2) *If $Bv = rv$, then* $\det(rI_{n\times n} - B)v = 0$.

Proof. (1) When R is a field, this is a basic linear algebra fact. We deduce the case of a general ring from the field case.

The ring R is a $\mathbb{Z}$-algebra, so we can write R as a quotient of some polynomial ring $\mathbb{Z}[X]$. Let $\psi : \mathbb{Z}[X] \twoheadrightarrow R$ be a surjection, $a_{ij} \in \mathbb{Z}[X]$ be such that $\psi(a_{ij}) = b_{ij}$, and let $A = [a_{ij}]$. Note that

$$\psi(\operatorname{adj}(A)_{ij}) = \operatorname{adj}(B)_{ij} \quad \text{and} \quad \psi((\operatorname{adj}(A)A)_{ij}) = (\operatorname{adj}(B)B)_{ij},$$

since ψ is a homomorphism, and the entries are the same polynomial functions of the entries of the matrices A and B, respectively. Thus, it suffices to establish

$$\operatorname{adj}(B)B = \det(B)I_{n\times n}$$

in the case when $R = \mathbb{Z}[X]$, and we can do this entry by entry. Now, $R = \mathbb{Z}[X]$ is an integral domain, hence a subring of a field (its fraction field). Since both sides of the equation

$$(\operatorname{adj}(B)B)_{ij} = (\det(B)I_{n\times n})_{ij}$$

live in R and are equal in the fraction field (by linear algebra) they are equal in R. This holds for all i, j, and thus 1) holds.

(2) We have $(rI_{n\times n} - B)v = 0$, so by part 1)

$$\det(rI_{n\times n} - B)v = \operatorname{adj}(rI_{n\times n} - B)(rI_{n\times n} - B)v = 0. \quad \square$$

Theorem 1.22. *Let $A \subseteq R$ be module-finite. Then R is integral over A.*

Proof. Given $r \in R$, we want to show that r is integral over A. The idea is to show that multiplication by r, realized as a linear transformation over A, satisfies the characteristic polynomial of that linear transformation.

Write $R = Ar_1 + \cdots + Ar_t$. We may assume that $r_1 = 1$, perhaps by adding module generators. By assumption, we can find $a_{ij} \in A$ such that

$$rr_i = \sum_{j=1}^{t} a_{ij} r_j$$

for each i. Let $C = [a_{ij}]$, and v be the column vector $(r_1, \dots, r_t)$. We have $rv = Cv$, so by the determinant trick, $\det(rI_{n\times n} - C)v = 0$. Since we chose one of the entries of v to be 1, we have in particular that $\det(rI_{n\times n} - C) = 0$. Expanding this determinant as a polynomial in r, this is a monic equation with coefficients in A. $\square$

Collecting the previous results, we now have a useful characterization of module-finite extensions:

Corollary 1.23 (Characterization of module-finite extensions)**.** *Let $A \subseteq R$ be rings. R is module-finite over A if and only if R is integral and algebra-finite over A.*

Proof. ($\Rightarrow$): A generating set for R as an A-module serves as a generating set as an A-algebra. The remainder of this direction comes from the previous theorem. ($\Leftarrow$): If $R = A[r_1, \dots, r_t]$ is integral over A, so that each r_i is integral over A, then R is module-finite over A by Proposition 1.20. ☐

Corollary 1.24. *If R is generated over A by integral elements, then R is integral. Thus, if $A \subseteq S$, the set of elements of S that are integral over A form a subring of S.*

Proof. Let $R = A[\Lambda]$, with λ integral over A for all $\lambda \in \Lambda$. Given $r \in R$, there is a finite subset $L \subseteq \Lambda$ such that $r \in A[L]$. By the theorem, $A[L]$ is module-finite over A, and $r \in A[L]$ is integral over A.

For the latter statement, the first statement implies that

$$\{\text{integral elements}\} \subseteq A[\{\text{integral elements}\}] \subseteq \{\text{integral elements}\},$$

so equality holds throughout, and {integral elements} is a ring. ☐

Example 1.25. (1) Not all integral extensions are module-finite. Let $K = \overline{K}$, and consider the ring

$$R = K[x, x^{1/2}, x^{1/3}, x^{1/4}, x^{1/5}, \dots] \subseteq \overline{K(x)}.$$

Clearly R is generated by integral elements over $K[x]$, hence integral, but is not algebra-finite over $K[x]$.

(2) Let x, y, z be indeterminates. Set $R = \mathbb{C}[x, y]$ to be a polynomial ring, and $S = \mathbb{C}[x, y, z]/(x^2 + y^2 + z^2)$ to be a quotient of a polynomial ring. We claim that we can realize R as a subring of S; i.e., the $\mathbb{C}$-algebra homomorphism from R to S that sends x to x and y to y is injective. Indeed, the kernel is the set of polynomials in x, y that are multiples of $z^2 + x^2 + y^2$, but, thinking of $\mathbb{C}[x, y, z]$ as $R[z]$, any nonzero multiple of $z^2 + x^2 + y^2$ must have z-degree at least 2, so none only involve x, y. Thus, we have an inclusion $R \subseteq S$.

The ring S is module-finite over R: indeed, S is generated over R as an algebra by one element z that is integral over R.

Index