Problems on rings

Peter J. Cameron

Associated with *Introduction to Algebra*, OUP 2008

1. Let R be a commutative ring with identity. A *formal Laurent series* is an expression of the form $\sum_{n\in\mathbb{Z}} a_n x^n$, such that there exists $n_0 \in \mathbb{Z}$ for which $a_n = 0$ for all $n < n_0$. Addition of formal Laurent series is defined "coordinatewise", while multiplication is given by the rule

$$\left(\sum a_n x^n\right)\left(\sum b_n x^n\right) = \sum c_n x^n,$$

where

$$c_n = \sum_{i\in\mathbb{Z}} a_i b_{n-i}.$$

(a) Prove that multiplication is well defined (that is, the expression above for c_n as a sum has only finitely many non-zero summands).

(b) Prove that the set $R((x))$ of formal Laurent series (with addition and multiplication as above) is a ring containing the ring $R[[x]]$ of formal power series.

(c) Suppose that R is a field. Show that $R((x))$ is a field.

(d) Suppose that R is a field. Show that $R((x))$ is the field of fractions of $R[[x]]$.

(e) Suppose that R is a field. What is the relationship between $R((x))$ and $R(x)$ (the field of rational functions over R)?

2. Let K be a field containing $\mathbb{Q}$. An element $a \in K$ is an *algebraic number* if it is a root of a polynomial with coefficients in $\mathbb{Q}$.

(a) Show that an element $a \in K$ is an algebraic number if and only if it is a root of a polynomial with coefficients in $\mathbb{Z}$.

(b) Show that an element $a \in K$ is an algebraic number if and only if it is an eigenvalue of a matrix with entries in $\mathbb{Q}$.

An element $a \in K$ is an *algebraic integer* if it is a root of a *monic* polynomial with coefficients in $\mathbb{Z}$.

(c) Show that an element $a \in K$ is an algebraic integer if and only if it is an eigenvalue of a matrix with entries in $\mathbb{Z}$.

(d) Use (b) and (c) above to show that the set of algebraic numbers in K is a field, while the set of algebraic integers is a ring. [*Hint:* Let A and B be matrices with eigenvalues a and b respectively. Show that $a+b$ and ab are eigenvalues of $(A\otimes I)+(I\otimes B)$ and $A\otimes B$ respectively, where $\otimes$ denotes the *Kronecker product* of matrices.]

(e) Generalise to the case where R be an integral domain, F its field of fractions, and K a field containing F.

3. Let F be a field, and K a field containing F. An element $a\in K$ is called *transcendental* over F if it is not algebraic over F. More generally, an n-tuple $(a_1,\dots,a_n)\in K^n$ is *algebraically independent* over F if there does not exist a non-zero polynomial $f(x_1,\dots,x_n)\in F[x_1,\dots,x_n]$ such that $f(a_1,\dots,a_n)=0$.

(a) Show that the algebraically independent finite subsets satisfy the axioms for a matroid (see p.161 in the book).

(b) Deduce that, if there are no infinite sets of elements all of whose finite subsets are algebraically independent, then all maximal algebraically independent subsets have the same cardinality. (Such sets are called *transcendence bases*, and their cardinality the *transcendence degree*, of K over F.)

(c) Suppose that F is algebraically closed and that K has transcendence degree n over F. Show that K is an algebraic extension of $F(a_1,\dots,a_n)$, where $(a_1,\dots,a_n)$ is a transcendence basis for K over F.

4. Let R be a commutative ring with identity. Recall that, assuming the Axiom of Choice, every ideal of R is contained in a maximal ideal (exercise 6.11 on p.235 in the book). Define the *radical* $J(R)$ of R to be the intersection of the maximal ideals of R.

(a) Prove that $J(R)$ is an ideal of R.

(b) Prove that, if $a\in J(R)$, then $1+a$ is a unit. [*Hint:* Am element $r\in R$ is a unit if and only if $\langle r\rangle = R$.]

(c) Suppose that R has only finitely many maximal ideals. Prove that $R/J(R)$ is isomorphic to a direct sum of fields. [*Hint:* The isomorphism is

$$a+J(R)\mapsto (a+M_1,\dots,a+M_n),$$

where $M_1,\dots,M_n$ are the maximal ideals.

5. Let R be a finite commutative ring with identity, and let $J(R)$ be its radical.

(a) Show that, if $a \in J(R)$, then $a^m = 0$ for some positive integer m.

(b) Deduce that there is a positive integer n such taht $J(R)^n = \{0\}$, where

$$J(R)^n = \{a_1 a_2 \cdots a_n : a_1, a_2, \ldots, a_n \in J(R)\}.$$

6**. (a) Prove that a finite commutative ring with identity is isomorphic to a direct sum of local rings.

(b) Prove that any finite commutative ring with identity R has the property that, if S is a proper ideal of R, then $\mathrm{Ann}(S) \neq \{0\}$, where

$$\mathrm{Ann}(S) = \{r \in R : (\forall s \in S)(rs = 0)\}.$$

[*Hint:* Prove that the property holds for a local ring and is preserved under direct sums.]

(c) Prove that, if R is a finite commutative ring with identity and T a proper submodule of the free module R^n, then $T^\perp \neq \{0\}$, where

$$N^\perp = \{m \in R^n : (\forall t \in T)(m \cdot t = 0\},$$

where $m \cdot t$ is the dot product

$$m \cdot t = m_1 t_1 + m_2 t_2 + \cdots + m_n t_n.$$

(d) Find an example of a commutative ring with identity R with an ideal S such that $|\mathrm{Ann}(S)| \neq |R|/|S|$.

7. Let F be a field. An *algebra* over F, or for short an F-*algebra*, consists of a set A with operations of addition, multiplication, and scalar multiplication by elements of F, such that

- with addition and multiplication, A is a ring;
- with addition and scalar multiplication, A is a left vector space over F;
- For any $c \in F$ and $a, b \in A$, we have

$$c(ab) = (ca)b = a(cb).$$

(a) Prove that each of the following is an algebra (with operations which you should specity):

- The sets of polynomials and of formal power series over F;
- An extension field of F;
- The set of $n \times n$ matrices over F.

(b) Define *F-subalgebra* and *F-algebra homomorphism* and begin to develop the isomorphism theorems.

8. Let G be a group, and F a field. Define the *group algebra FG* of G over F to be the set of functions from G to F which are non-zero on only finitely many elements of G, with addition and scalar multiplication defined as usual for functions, and multiplication given by *convolution*:

$$(f_1 f_2)(g) = \sum_{\substack{h,k\in G \\ hk=g}} f_1(h) f_2(k).$$

(a) Show that FG is an F-algebra with identity, which is commutative if and only if G is. [You have to prove that multiplication is well-defined.]

(b) Define $\varepsilon : FG \to F$ by

$$f\varepsilon = \sum_{g\in G} f(g).$$

Show that ε is an F-algebra homomorphism and describe its kernel.

9. A *graded F-algebra* is an F-algebra A with an expression

$$A = \bigoplus_{n\geq 0} A_n$$

as F-vector space, satisfying $A_m A_n \subseteq A_{m+n}$.

(a) Prove that A_0 is an F-subalgebra of A, containing the identity of A if there is one, and that A_n is an (A_0, A_0)-bimodule for all n.

(b) Suppose that

- A is commutative;

- A is generated by a finite number of homogeneous elements (belonging to A_n for varioius n); and
- $A_0 = F \cdot 1$, where 1 is the identity.

Prove that there is a polynomial $p(x)$ over $\mathbb{Z}$ satisfying

$$\dim(A_n) \leq p(n)$$

(where dim means F-vector space dimension).

(c) Let $A = F[x_1, \ldots, x_d]$, and let A_n be spanned by the monomials of total degree d. Show that A is a graded algebra satisying the hypotheses of (b), and calculate the dimension of A_n as F-vector space.