Ezzeddine El Sai
Howie Jordan
Toby Aldape

Commutative Algebra
Assignment 1

1. Every commutative ring is a homomorphic image of a subring of a field. It follows that any positive universal sentence satisfied by fields is also satisfied by any commutative ring (e.g. the Cayley-Hamilton Theorem).

Proof.

First we note that any integral domain D can inject into a field via constructing the field of fractions. Hence, every integral domain is isomorphic to a subring of a field.

Next, we note that for any set X we can construct a free commutative ring of characteristic 0 $F(X)$ on X. This can be given explicitly by taking the ring $\mathbb{Z}[X]$ consisting of finite sums of integers and integer multiples of finite formal products of elements of X.

We show that $\mathbb{Z}[X]$ is an integral domain. Any element of $\mathbb{Z}[X]$ can be represented as a multivariate polynomial in the elements of X, say

$$p(X) = \sum_{i=0}^{D} z_i \prod_{j=0}^{N_i} x_j^i$$

where each $z_i \in \mathbb{Z}$, $D, M_i \in \mathbb{N}$, and x_j^i are formal indeterminants, one for each element of X. We take these representations to be reduced, so that each product of N_i indeterminants in X is distinct. We also impose a linear order on the set of indeterminants X[1] and then impose the induced lexicographic order on the set of monomials.

For any two $p(X), q(X) \in \mathbb{Z}[X]$, $p(X)q(X)$ can then be given by

$$p(X)q(X) = (\sum_{i=0}^{D_p} z_i \prod_{j=0}^{N_i} x_j^i)(\sum_{i=0}^{D_q} w_i \prod_{j=0}^{M_i} x_j^i).$$

Consider the greatest monomial of $p(X)$ and $q(X)$ under the lexicographic ordering, say $p_1(X) = z \prod_{a=0}^{N} x_a$ and $q_1(X) = w \prod_{b=0}^{M} x'_b$. Then the product of these monomials will be given by

$$zw \prod_{a=0}^{N} x_a \prod_{b=0}^{M} x'_b$$

and since $z, w \in \mathbb{Z}$ are nonzero, and $\mathbb{Z}$ is an integral domain, their product zw is nonzero. We also claim that there will be no other monomials in the product $p(X)q(X)$ with the same indeterminates. To see this, consider that for any other monomial of $p(X)$, say $p_0(X)$ we have $p_0(X) < p_1(X)$. Hence for any $q_0(X)$ a monomial of $q(X)$, the product $p_0(X)q_0(X)$ then is strictly less than $p_1(X)q_1(X)$ in the lexicographic ordering and will not cancel will $p_1(X)q_1(X)$. Thus, the product $p(X)q(X)$ is not 0, so $\mathbb{Z}[X]$ is an integral domain for any X.

We will also show that $\mathbb{Z}[X]$ satisfies the universal property for the free commutative ring, that is, the set maps $X \to U(R)$ are in bijection with the ring homomorphisms $\mathbb{Z}[X] \to R$, where $U : \mathbf{CRing} \to \mathbf{Set}$ is the functor taking a ring to its underlying set.

First, suppose that we are given a set map $f : X \to U(R)$. Then we can define $\phi : \mathbb{Z}[X] \to R$ by mapping each formal indeterminant $x \in X$ to $f(x) \in R$ and each element

[1] This may require the well-ordering principle, and hence the axiom of choice.

Ezzeddine El Sai
Howie Jordan
Toby Aldape

$z \in \mathbb{Z}$ to $z \cdot 1_R$ (and in particular, $0 \in \mathbb{Z}$ to $0_R \in R$). Then ϕ is a ring homomorphism as it trivially respects all the ring operations. Note that if $g : X \to U(R)$ is another set map that induces the same homomorphism ϕ, then it must be that $f(x) = g(x)$ for all $x \in X$ so that $f = g$, so that this assignment is injective.

Now suppose that we are given a ring homomorphism $\phi : \mathbb{Z}[X] \to R$. Then define $f : X \to U(R)$ by mapping $x \mapsto \phi(x)$. This is clearly a function in **Set**, and this is exactly the f which induces ϕ, hence the assignment of ring homomorphisms to set functions is also surjective. Thus, we have the desired bijection so that $\mathbb{Z}[X]$ is indeed free.

By the universal property of the free commutative ring, for any commutative ring R any set function $X \to U(R)$ extends to a ring homomorphism $F(X) \to R$. In particular then, this is true for the identity map $id : U(R) \to U(R)$, that is, we have a commutative ring homomorphism $f : F(R) \to R$ extending the identity map. This map is surjective, as for each $r \in R$ there is a formal symbol $r' \in F(R)$ and we have that $f(r') = id(r) = r$. Thus we have shown that R is a homomorphic image of the integral domain $F(R)$, establishing the first claim.

Say the sentence $\forall x_1 \forall x_2 \ldots \forall x_n \phi(x_1, \ldots, x_n)$ where ϕ is positive and quantifier free is satisfied by all fields. Since the quantifier free sentence ϕ is true for all $x_1, \ldots, x_n$ in F it is true in particular for those $x_1, \ldots, x_n$ which fall in any subring, hence it is satisfied by any integral domain. Since the sentence is positive universal, it is preserved under any homomorphism[2]. Hence it is also true for any commutative ring, by the first claim. ■

Consider for instance, the Cayley-Hamilton Theorem. For fields F, this says that any square matrix over F satisfies its own characteristic polynomial. That is, for any $A \in Mat_n(F)$, $\chi_A(A) = 0$, consider $\chi_A(x)$, the characteristic polynomial of A given by

$$\chi_A(x) = \det(xI_n - A)$$

where I_n is the $n \times n$ identity matrix. Then, writing

$$\chi_A(x) = \Sigma_{i=0}^{n} k_i x^i$$

we have that

$$\Sigma_{i=0}^{n} k_i A^i = 0$$

where $A^0 = I_n$

To see that this statement is positive universal, note that for any $n \times n$ matrix A the statement $\chi_A(A) = 0$ amounts to a conjunction of n^2 equations, all of which are of the form "this sum of products of entries of $A = 0$", which is a positive statement. In general then, the Cayley-Hamilton Theorem says that for any choice of n^2 elements of the field F, a certain family of n^2 equations hold true.

We illustrate this in the case of 2×2 matrices over a field F. Suppose

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

[2]See *Model Theory* by Chang and Keisler, corollary 3.2.5

Ezzeddine El Sai
Howie Jordan
Toby Aldape

where $a, b, c, d \in F$. Then $\det(xI_n - A) = (x-a)(x-d) - bc = x^2 - (a+d)x + (ad-bc)$. Hence, Cayley-Hamilton is the claim that $A^2 - (a+d)A + (ad-bc)I_2 = 0$. Since

$$A^2 = \begin{bmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{bmatrix}$$

this amounts to statements $a^2 + bc - (a+d)a + (ad-bc) = 0$, $ab + bd - (a+d)b = 0$, $ac + cd - (a+d)c = 0$, and $bc + d^2 - (a+d)d + (ad-bc) = 0$. So the Cayley-Hamilton Theorem for 2×2 matrices of a field F is exactly the formal sentence

$$\begin{aligned} &(\forall a)(\forall b)(\forall c)(\forall d) \\ &\qquad ((a^2 + bc - (a+d)a + (ad-bc) = 0) \\ &\qquad \wedge (ab + bd - (a+d)b = 0) \\ &\qquad \wedge (ac + cd - (a+d)c = 0) \\ &\qquad \wedge (bc + d^2 - (a+d)d + (ad-bc) = 0)). \end{aligned}$$