MA 3G6 COMMUTATIVE ALGEBRA: INTEGRAL CLOSURE

DIANE MACLAGAN

Exercise 1. (1) Show that $\mathbb{C}[x]$ is integral over $\mathbb{C}[x^2]$.
(2) Show that $\mathbb{Z}[1/3]$ is not integral over $\mathbb{Z}$.
(3) Let $R = K[x]$, when K is a field, and let $f \in R$. Let $U = \{f^i : i \geq 0\}$. When is $R[U^{-1}]$ integral over R?

Solution:

(1) Let $f = \sum_{i=0}^{r} a_i x^i \in \mathbb{C}[x]$. Write $f_e = \sum_{i=0}^{\lfloor r/2 \rfloor} a_i x^i$, and $f_o = f - f_e$. We then have $f_e \in \mathbb{C}[x^2]$, and $f = f_e + f_o$. Note that $f_o^2 \in \mathbb{C}[x^2]$, so f satisfies the monic polynomial $(y - f_e)^2 - f_o^2 = y^2 - 2f_e y + (f_e^2 - f_o^2) = 0$, so f is integral over $\mathbb{C}[x^2]$.

(2) Suppose $1/3$ satisfied a monic equation $x^n + \sum_{i=0}^{n-1} a_i x^i$ with $a_i \in \mathbb{Z}$ for all i, so $(1/3)^n + \sum_{i=0}^{n-1} a_i (1/3)^i = 0$. Multiplying both sides by 3^n, we get $1 + \sum_{i=0}^{n-1} a_i 3^{n-i} = 0$. This reduces modulo 3 to $1 = 0$, which is a contradiction, so we conclude that $1/3$ is not integral over $\mathbb{Z}$.

(3) If $R[U^{-1}]$ is integral over R, then $1/f$ must satisfy a monic equation with coefficients in R: $(1/f)^n + \sum_{i=0}^{n-1} a_i (1/f)^i = 0$. Multiplying by f^n, we get the equation $1/1 + \sum_{i=0}^{n-1} a_i f^{n-i}/1 = 0/1$ in $R[U^{-1}]$. This implies that $1 = f(-\sum_{i=0}^{n-1} a_i f^{n-1-i})$). We are using here that R is a domain, so the map $R \to R[U^{-1}]$ is an injection. Thus f is must be a unit in R. This necessary condition also suffices, as if f is a unit we have $R[U^{-1}] \cong R$. The only units of $R = K[x]$ are the elements of K, so for any nonconstant polynomial f the localization $R[U^{-1}$ is not integral over R.

Exercise 2. Show that every element of $R[s_1, \ldots, s_m]$ can be written as a polynomial in the s_i with coefficients in R, and this subring contains all such polynomials.

Solution: Since $R[s_1, \ldots, s_m]$ is a subring containing R and $s_1, \ldots, s_m$, it must contain all products and sums of these elements, so must contain all polynomials in the s_i with coefficients in R. It thus suffices to observe that these elements form a subring, as the set of such polynomials is closed under addition, multiplication, and taking additive inverses.

Exercise 3. We have $\sqrt{2}$ and $\sqrt{3}$ both integral over $\mathbb{Z}$. Show directly that $\sqrt{2}+\sqrt{3}$ is integral over $\mathbb{Z}$ by giving the monic equation it satisfies. Repeat this with 2 and 3 replaced by your favourite smallish positive squarefree integers, and square roots replaced by larger roots. Note how much easier (thanks to the corollary of the Cayley-Hamilton theorem!) the proof of the last part of the theorem was than your computations.

Solution: One method is to write $x = \sqrt{2} + \sqrt{3}$, and then observe that $x^2 = 5 + 2\sqrt{6}$, so $(x^2 - 5)^2 = 24$, so $\sqrt{2} + \sqrt{3}$ satisfies the monic polynomial $x^4 - 10x^2 + 1 = 0$. This gets harder for more complicated expressions, and particularly for more complicated polynomials in radicals (such as $\sqrt{3}(\sqrt[5]{5}^2 - 7\sqrt[3]{3})^2 - 8\sqrt{11})$. One method to solve this in general is to use Gröbner bases: if p is a polynomial in radicals, we add an extra variable y for each radical $\sqrt[m]{a}$, replace the radicals in p by these variables, and consider the ideal generated by p and the expressions $y^m - a$. The required polynomial is the generator of the intersection of this ideal with the original polynomial ring.

Exercise 4. Let n be a squarefree integer (no divisible by m^2 for any integer m), and let $K = \mathbb{Q}(\sqrt{n})$. Let $\alpha = (1 + \sqrt{n})/2$ if $n \equiv 1 \mod 4$, and $\alpha = \sqrt{n}$ if $n \equiv 2$ or $3 \mod 4$ (the case $n \equiv 0 \mod 4$ is ruled out by the squarefree hypothesis). Show that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{n})$ is $\mathbb{Z}[\alpha]$.

Solution: We first prove the following lemma, which is of independent interest: If $h \in \mathbb{Z}[x]$ is a monic polynomial, and $h = fg$ with $f, g \in \mathbb{Q}[x]$ monic, then $f, g \in \mathbb{Z}[x]$. Indeed, suppose that m is the smallest common denominator of the coefficients of f, and n is the smallest common denominator of the coefficients of g, so the coefficients of $mf, ng \in \mathbb{Z}[x]$ each have no common factor. If one of m, n is not 1, let p be a prime factor of mn. Let i be the largest integer for which the coefficient of x^i in mf is not divisible by p, and let j be the corresponding integer for ng. These must exist, as the coefficients of mf and ng do not have a common factor. Write $mf = \sum_{l=0}^{r} a_l x^l$, and $ng = \sum_{q=0}^{s} b_q x^q$. Then the coefficient of x^{i+j} in $(mf)(ng) = mnh$ is $\sum_{(l,q):l+q=i+j} a_l b_q$. The term $a_i b_j$ of this sum is not divisible by p, but each other term is by the choice of i, j, as either $l > i$ or $q > j$. Thus this coefficient is not divisible by p. This contradicts the fact that $h \in \mathbb{Z}[x]$, so every coefficient of mnh is divisible by p. This completes the proof of the lemma.

Now, every element β of $\mathbb{Q}(\sqrt{n})$ can be written in the form $a+b\sqrt{n}$ for some $a, b \in \mathbb{Q}$. The element β is a root of the polynomial $(x-a)^2-b^2n = x^2 - 2ax + (a^2 - b^2n)$. If β satisfies a monic polynomial p with integral coefficients, then we can divide this by $x^2 - 2ax + (a^2 - b^2n)$ to see that either $x^2 - 2ax + (a^2 - b^2n)$ divides p, so β also satisfies a linear equation with rational coefficients, so $\beta \in \mathbb{Q}$. In the second case we must have $\beta \in \mathbb{Z}$ by the lemma of the first paragraph, so $b = 0$, $a \in \mathbb{Z}$. In the first case, we must have $x^2 - 2ax + (a^2 - b^2n) \in \mathbb{Z}[x]$, again by the lemma of the first paragraph.

Thus if β is integral over $\mathbb{Z}$ we must have $2a, a^2 - b^2n \in \mathbb{Z}$. If $a \in \mathbb{Z}$, then $2a \in \mathbb{Z}$. The assumption $a^2 - b^2n \in \mathbb{Z}$ then implies that $b^2n \in \mathbb{Z}$, so since n is squarefree we must have $b \in \mathbb{Z}$.

Otherwise we have $a = a'/2$ for some odd $a' \in \mathbb{Z}$. Since ${a'}^2/4-b^2n \in \mathbb{Z}$, we must also have $b = b'/2$ where b' is an odd integer. This implies that ${a'}^2-({b'}^2n \equiv 0$ modulo 4. Since a', b' are odd, we have ${a'}^2 \equiv {b'}^2 \equiv 1 \mod 4$, so $n \equiv 1 \mod 4$. Thus this case $(a = a'/2)$ does not happen unless $n \equiv 1 \mod 4$.

We thus conclude that if $n \equiv 2, 3 \mod 4$, then $a + b\sqrt{n}$ is integral over $\mathbb{Z}$ if and only if $a, b \in \mathbb{Z}$, so the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{n})$ is $\mathbb{Z}[\sqrt{n}]$. If $n \equiv 1 \mod 4$ then $a + b\sqrt{n}$ if integral over $\mathbb{Z}$ if and only if $2a, 2b \in \mathbb{Z}$, and $2a \equiv 2b \mod 2$. As $\sqrt{n} = 2(1 + \sqrt{2})/2$, all such elements are in $\mathbb{Z}[(1 + \sqrt{n})/2$, so this is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{n})$.

Exercise 5. We claim that C is nonsingular at all points $(a, b) \in C$ if and only if $\mathbb{C}[x, y]/\langle f\rangle$ is normal. Check this for the polynomial $f = x + y + 1$ (i.e., confirm that C is nonsingular at all points, and that $\mathbb{C}[x, y]/\langle f\rangle$ is integrally closed in its field of fractions).

Solution: We have $\partial f/\partial x = \partial f \partial y = 1$, so C is nonsingular at all points $(a, b) \in C = \{(a, b) \in \mathbb{C}^2 : a + b + 1 = 0\}$. We have $\mathbb{C}[x, y]/\langle x + y + 1\rangle \cong \mathbb{C}[x]$, so the field of fractions of $\mathbb{C}[x, y]/\langle f\rangle$ is isomorphic to $\mathbb{C}(x)$. If $g/h \in \mathbb{C}(x)$ is integral over $\mathbb{C}[x]$, where g, h are relatively prime, then $(g/h)^n + \sum_{i=0}^{n} a_i(g/h)^i = 0$ for some choices of $a_i \in \mathbb{C}[x]$, and so, clearing denominators, $g^n + \sum_{i=0}^{n} a_i g^i h^{n-i} = 0$. This shows that g^n is a multiple of h, so g and h must have a common factor, contradicting our assumption. We thus conclude that $\mathbb{C}[x]$ is integrally closed in its field of fractions, and thus so is $\mathbb{C}[x, y]/\langle x + y + 1\rangle$.