Commutative Algebra

D-MATH, HS 2014

Prof. Brent R. Doran

Solutions Sheet 6

1. As surjective homomorphisms are closed, it is enough to show the statement for the inclusion $\varphi(A) \subset B$. We are thus reduced to showing the exercise for φ being injective. Consider any ideal $\mathfrak{b} \subset B$. We claim that $\varphi^*(V(\mathfrak{b})) = V(A \cap \mathfrak{b})$, from which we deduce that φ^* is closed. The claim is equivalent to $\overline{\varphi}^*$ being surjective, where $\overline{\varphi}$ is the injective homomorphism $A/(\mathfrak{b} \cap A) \to B/\mathfrak{b}$ induced by φ. As φ is integral, also $\overline{\varphi}$ is integral. Surjectivity of $\overline{\varphi}^*$ is thus equivalent to the Going-up Lemma (Theorem 5.10 in A-M).

2. Let $f : A \longrightarrow \Omega$ be the homomorphism and $A \subset B$ with B integral over A. Let $\mathfrak{p}$ be the kernel of f. Since Ω is a field, this is a prime ideal. By the Going-up Lemma (Theorem 5.10 in A-M), there exists a prime ideal $\mathfrak{q}$ in B such that $\mathfrak{q} \cap A = \mathfrak{p}$. By replacing A with $A/\mathfrak{p}$ and B with $B/\mathfrak{q}$ we can reduce to the case where A is an integral domain and $f : A \longrightarrow \Omega$ is injective.

Let now $S = A \backslash \{0\}$. The map $f : A \longrightarrow \Omega$ factors through $A \longrightarrow S^{-1}A \longrightarrow \Omega$, and since there is a natural map $B \longrightarrow S^{-1}B$ it is enough to find an extension of $\bar{f} : S^{-1}A \longrightarrow \Omega$ to $S^{-1}B$. As localization preserves integrality (Proposition 5.6 in A-M), we have reduced to the case where A is a field.

So suppose A is a field, and $A \subset B$ is integral. Then by Proposition 5.7 in A-M, B is a field. Since B is integral over A, B is an algebraic field extension. It is generally true that for any algebraic field extension L/K and any embedding $f : K \longrightarrow \Omega$ into an algebraically closed field there exists an embedding $L \longrightarrow \Omega$ which extends it (see e.g. *Lang, Algebra* Part II. Theorem 2.8).

3. Let a be any element of A and consider the polynomial $\prod_{\sigma \in G}(t - \sigma(a)) \in A[t]$. This polynomial is in fact in $A^G[t]$ because all its coefficients are symmetric polynomial expressions in the $(\sigma(a))_{\sigma \in G}$ and therefore G-invariant. This shows that A is integral over A^G.
In the setting of the second part of this exercise, let $b \in B$ and $\sigma \in G$. As σ acts as the identity on A, any polynomial in $A[t]$ which has b as a root also has $\sigma(b)$ as a root. This shows $\sigma(B) \subset B$. Moreover, we have $A \subset B^G$ because $A \subset B$ and A is G-invariant. Conversely, any element of B^G lies in K, because the field extension is galois. It thus also lies in A, because A is integrally closed.

4. Let $f \in K[x]$ denote the minimal polynomial of a and let $g \in A[x]$ be a monic polynomial with $g(a) = 0$. The zeroes of g in some algebraic closure of L are therefore integral over A. As f divides g in $K[x]$, the same is true for the zeroes of f. Being polynomial expressions in these zeroes, the coefficients of f are therefore integral over A. As they lie in K and as A is integrally closed, they must lie in A.

5. (i) For the case where B is an integral domain we refer to Exercise 8 in Chapter 5 of A-M, whose hints serve as a proof. For a general B the same proof applies as long as any monic polynomial with coefficients in B has a zero in some over ring. But this is generally true and is proven in the same way as for fields: Let $f \in B[x]$ be monic. Consider the composition $B \to B[x] \to B[x]/(f)$. As f is monic, it is injective. Moreover, the image of x in $B[x]/(f)$ is a zero of f.

(ii) We refer to Exercise 9 of Chapter 5 in A-M, whose hints serve as an almost complete proof. The remaining subtlety is to show that the polynomials used to apply the previous exercise are monic. This, however, follows from the property of r being chosen larger than the degrees of $g_1, \ldots, g_m$ and f.

(iii) Let K denote the quotient field of A. We have the inclusion of rings $A[x] \subset K[x] \subset K(x)$. The first inclusion is integrally closed by part (ii) and because A is integrally closed. The second inclusion is integrally closed because $K[x]$ is factorial (Proposition 4.10 in Eisenbud). Therefore $A[x] \subset K(x)$ is integrally closed.

6. We closely follow the hints given in Eisenbud. For any integer n, we have that $\sqrt{n}$ is integral over $\mathbb{Z}$. Hence the integral closure of $\mathbb{Z}[\sqrt{n}]$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{n})$. For $n = k^2 m$, where k, m are also integers, we have $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}(\sqrt{m})$. Dividing n by its squares therefore does not change the resulting integral closure. We may therefore assume that n is square-free. Let R denote the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{n})$. Consider any element $\alpha = a + b\sqrt{n} \in \mathbb{Q}(\sqrt{n})$, where $a, b \in \mathbb{Q}$. Then its minimal polynomial is $x^2 + 2ax + a^2 - b^2 n$. By Exercise 4 we have $\alpha \in R$ if and only if $2a \in \mathbb{Z}$ and $a^2 - b^2 n \in \mathbb{Z}$. As $\mathbb{Z} \subset R$ we may only deal with the cases $a = 0$ and $a = \frac{1}{2}$. If $a = 0$, then $b^2 n =: m \in \mathbb{Z}$. Write $b = \frac{r}{s}$ for coprime $r, s \in \mathbb{Z}$. Hence $r^2 n = s^2 m$. As n is square-free, we find that s is a unit in $\mathbb{Z}$. Hence $a = 0$ implies $b \in \mathbb{Z}$. If $a = \frac{1}{2}$, then $\frac{1}{4} - b^2 n =: m \in \mathbb{Z}$. Writing again $b = \frac{r}{s}$ for coprime $r, s \in \mathbb{Z}$ we find $4r^2 n = s^2 - s^2 4m$. Thus s^2 divides $4n$. As n is square-free and because s is not a unit, $s = 2$. Hence $a = \frac{1}{2}$ implies $b \in \frac{1}{2}\mathbb{Z}$. If $a = \frac{1}{2}$, we have $\alpha \in R$ if and only if $\frac{1}{2} + \frac{1}{2}\sqrt{n} \in R$. This is because $\mathbb{Z}\sqrt{n} \subset R$ and because $b \neq 0$. But $\frac{1}{2} + \frac{1}{2}\sqrt{n} \in R$ if and only if $\frac{1}{4} + \frac{1}{4}n \in \mathbb{Z}$ which holds if and only if $n = 1 \ (mod\ 4)$. We conclude that $R = \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{n}]$ if $n = 1 \ (mod\ 4)$ and $R = \mathbb{Z}[\sqrt{n}]$ if $n \neq 1 \ (mod\ 4)$.