Part 1

Exercise 2.6

For any A-module, let $M[x]$ denote the set of all polynomials in x with coefficients in M, that is to say expressions of the form

$$m_0 + m_1 x + \cdots + m_r x^r \quad (m_i \in M).$$

Defining the product of an element of $A[x]$ and an element of $M[x]$ in the obvious way, show that $M[x]$ is an $A[x]$-module. Show that $M[x] \cong A[x] \otimes_A M$.

Observe that $M[x]$ is an abelian group, and let $\sum_{i=0}^k m_i x^i \in M[x]$ and $\sum_{i=0}^l a_i x^i \in A[x]$. Then

$$\left(\sum_{i=0}^{l} a_i x^i\right)\left(\sum_{i=0}^{k} m_i x^i\right) = \sum_{i=0}^{k+l} \sum_{r+s=i} a_r m_s x^i$$

is an element of $M[x]$ since for each i $\sum_{r+s=i} a_r m_s$ is in M, and furthermore this multiplication is associative and distributive since polynomial multiplication is associative and distributive. Thus $M[x]$ has the structure of an $A[x]$-module.

Now we will show that $M[x] \cong A[x] \otimes_A M$. For

$$\begin{aligned}
M \otimes_A A[x] &= M \otimes_A \left(\bigoplus_{i\in\mathbb{N}} Ax^i\right) \\
&\cong \bigoplus_{i\in\mathbb{N}} \left(M \otimes_A Ax^i\right) && \text{(Exercise 4, Assignment 2)} \\
&\cong \bigoplus_{i\in\mathbb{N}} Mx^i && (Ax^i \text{ is free over } i\text{, hence flat}) \\
&= M[x].
\end{aligned}$$

Exercise 5.3

> Let $f : B \to B'$ be a homomorphism of A-algebras, and let C be an A-algebra. If f is integral, prove that $f \otimes 1 : B \otimes_A C \to B' \otimes_A C$ is integral. (This includes (5.6) ii) as a special case.)

Since f is integral, for every $x \in B'$ there are $b_1, \ldots, b_n \in B$ such that

$$x^n + f(b_1)x^{n-1} + \cdots + f(b_{n-1})x + f(b_n) = 0.$$

Then given any $c \in C$, we have (writing $\otimes$ for $\otimes_A$)

$$\begin{aligned}
& (x \otimes c)^n + f \otimes 1(b_1 \otimes c)(x \otimes c)^{n-1} + \cdots + f \otimes 1(b_{n-1} \otimes c^{n-1})(x \otimes c) + f \otimes 1(b_n \otimes c^n) \\
= \ & x^n \otimes c^n + (f(b_1) \otimes c)(x^{n-1} \otimes c^{n-1}) + \cdots + (f(b_{n-1}) \otimes c)(x \otimes c^{n-1}) + f(b_n) \otimes c^n \\
= \ & x^n \otimes c^n + f(b_1)x^{n-1} \otimes c^n + \cdots + f(b_{n-1})x \otimes c^n + f(b_n) \otimes c^n \\
= \ & (x^n + f(b_1)x^{n-1} + \cdots + f(b_{n-1})x + f(b_n)) \otimes c^n \\
= \ & 0.
\end{aligned}$$

Thus $f \otimes 1$ is integral.

Exercise 5.8

> (i) Let A be a subring of an integral domain B, and let C be the integral closure of A in B. Let f, g be monic polynomials in $B[x]$ such that $fg \in C[x]$. Then f, g are in $C[x]$. [Take a field containing B in which the polynomials f, g split into linear factors: say $f = \prod(x - \xi_i)$, $g = \prod(x - \eta_i)$. Each ξ_i and each η_i is a root of fg, hence is integral over C. Hence the coefficients of f and g are integral over C.]
>
> (ii) Prove the same result without assuming that B (or A) is an integral domain.

We follow the hint.

(i) Identify B with its inclusion in its field of quotients k. Then there is a splitting field F of f and g containing k, hence containing B. Let f and g have the factorizations

$$f = \prod(x - \xi_i), \quad g = \prod(x - \eta_i).$$

Since $fg \in C[x]$ and C is the integral closure of A in B, each ξ_i and each η_i is a root of a monic polynomial with coefficients in C, hence integral over C. Since the integral closure of A in B (namely C) is integrally closed in B, this means that the ξ_i and η_i are *in* C. But each coefficient of f is a sum of products of the ξ_i, and each coefficient of g is a sum of products of the η_i. Since C is a ring, this means each coefficient of f and each coefficient of g is an element of C also. So $f \in C[x]$ and $g \in C[x]$.

(ii) Let $\mathfrak{b}$ be a prime ideal of B and let $\mathfrak{a} = A \cap \mathfrak{b}$ and $\mathfrak{c} = C \cap \mathfrak{b}$. Then $A/\mathfrak{a}$, $B/\mathfrak{b}$, and $C/\mathfrak{c}$ are integral domains, and by Proposition 5.6, $C/\mathfrak{c}$ is integral over $A/\mathfrak{a}$, hence a subring of the integral closure of $A/\mathfrak{a}$ in $B/\mathfrak{b}$. Since $f \cdot g \in C[x]$, reducing everything mod $\mathfrak{b}$ gives us $\widehat{f} \cdot \widehat{g} \in (C/\mathfrak{c})[x]$, where $\widehat{f}$ and $\widehat{g}$ are the reductions of f and g, respectively. Therefore by part (i) of this exercise, $\widehat{f}, \widehat{g} \in D[x]$, where D is the integral closure of $A/\mathfrak{a}$ in $B/\mathfrak{b}$. We wish to show $f, g \in C[x]$.

To see this, observe that nothing we have said so far depends on the choice of prime ideal $\mathfrak{b}$ of B. Thus we have proven that for *any* prime ideal $\mathfrak{b}$ of

B, the coefficients of $\widehat{f}$ and those of $\widehat{g}$ are integral over $A/\mathfrak{a}$. We will show that the coefficients are in fact in C. For suppose by way of contradiction that there is some $x \in B \setminus C$ such that $x + \mathfrak{b}$ is integral over $A/\mathfrak{a}$ for every prime ideal $\mathfrak{b}$ of B. Define

$$S = \{p(x) : p \in A[t] \text{ monic}\}.$$

Since $x \notin C$, x is not integral over A and so $0 \notin S$. Since also the product of two monic polynomials over A is a monic polynomial over A, S is a multiplicative submonoid of B. Thus by Lindenbaum's lemma,[1] $B \setminus S$ is a prime ideal of B; choose this as our prime ideal $\mathfrak{b}$. Then using the same notation as before, $x + \mathfrak{b}$ is integral over $A/\mathfrak{a}$. Then there is a monic polynomial over $A/\mathfrak{a}$ with $x + \mathfrak{b}$ as a root. But this is just to say that there is a monic polynomial over A which on x takes on a value in $\mathfrak{b} = B \setminus S$, which contradicts the definition of S.

[1] I am unsure of the name of this result, which is given as a parenthetical note in Example 1 on p.38 of the textbook. The name "Lindenbaum's lemma" is given to a family of similar facts in logic.

Exercise 5.9

Let A be a subring of B and let C be the integral closure of A in B. Prove that $C[x]$ is the integral closure of $A[x]$ in $B[x]$. [If $f \in B[x]$ is integral over $A[x]$, then

$$f^m + g_1 f^{m-1} + \cdots + g_m = 0 \quad (g_i \in A[x]).$$

Let r be an integer larger than m and the degrees of $g_1, \ldots, g_m$ and let $f_1 = f - x^r$, so that

$$(f_1 + x^r)^m + g_1(f_1 + x^r)^{m-1} + \cdots + g_m = 0$$

or say

$$f_1^m + h_1 f_1^{m-1} + \cdots + h_m = 0,$$

where $h_m = (x^r)^m + g_1(x^r)^{m-1} + \cdots + g_m \in A[x]$. Now apply Exercise 8 to the polynomials $-f_1$ and $f_1^{m-1} + h_1 f_1^{m-2} + \cdots + h_{m-1}$.]

Since $x \in C[x]$ and x is integral over $C[x]$; and since $C \subset C[x]$ and C is integral over $A[x]$ since it is integral over $A \subset A[x]$; and since the set of elements of $B[x]$ which are integral over $A[x]$ form a ring; and since every element of $C[x]$ can be built up from x and C by means of ring operations, it follows that every element of $C[x]$ is integral over $A[x]$. Therefore if $C[x]$ is integrally closed, then it is the integral closure of $A[x]$ in $B[x]$.

To that end, let $f \in B[x]$ be integral over $C[x]$. We will show that $f \in C[x]$. Let $g_1, \ldots, g_n \in C[x]$ be such that

$$f^n + g_1 f^{n-1} + \cdots + g_{n-1} f + g_n = 0.$$

Then

$$f^n + g_1 f^{n-1} + \cdots + g_{n-1} f = -g_n \in C[x],$$

so

$$f\left(f^{n-1} + g_1 f^{n-2} + \cdots + g_{n-1}\right) \in C[x]$$

and by Exercise 5.8 above, this implies $f \in C[x]$ as well, completing the proof.

Exercise 5.28

Let A be an integral domain, K its field of fractions. Show that the following are equivalent:

(1) A is a valuation ring of K;

(2) If $\mathfrak{a}$, $\mathfrak{b}$ are any two ideals of A, then either $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$.

Deduce that if A is a valuation ring and $\mathfrak{p}$ is a prime ideal of A, then $A_\mathfrak{p}$ and $A/\mathfrak{p}$ are valuation rings of their fields of fractions.

- (1)$\Rightarrow$(2). Let A be a valuation ring of K and $\mathfrak{a}, \mathfrak{b}$ be any two ideals of A, and suppose $\mathfrak{a} \not\subset \mathfrak{b}$, and suppose by way of contradiction that $\mathfrak{b} \not\subset \mathfrak{a}$. Then $\mathfrak{b} \neq 0$, so there is some $0 \neq b \in \mathfrak{b}$, and there is some $0 \neq a \in \mathfrak{a} \setminus \mathfrak{b}$. Then since A is a valuation ring of K, either $a/b \in A$ or $b/a \in A$. But $a/b \in A$ implies $(a/b)b \in \mathfrak{b}$, i.e. $a \in \mathfrak{b}$, which contradicts one of our hypotheses. But if on the other hand $b/a \in A$, then $(b/a)a \in \mathfrak{a}$, i.e. $b \in \mathfrak{a}$. But since this conclusion is independent of our choice of nonzero $b \in \mathfrak{b}$, it follows that $\mathfrak{b} \subset \mathfrak{a}$, which is a contradiction. We conclude therefore that if $\mathfrak{a} \not\subset \mathfrak{b}$, then $\mathfrak{b} \subset \mathfrak{a}$.

- (2)$\Rightarrow$(1). Let $0 \neq a, b \in A$. By hypothesis, either $(a) \subset (b)$ or $(b) \subset (a)$, so either $a = cb$ for some $c \in A$ or else $b = da$ for some $d \in A$. If the first case holds, then $c = a/b \in A$. Otherwise, $d = b/a \in A$. Since the choice of $a, b \neq 0$ was arbitrary, it follows that A is a valuation ring of K.

Now suppose A is a valuation ring and $\mathfrak{p}$ is a prime ideal of A. Then condition (2) above holds of A, and so condition (2) holds of $A_\mathfrak{p}$ since containment of ideals is a local property. Likewise, condition (2) holds of $A/\mathfrak{p}$ by the 1-1 order-preserving correspondence between ideals of A and ideals of $A/\mathfrak{p}$ of Proposition 1.1.

Exercise 5.30

Let A be a valuation ring of a field K. The group U of units of A is a subgroup of the multiplicative group K^* of K.
Let $\Gamma = K^*/U$. If $\xi, \eta \in \Gamma$ are represented by $x, y \in K$, define $\xi \geq \eta$ to mean $xy^{-1} \in A$. Show that this defines a total ordering on Γ which is compatible with the group structure (i.e., $\xi \geq \eta \Rightarrow \xi\omega \geq \eta\omega$ for all $\omega \in \Gamma$). In other words, Γ is a totally ordered abelian group. It is called the *value group* of A.
Let $v : K^* \to \Gamma$ be the canonical homomorphism. Show that $v(x + y) \geq \min(v(x), v(y))$ for all $x, y \in K^*$.

We show that $\geq$ is a total order.

- Reflexivity. Suppose $\xi \in \Gamma$ is represented by $x \in K$. Since $xx^{-1} = 1 \in A$, $\xi \geq \xi$.
- Transitivity. Suppose $\xi, \eta, \omega \in \Gamma$ are represented by $x, y, w \in K$, respectively, and that $\xi \geq \eta$ and $\eta \geq \omega$. Then $xy^{-1} \in A$ and $yz^{-1} \in A$, so

  $$xy^{-1}yz^{-1} = xz^{-1} \in A.$$

  Therefore $\xi \geq \omega$.
- Antisymmetry. Suppose $\xi, \eta \in \Gamma$ are represented by $x, y \in K$, respectively, and that $\xi \geq \eta$ and $\eta \geq \xi$. Then $xy^{-1} \in A$ and $yx^{-1} \in A$. But xy^{-1} and yx^{-1} are inverses, so xy^{-1} is a unit of A, hence of K; i.e. $xy^{-1} \in U$. This implies $\xi\eta^{-1} = xy^{-1}U = 1 \bmod U$, so ξ and η^{-1} are inverses, i.e. $\xi = \eta$.
- Totality. Suppose $\xi, \eta \in \Gamma$ are represented by $x, y \in K$, respectively. Since A is a valuation ring of K, either $xy^{-1} \in A$ or else $yx^{-1} = (xy^{-1})^{-1} \in A$, hence either $\xi \geq \eta$ or $\eta \geq \xi$.
- Compatibility with the group structure. Suppose $\xi, \eta, \omega \in \Gamma$ are represented by $x, y, w \in K$, respectively, and that $\xi \geq \eta$. Then $xy^{-1} = xww^{-1}y^{-1} = (xw)(yw)^{-1} \in A$. But this is just to say that $\xi\omega \geq \eta\omega$.

Now let $x, y \in K^*$ and let $v(x) = \xi$ and $v(y) = \eta$ and $v(x + y) = \omega$. Then we will show that $v(x + y) \geq \min\{v(x), v(y)\}$, i.e. that either $\omega \geq \xi$ or $\omega \geq \eta$. From the definition of $\geq$, this means that either $(x + y)x^{-1} = 1 + yx^{-1} \in A$ or else $(x + y)y^{-1} = 1 + xy^{-1} \in A$. But A is a valuation ring of K, so either $xy^{-1} \in A$ or else $(xy^{-1})^{-1} = yx^{-1} \in A$, hence either $1 + xy^{-1} \in A$ or else $1 + yx^{-1} \in A$. This completes the proof.

Part 3

Exercise 5.31, corrected

Let Γ be a totally ordered abelian group (written additively), and let K be a field. A *valuation of K with values in Γ* is a mapping $v : K^* \to \Gamma$ such that:

(1) $\quad v(xy) = v(x) + v(y)$ and

(2) $\quad v(x + y) \geq \min\{v(x), v(y)\}$

for all $x, y \in K^*$. Show that the set $A = \{0\} \cup \{x \in K^* \mid v(x) \geq 0\}$ is a valuation ring of K. This ring is called the *valuation ring of v*, and the subgroup $v(K^*)$ of Γ is the *value group of v*. Describe the maximal ideal of A.

First we show that A is a ring.

- $0 \in A$, and for any $y \in K^*$, $v(y) = v(1y) = v(1) + v(y)$. Thus $v(1) = 0$, so $1 \in A$.
- Suppose $a, b \in A$. Then $v(a + b) \geq \min\{v(a), v(b)\} \geq 0$, so $a + b \in A$.
- Suppose $a, b \in A$. Then $v(ab) = v(a) + v(b) \geq 0$, so $ab \in A$.
- Suppose $a \in A$. Then $a^2 \in A$, so
$$0 \leq v(a^2) = v(-a \cdot -a) = v(-a) + v(-a),$$
so $v(-a) \geq 0$ and $-a \in A$.
- A satisfies all the additional properties of a ring since it is a subset of K satisfying the above properties.

Next, suppose $x \in K^*$. We must show that either $x \in A$ or $x^{-1} \in A$. But $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$, so it cannot be the case that both $v(x) < 0$ and $v(x^{-1}) < 0$. Hence one of x, x^{-1} is in A.

Finally, the maximal ideal A is $\mathfrak{m} = \{x \in K^* \mid v(x) > 0\}$. It is an ideal by (1) and (2), and it is maximal because it is the set of all non-units of A. For if $a \in A$ is a unit then $0 = v(1) = v(aa^{-1}) = v(a) + v(a^{-1})$, and since $v(a), v(a^{-1}) \geq 0$ this implies $v(a) = v(a^{-1}) = 0$. And the reasoning here runs in reverse, so conversely $v(a) = 0$ implies a is a unit in A.

Part 4

Let A be the ring of all Gaussian integers with even imaginary parts, i.e., all $a + 2bi$, a and b integers, $i^2 = -1$. Prove that A is not integrally closed. What is the integral closure of A?

Observe that $\pm i \notin A$, since $\pm i = 0 \pm 1i$ has odd imaginary part. However, the monic polynomial $x^2 + 1 \in A[x]$ since its coefficients have imaginary part 0, and has roots $\pm i$. So i and $-i$ are integral over A but not in A. Thus A is not integrally closed.

Since i and A are both integral over A, every Gaussian integer is integral over A. Hence the ring G of all Gaussian integers is contained in the integral closure of A (in the field of fractions of A). But G is a UFD, hence integrally closed. So G is the integral closure of A.