Assignment number | due date       | Problems                           
-------------------|---------------|------------------------------------
1                  | Friday, Sept. 2 | 1.7, 1.16, 1.19, 1.20, 1.29, 1.30  
2                  | Friday, Sept. 9 | 1.43, 2.4, 2.5                     
3                  | Friday, Sept. 16| 2.16, 2.22, 2.25, 2.30, 2.33, 2.40 
4                  | Friday, Sept. 23| 3.29, 3.31, 3.42, 3.47             
5                  | Friday, Sept. 30| 3.50, 3.51, 3.53, 4.7, 4.8         

Contents

Homework grading scheme

Hints

Assignment 2

If \( f = \sum_{i=0}^{\infty} f_i, g = \sum_{i=0}^{\infty} g_i \in R[[X_1, \ldots, X_n]] \) then \( fg = \sum_{i=0}^{\infty} \left( \sum_{j=0}^{i} f_j g_{i-j} \right) \) (see Sharp p. 11). Hence, \( fg = 1 \) if and only if

\[
1 = f_0 g_0.
\]
0 = f_0 g_1 + f_1 g_0,
0 = f_0 g_2 + f_1 g_1 + f_2 g_0.

2.5 Use the binomial theorem, which is valid in any commutative ring \( R \): If \( x, y \in R \), and \( n \in \mathbb{N} \), then
\[
(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}, \quad \binom{n}{k} = \frac{n!}{k!(n-k)!}.
\]

2.22 It may be useful to use the (total) degree function \( \text{deg} : K[X_1, X_2] \rightarrow \mathbb{N} \) (see p. 9 of Sharp). This function satisfies \( \text{deg}(pq) = \text{deg}(p) + \text{deg}(q) \) for non-zero elements \( p \) and \( q \) of \( K[X_1, X_2] \).

Assignment 5

For Exercise 3.50 and Exercise 3.51 consider using Corollary 3.49. For Exercise 4.7 first read and understand Exercise 2.46. For Exercise 4.8 consider using Exercise 4.7.

Suggested solutions to selected problems

Assignment 1

1.16 Let \( R' \) be a commutative ring, and let \( \xi_1, \ldots, \xi_n \in R' \) be algebraically independent over the subring \( R \) of \( R' \). Let \( T \) be a commutative \( R \)-algebra with structural ring homomorphism \( f : R \rightarrow T \) and let \( \alpha_1, \ldots, \alpha_n \in T \). Show that there is exactly one ring homomorphism
\[
g : R[\xi_1, \ldots, x_n] \rightarrow T
\]
which extends \( f \) (that is, is such that \( g|_R = f \)) and is such that \( g(\xi_i) = \alpha_i \) for all \( i = 1, \ldots, n \).

Suggest solution: We begin with some notation. For \( \lambda = (i_1, \ldots, i_n) \in \mathbb{N}_0^n \) we will write
\[
\xi^\lambda = \xi_1^{i_1} \cdots \xi_n^{i_n}.
\]

With this notation every element \( p \) of \( R[\xi_1, \ldots, \xi_n] \) can be written uniquely in the form
\[
p = \sum_{\lambda \in \mathbb{N}_0^n} r_\lambda \xi^\lambda
\]
where \( r_\lambda \in R \) for \( \lambda \in \mathbb{N}_0^n \) and \( r_\lambda = 0 \) for all but finitely many \( \lambda \in \mathbb{N}_0^n \) (see 1.14). If
\[
q = \sum_{\lambda \in \mathbb{N}_0^n} s_\lambda \xi^\lambda
\]
is another element of $R[\xi_1, \ldots, \xi_n]$, then we have

$$p + q = \sum_{\lambda \in \mathbb{N}_0^n} (r_\lambda + s_\lambda) \xi^\lambda,$$

$$pg = \sum_{\lambda \in \mathbb{N}_0^n} \left( \sum_{\lambda_1, \lambda_2 \in \mathbb{N}_0, \lambda_1 + \lambda_2 = \lambda} r_{\lambda_1} s_{\lambda_2} \right) \xi^\lambda.$$

We now define

$$g : R[\xi_1, \ldots, x_n] \longrightarrow T$$

by

$$g(p) = \sum_{\lambda \in \mathbb{N}_0^n} f(r_\lambda) \alpha^\lambda$$

for $p$ as above; here, for $\lambda = (i_1, \ldots, i_n) \in \mathbb{N}_0^n$ we define $\alpha^\lambda = \alpha_1^{i_1} \cdots \alpha_n^{i_n}$. With $p$ and $q$ as above, and using that $f$ is a ring homomorphism, we have:

$$g(p + q) = g \left( \sum_{\lambda \in \mathbb{N}_0^n} (r_\lambda + s_\lambda) \xi^\lambda \right)$$

$$= \sum_{\lambda \in \mathbb{N}_0^n} f(r_\lambda + s_\lambda) \alpha^\lambda$$

$$= \sum_{\lambda \in \mathbb{N}_0^n} f(r_\lambda) \alpha^\lambda + \sum_{\lambda \in \mathbb{N}_0^n} f(s_\lambda) \alpha^\lambda$$

$$= g(p) + g(q).$$

And:

$$g(pq) = g \left( \sum_{\lambda \in \mathbb{N}_0^n} \left( \sum_{\lambda_1, \lambda_2 \in \mathbb{N}_0, \lambda_1 + \lambda_2 = \lambda} r_{\lambda_1} s_{\lambda_2} \right) \xi^\lambda \right)$$

$$= \sum_{\lambda \in \mathbb{N}_0^n} f \left( \sum_{\lambda_1, \lambda_2 \in \mathbb{N}_0, \lambda_1 + \lambda_2 = \lambda} r_{\lambda_1} s_{\lambda_2} \right) \alpha^\lambda$$

$$= \left( \sum_{\lambda \in \mathbb{N}_0^n} f(r_\lambda) \alpha^\lambda \right) \left( \sum_{\lambda \in \mathbb{N}_0^n} f(s_\lambda) \alpha^\lambda \right)$$

$$= g(p)g(q).$$

It is clear that $g(1) = 1$. It follows that $g$ is a ring homomorphism. It is also clear that $g$ extends $f$. Finally, to prove that $g$ has the required uniqueness property, assume that $h : R[\xi_1, \ldots, \xi_n] \rightarrow T$
is another right homomorphism such that $h|_R = f$ and $h(\xi_i) = \alpha_i$ for all $i = 1, \ldots, n$. Let $p$ be as above. We then have

$$h(p) = h\left(\sum_{\lambda \in \mathbb{N}_{0}^n} r_\lambda \xi^\lambda\right)$$

$$= \sum_{\lambda \in \mathbb{N}_{0}^n} h(r_\lambda) h(\xi^\lambda)$$

$$= \sum_{\lambda \in \mathbb{N}_{0}^n} f(r_\lambda) \alpha^\lambda$$

$$= g(p).$$

It follows that $h = g$.

**1.19** Let $K$ be an infinite field, let $\Lambda$ be a finite subset of $K$, and let $f \in K[X_1, \ldots, X_n]$, the ring of polynomials over $K$ in the indeterminates $X_1, \ldots, X_n$. Suppose that $f \neq 0$. Show that there exist infinitely many choices of

$$(\alpha_1, \ldots, \alpha_n) \in (K - \Lambda)^n$$

for which $f(\alpha_1, \ldots, \alpha_n) \neq 0$.

Suggest solution: We prove this by induction on $n$. The case $n = 1$ is clear because a non-zero polynomial in one variable over $K$ has finitely many distinct roots and $K - \Lambda$ is infinite. Assume that $n > 1$ and that the statement holds for $n - 1$; we will prove that it holds for $n$. There exists a non-negative integer $N$ such that

$$f(X_1, \ldots, X_n) = \sum_{k=0}^{N} f_k(X_1, \ldots, X_{n-1}) X_n^k$$

where $f_k(X_1, \ldots, X_{n-1}) \in K[X_1, \ldots, X_{n-1}]$ for $k = 1, \ldots, N$, and $f_N(X_1, \ldots, X_{n-1})$ is non-zero. By the induction hypothesis, there exists $(\alpha_1, \ldots, \alpha_{n-1}) \in (K - \Lambda)^{n-1}$ such that $f_N(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$. Consider the polynomial

$$g(X_n) = f(\alpha_1, \ldots, \alpha_{n-1}, X_n) = \sum_{k=0}^{N} f_k(\alpha_1, \ldots, \alpha_{n-1}) X_n^k$$

in the variable $X_n$. This polynomial is non-zero because $f_N(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$. By the case $n = 1$, there exist infinitely many $\alpha_n \in K - \Lambda$ such that $g(\alpha_n) \neq 0$, i.e., $f(\alpha_1, \ldots, \alpha_n) \neq 0$; moreover, for any such $\alpha_n$ we have $(\alpha_1, \ldots, \alpha_n) \in (K - \Lambda)^n$. This proves the statement for $n$. 
Assignment 2

1.43 Let $R$ be a commutative ring, and consider the ring $R[[X_1,\ldots,X_n]]$ of formal power series over $R$ in indeterminates $X_1,\ldots,X_n$. Let

\[ f = \sum_{i=0}^{\infty} f_i \in R[[X_1,\ldots,X_n]], \]

where $f_i$ is either zero or a homogeneous polynomial of degree $i$ in $R[X_1,\ldots,X_n]$ (for each $i \in \mathbb{N}_0$).

Prove that $f$ is a unit of $R[[X_1,\ldots,X_n]]$ if and only if $f_0$ is a unit of $R$.

Suggested solution: Assume that $f$ is a unit. Let $g \in R[[X_1,\ldots,X_n]]$ be such that $fg = 1$. Let $g = \sum_{i=0}^{\infty} g_i$ be the standard representation of $g$. Now

\[
fg = \sum_{i=0}^{\infty} \left( \sum_{j=0}^{i} f_j g_{i-j} \right)
\]

and this expression is the standard representation of $fg$ in $R[[X_1,\ldots,X_n]]$. Since $fg = 1$ we must therefore have

\[ 1 = f_0 g_0 \quad \text{and} \quad 0 = \sum_{j=0}^{i} f_j g_{i-j} \quad \text{for } i > 0. \]

In particular, we see that $f_0 g_0 = 1$, i.e., $f_0$ is a unit. Now assume that $f_0$ is a unit. We inductively define a sequence $(g_i)_{i \in \mathbb{N}_0}$ by setting $g_0 = f_0^{-1}$, and for $i > 0,$

\[ g_i = -f_0^{-1} \left( \sum_{j=1}^{i} f_j g_{i-j} \right). \]

Evidently, each $g_i$ is either zero or a homogeneous polynomial of degree $i$ in $R[X_1,\ldots,X_n]$. Also, we have $f_0 g_0 = 1$ and for $i > 0,$

\[ 0 = \sum_{j=0}^{i} f_j g_{i-j}. \]

Now define

\[ g = \sum_{i=0}^{\infty} g_i. \]

Then $g$ is in $R[[X_1,\ldots,X_n]]$, and this is the standard representation of $g$. Using the above formula for $fg$ we see that $fg = 1$.

Assignment 3

2.22 Let $K$ be a field. Show that the ideal $(X_1, X_2)$ of the commutative ring $K[X_1, X_2]$ (of polynomials over $K$ in indeterminates $X_1, X_2$) is not principal.

Assume that $(X_1, X_2) = (f)$ for some $f \in K[X_1, X_2]$; we will obtain a contradiction. Since
$X_1, X_2 \in (f)$, there exist $g_1, g_2 \in K[X_1, X_2]$ such that

$$X_1 = g_1f, \quad X_2 = g_2f.$$ 

Applying the degree function to the first equation we obtain

$$\deg(X_1) = \deg(g_1f)$$

$$1 = \deg(g_1) + \deg(f).$$

Similarly,

$$1 = \deg(g_2) + \deg(f).$$

Since $\deg(f), \deg(g_1), \text{ and } \deg(f)$ are in $\mathbb{N}_0$, we must have $\deg(f) = 0$ or $\deg(f) = 1$. Assume first that $\deg(f) = 0$. Then $f \in K$. Moreover, since $f \neq 0$ (otherwise $X_1 = 0$ and $X_2 = 0$, which is impossible), $f$ is a unit in $K$ and hence a unit in $K[X_1, X_2]$. Now $f \in (X_1, X_2)$. Hence, there exist $h_1, h_2 \in K[X_1, X_2]$ such that

$$f = h_1X_1 + h_2X_2.$$ 

Evaluating both sides at $X_1 = 0$ and $X_2 = 0$, we obtain $f = 0$, a contradiction (recall that we just showed that $f$ is a non-zero constant). Hence, $\deg(f) = 1$. It follows that $\deg(g_1) = \deg(g_2) = 0$, so that $g_1, g_2 \in K$. Again, we see that $g_1$ and $g_2$ are non-zero and are hence units in $K$ and hence units in $K[X_1, X_2]$. Now

$$X_1 = g_1f = g_1g_2^{-1}g_2f = g_1g_2^{-1}X_2.$$ 

That is,

$$X_1 = (g_1g_2^{-1})X_2.$$ 

Evaluating both sides at $X_1 = 1$ and $X_2 = 0$, we obtain $1 = 0$, a contradiction.

2.30 Let $I, J$ be ideals of the commutative ring $R$. Show that

$$\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}.$$ 

Let $r \in \sqrt{IJ}$. Then there exists $n \in \mathbb{N}$ such that $r^n \in IJ$. Since $IJ \subseteq I \cap J$ we have $r^n \in I \cap J$. Hence, $r \in \sqrt{I \cap J}$. It follows that

$$\sqrt{IJ} \subseteq \sqrt{I \cap J}.$$ 

Let $r \in \sqrt{I \cap J}$. Then there exists $n \in \mathbb{N}$ such that $r^n \in I \cap J$. Since $I \cap J \subseteq I$ and $I \cap J \subseteq J$ we have $r \in \sqrt{I}$ and $r \in \sqrt{J}$. Thus, $r \in \sqrt{I} \cap \sqrt{J}$. It follows that

$$\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}.$$ 

Let $r \in \sqrt{I} \cap \sqrt{J}$. Then there exist $m, n \in \mathbb{N}$ such that $r^m \in I$ and $r^n \in J$. Hence, $r^{mn} = r^m r^n \in IJ$. 

6
so that \( r \in \sqrt{IJ} \). It follows that
\[
\sqrt{I} \cap \sqrt{J} \subseteq \sqrt{IJ}.
\]
We have proven that
\[
\sqrt{IJ} \subseteq \sqrt{I} \cap \sqrt{J} \subseteq \sqrt{I} \cap \sqrt{J} \subseteq \sqrt{IJ}.
\]
This implies that
\[
\sqrt{IJ} = \sqrt{I} \cap \sqrt{J} = \sqrt{I} \cap \sqrt{J}.
\]

**Assignment 4**

3.29 Determine the prime ideals of the ring \( \mathbb{Z}/60\mathbb{Z} \) of residue classes of integers modulo 60.

By 3.28, every prime ideal of \( \mathbb{Z}/60\mathbb{Z} \) is of the form \( P/60\mathbb{Z} \) where \( P \) is a prime ideal of \( \mathbb{Z} \) such that \( 60\mathbb{Z} \subseteq P \). By 3.34, every prime ideal \( P \) of \( \mathbb{Z} \) such that \( 60\mathbb{Z} \subseteq P \) is of the form \( P = p\mathbb{Z} \), where \( p \) is a prime of \( \mathbb{Z} \) such that \( 60\mathbb{Z} \subseteq p\mathbb{Z} \), i.e., \( p \mid 60 \). It follows that the prime ideals of \( \mathbb{Z}/60\mathbb{Z} \) are \( 2\mathbb{Z}/60\mathbb{Z} \), \( 3\mathbb{Z}/60\mathbb{Z} \), and \( 5\mathbb{Z}/60\mathbb{Z} \).

3.31 Let \( R \) be an integral domain. Recall that for \( a_1, \ldots, a_n \in R \), where \( n \in \mathbb{N} \), a greatest common divisor (GCD for short) or highest common factor of \( a_1, \ldots, a_n \) is an element \( d \) of \( R \) such that
(i) \( d \mid a_i \) for all \( i = 1, \ldots, n \), and
(ii) whenever \( c \in R \) is such that \( c \mid a_i \) for all \( i = 1, \ldots, n \), then \( c \mid d \).

Show that every non-empty finite set of elements in a PID has a GCD.

Assume that \( R \) is a PID, and let \( a_1, \ldots, a_n \in R \). Consider the ideal \( (a_1, \ldots, a_n) \). Since \( R \) is a PID, there exists \( d \in R \) such that \( (a_1, \ldots, a_n) = (d) \). We claim that \( d \) is a GCD of \( a_1, \ldots, a_n \). Since \( a_1, \ldots, a_n \in (a_1, \ldots, a_n) = (d) \), we see that \( d \mid a_i \) for \( i = 1, \ldots, n \). Assume that \( c \in R \) is such that \( c \mid a_i \) for \( i = 1, \ldots, n \). Let \( r_j \in R \) be such that \( a_i = r_i c \) for \( i = 1, \ldots, n \). Also, let \( x_1, \ldots, x_n \) be such that \( x_1 a_1 + \cdots + x_n a_n = d \); note that \( x_1, \ldots, x_n \) exist because \( d \in (a_1, \ldots, a_n) \). Then
\[
d = x_1 a_1 + \cdots + x_n a_n = x_1 r_1 c + \cdots + x_n r_n c = (x_1 r_1 + \cdots + x_n r_n)c.
\]
Thus, \( c \mid d \).

3.42 Show that an irreducible element in a unique factorization domain \( R \) generates a prime ideal of \( R \).

Let \( r \in R \) be irreducible. Then by definition \( r \) is non-zero and not a unit. Since \( r \) is not a unit we have \( (r) \not\subseteq R \) (otherwise, \( 1 \in (r) \) so that \( r \) is a unit). Let \( a, b \in R \) be such that \( ab \in (r) \); to prove that \( (r) \) is a prime ideal it will suffice to prove that \( a \in (r) \) or \( b \in (r) \). If \( a = 0 \) or \( b = 0 \), then clearly \( a \in (r) \) or \( b \in (r) \); we may thus assume that \( a \neq 0 \) and \( b \neq 0 \). If \( a \) or \( b \) is a unit, then also \( a \in (r) \) or \( b \in (r) \); we may thus also assume that \( a \) and \( b \) are non-units. Since \( ab \in (r) \), there exists \( s \in R \) such that \( ab = rs \). Since \( R \) is an integral domain we have \( rs = ab \neq 0 \); also, \( rs \) is not a unit (otherwise \( (r) \) contains a unit, contradicting \( (r) \not\subseteq R \)). As \( R \) is a UFD, there exist irreducible
elements \( p_1, \ldots, p_k, q_1, \ldots, q_\ell, y_1, \ldots, y_n \) in \( R \) such that

\[
a = p_1 \cdots p_k, \quad b = q_1 \cdots q_\ell, \quad rs = y_1 \cdots y_n;
\]

Since \( r \) is irreducible, we may assume that \( y_1 = vr \) for some unit \( v \) in \( R \). Since \( ab = rs \) we have

\[
p_1 \cdots p_k q_1 \cdots q_\ell = vry_2 \cdots y_n.
\]

Since \( r \) is irreducible and \( R \) is a UFD, there exists a unit \( u \) in \( R \) such that \( r = up_i \) for some \( i \in \{1, \ldots, k\} \) or \( r = uq_j \) for some \( j \in \{1, \ldots, \ell\} \). Hence, \( p_i \in (r) \) for some \( i \in \{1, \ldots, k\} \) or \( q_j \in (r) \) for some \( j \in \{1, \ldots, \ell\} \) (recall that \( u \) is a unit, so that \( p_i = u^{-1}r \) or \( q_j = u^{-1}r \)). This implies that \( a \in (r) \) or \( b \in (r) \), as desired.

**3.47** Let \( P \) be a prime ideal of the commutative ring \( R \). Show that \( \sqrt{P^n} = P \) for all \( n \in \mathbb{N} \).

Let \( n \in \mathbb{N} \). Let \( x \in \sqrt{P^n} \). Then there exits \( m \in \mathbb{N} \) such that \( x^m \in P^n \). Now \( P^n \subseteq P \). Hence, \( x^m \in P \). Since \( P \) is prime we have \( x \in P \). This proves that \( \sqrt{P^n} \subseteq P \). Let \( x \in P \). Then \( x^n \in P^n \). Therefore, \( x \in \sqrt{P^n} \). This proves that \( P \subseteq \sqrt{P^n} \). We conclude that \( P = \sqrt{P^n} \).