Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 20, 2020

Problems in Section 3.11.

1. Prove that $R[x]$ is a commutative ring with unit element whenever R is.

Proof. Let $p(x), q(x) \in R[x]$. We can write $p(x)$ and $q(x)$ as

$$p(x) = a_0 + a_1x + \cdots + a_nx^n, \quad q(x) = b_0 + b_1x + \cdots + b_mx^m$$

where $a_i, b_j \in R$, $a_n, b_m \neq 0$, $a_{n+1} = a_{n+2} = \cdots = a_t = a_{t+1} \cdots = 0$ and $b_{m+1} = b_{m+2} = \cdots = b_t = b_{t+1} = \cdots = 0$. Consequently,

$$p(x) + q(x) = c_0 + c_1x + \cdots c_tx^t$$

where for each valid i, $c_i = a_i+b_i \in R$. Thus, $p(x)+q(x) \in R[x]$. Additive identity is clearly 0. Inverse element for $p(x)$ can be defined as $-p(x) = (-a_0)+(-a_1)x+\cdots(-a_n)x^n \in R[x]$. Now for the multiplication,

$$p(x)q(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$$

where $c_i = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0$. Clearly, $c_i \in R$ and hence $p(x)q(x) \in R[x]$. Suppose $q(x)p(x) = d_0+d_1x+\cdots+d_{n+m}x^{n+m}$. Then $d_i = b_0a_i+b_1a_{i-1}+\cdots+b_{i-1}a_1+b_ia_0 = a_ib_0 + a_{i-1}b_1 + \cdots + a_1b_{i-1} + a_0b_i = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0 = c_i$ so that $p(x)q(x) = q(x)p(x)$ and hence $R[x]$ is commutative. The unit element 1 is clearly in $R[x]$. For the distributive property, $t(x)(p(x)+q(x))$ where $t(x) = t_0 + t_1x + t_kx^k$. Observe that

$$\begin{aligned} r(x)(p(x)+q(x)) &= r(x)(c_0 + c_1 + \cdots c_tx^t) \\ &= e_0 + e_1x + \cdots e_{k+t}x^{k+t} \end{aligned}$$

where $e_i = r_0c_i + r_1c_{i-1} + \cdots + r_ic_0 = r_0(a_i+b_i) + r_1(a_{i-1}+b_{i-1}) + \cdots r_i(a_0+b_0)$. In other side,

$$\begin{aligned}
r(x)p(x)+r(x)q(x) &= ((r_0a_0)+(r_0a_1+r_1a_0)x+\cdots(r_0a_{t+k}+r_1a_{t+k-1}+\cdots r_{t+k}a_0)x^{t+k}) \\
&\quad +((r_0b_0)+(r_0b_1+r_1b_0)x+\cdots(r_0b_{t+k}+t_1b_{t+k-1}+\cdots r_{t+k}b_0)x^{t+k}) \\
&= r_0(a_0+b_0)+(r_0(a_1+b_1)+r_1(a_0+b_0))x+\cdots+(r_0(a_i+b_i)+r_1(a_{i-1}+b_{i-1}))+\cdots \\
&\quad +r_i(a_0+b_0))x^i+\cdots+(r_0(a_{t+k}+b_{t+k})+r_1(a_{t+k-1}+b_{t+k-1}))+\cdots r_{t+k}(a_0+b_0))x^{t+k} \\
&= r_0c_0+(r_0c_1+r_1c_0)x+\cdots(r_0c_i+r_1c_{i-1}+\cdots+r_ic_0)x^i+ \\
&\quad \cdots+(r_0c_{t+k}+r_1c_{t+k-1}+\cdots r_{t+k}c_0)x^{t+k} \\
&= e_0+e_1x+\cdots e_ix^i+\cdots+e_{t+k}x^{t+k}=r(x)(p(x)+q(x)).
\end{aligned}$$

Therefore, the distributive property is verified. The other distributive property also holds clearly. Thus, $R[x]$ is also a ring with unit element whenever R is. □

2. Prove that $R[x_1,\cdots,x_n]=R[x_{i_1},\cdots,x_{i_n}]$, where $(i_1,\cdots,i_n)$ is a permutation of $(1,2,\cdots,n)$.

Proof. Note that every elements $f(x_1,\cdots,x_n)$ in $R[x_1,\cdots,x_n]$ is of the form

$$f(x_1,\cdots,x_n)=\sum_{j=1}^{n} a_{j_1,j_2,\cdots,j_n}x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}.$$

For any permutation $(i_1,i_2,\cdots,i_n)$,

$$x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}=x_{i_1}^{j_{i_1}}x_{i_2}^{j_{i_2}}\cdots x_{i_n}^{j_{i_n}}$$

so that

$$f(x_1,\cdots,x_n)=\sum_{j=1}^{n} a_{j_1,j_2,\cdots,j_n}x_{i_1}^{j_{i_1}}x_{i_2}^{j_{i_2}}\cdots x_{i_n}^{j_{i_n}}\in R[x_{i_1},\cdots,x_{i_n}].$$

The opposite inclusion can be shown by the same method above. Thus $R[x_1,\cdots,x_n]=R[x_{i_1},\cdots,x_{i_n}]$. □

3. If R is an integral domain, prove that for $f(x)$, $g(x)$ in $R[x]$, $deg(f(x)g(x))=deg(f(x)+deg(g(x))$.

Proof. Same method for the proof of Lemma 3.9.1 can be used here. □

4. If R is an integral domain with unit element, prove that any unit in $R[x]$ must already be a unit in R.

Proof. Suppose $f(x)$ is an unit in $R[x]$. Then there is $q(x) \in R[x]$ such that $f(x)g(x) = 1$. Consequently, $deg(f(x)g(x)) = deg(f(x)) + deg(g(x)) = 0$, implying $deg(f(x)) = deg(g(x)) = 0$ so that $f(x) = a$, $g(x) = b$ for some $a, b \in R$. Recall that $ab = 1$. Thus $f(x) = a$ is an unit in R. $\square$

5. Let R be a commutative ring with no nonzero nilpotent elements(that is, $a^n = 0$ implies $a = 0$). If $f(x) = a_0 + a_1x + \cdots + a_mx^m$ in $R[x]$ is a zero divisor, prove that there is an element $b \neq 0$ in R such that $ba_0 = ba_1 = \cdots = ba_m = 0$.

Proof. We assume that $a_m \neq 0$. Since $f(x) \in R[x]$ is a zero-divisor, there is $g(x) = b_0 + b_1x + \cdots + b_nx^n \in R[x]$, $b_n \neq 0$ such that $f(x)g(x) = 0$. Suppose $f(x)g(x) = c_0 + c_1x + \cdots c_tx^t$. Then

$$c_{m+n} = a_mb_n, \quad c_{m+n-1} = a_{m-1}b_n + a_mb_{n-1}, \quad \cdots \quad c_1 = a_1b_0 + a_0b_1, \quad c_0 = a_0b_0.$$

Since $c_i = 0$ for all i, $c_{m+n} = a_mb_n = 0$. Observe that

$$\begin{aligned} 0 = c_{m+n-1} \cdot b_n &= (a_{m-1}b_n + a_mb_{n-1})b_n \\ &= a_{m-1}b_n^2 + (a_mb_n)b_{n-1} \\ &= a_{m-1}(b_n)^2 \end{aligned}$$

so that $a_{m-1}(b_n)^2 = 0$. Similarly,

$$\begin{aligned} 0 = c_{m+n-2} \cdot b_n^2 &= (a_{m-2}b_n + a_{m-1}b_{n-1} + a_mb_{n-2})b_n^2 \\ &= a_{m-2}b_n^3 + (a_{m-1}b_n^2)b_{n-1} + (a_mb_n)b_nb_{n-2} \\ &= a_{m-2}(b_n)^3 \end{aligned}$$

so that $a_{m-2}(b_n)^3 = 0$. Hence, we can inductively find that $a_{m-k}(b_n)^{k+1} = 0$ for all $k = 0, 1, 2, \cdots m$. Now we know that R has no nonzero nilpotent elements. Thus, $b_n^{m+1} \neq 0$. Let $b = b_n^{m+1}$. It is now clear that $a_{m-k}b = a_{m-k}(b_n^{k+1})(b_n^{m-k}) = 0$ for all k. $\square$

6. Do Problem 5 dropping the assumption that R has no nonzero nilpotent elements.

Proof. We prove that if $f(x) = a_0 + a_1x + \cdots + a_mx^m$ is a zero-divisor of $R[x]$, there is $r \neq 0 \in R[x]$ such that $rf(x) = 0$. Suppose not, then there exists a non-constant polynomial $g(x) = b_0 + b_1x + \cdots + b_kx^k$ of lowest degree in $R[x]$. Note that there is coefficient a_i of highest degree such that $a_ig(x) \neq 0$, otherwise $b_kf(x) = 0$, a contradiction. So we have

$$f(x)g(x) = (a_0 + a_1x + \cdots + a_ix^i)(b_0 + b_1x + \cdots + b_kx^k) = 0.$$

Hence $a_ib_k = 0$, so that $deg(a_ig(x)) < k$. Consequently, $f(x)(a_ig(x)) = a_if(x)g(x) = 0$ but $a_ig(x)$ is a polynomial of degree less than $g(x)$. This contradicts the definition of $g(x)$. Therefore, there exists $r \neq 0 \in R$ such that $rf(x) = 0 \iff ra_0 = ra_1 \cdots = ra_n = 0$. $\square$

7. If R is a commutative ring with unit element, prove that $a_0 + a_1 x + \cdots + a_n x^n$ in $R[x]$ has an inverse in $R[x]$(i.e., is a unit in $R[x]$) if and only if a_0 is a unit in R and $a_1, \cdots, a_n$ are nilpotent elements in R.

Proof. We first introduce a lemma.

Lemma. Let x and y be nilpotent elements in a commutative ring R with unit element. Then $x + y$ is also nilpotent. Further, for $r \in R$, rx is nilpotent. That is, collection of nilpotent elements form an ideal in R. Moreover, $1 + x$ is an unit in R. Hence, sum of an unit and nilpotent element is an unit in R.
(*claim*) Suppose m and n are the integers satisfying $x^m = y^n = 0$. Then

$$\begin{aligned}(x+y)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k} &= (y^{m+n} + xy^{m+n-1} + \cdots + x^{m-1}y^{n+1} \\ &+ x^m y^n + x^{m+1}y^{n-1} + \cdots + x^{m+n-1}y + x^{m+n}) = 0\end{aligned}$$

so that $x + y$ is nilpotent in R. Also, for any $r \in R$, $(rx)^m = r^m x^m = 0$ so that rx is also nilpotent in R. Now, we claim that $1 + x$ is an unit in R. Observe that

$$\begin{aligned}(1+x)(1 - x + x^2 + \cdots + (-1)^{m-1}x^{m-1}) &= 1 - x + x^2 + \cdots + (-1)^{m-1}x^{m-1} \\ &\quad + x - x^2 + \cdots + (-1)^{m-1}x^m \\ &= 1 + (-1)^{m-1}x^m = 1\end{aligned}$$

so that $1 + x$ is clearly an unit in R. Now we prove that sum of an unit and nilpotent element is an unit. Let u be an unit of R. Then $uu' = 1$ for some $u' \in R$. Consequently, $(u + x)u' = 1 + xu'$. Recall that xu' is nilpotent. Thus, $(u + x)u'$ is an unit in R. Thus, $(u + x)u'v = (u + x)(u'v) = 1$ for some $v \in R$. Therefore, $u + x$ is also an unit in R.

Now we head to our problem. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a unit in $R[x]$. That is, there is $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ such that

$$f(x)g(x) = (a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m) = 1.$$

Clearly, this implies that

$$a_0 b_0 = 1, \quad a_0 b_1 + a_1 b_0 = 0, \cdots, a_{n-1}b_m + a_n b_{m-1} = 0, \quad a_n b_m = 0.$$

From above, we know that a_0 is an unit in R. Further, without loss of generality, we can assume that $a_n \neq 0$. We shall now claim that $a_n^{r+1} b_{m-r} = 0$ for all $r = 0, 1, \cdots m$. For $r = 0$, it is trivial. Observe that

$$0 = a_n(a_{n-1}b_m + a_n b_{m-1}) = 0 + a_n^2 b_{m-1} \implies a_n^2 b_{m-1} = 0.$$

We can repeat this process and inductively get the required result of $a_n^{r+1}b_{m-r} = 0$ for all $r = 0, 1, \cdots m$. But note that since $a_0b_0 = 1$, $a_n^{m+1}a_0b_0 = a_n^{m+1} \cdot 1 = a_0(a_n^{m+1}b_0) = 0$. Hence a_n is nilpotent. From the lemma we established, $f(x) - a_nx^n$ is a sum of unit and nilpotent element, so that it is now an unit. So we can repeat the same process to obtain that each of $a_{n_1}, a_{n-2}, \cdots, a_1$ are, in fact, nilpotent.
Conversely, assume that a_0 is an unit and $a_i, i \geq 1$ is nilpotent. Given the fact that sum of an unit and nilpotent element is an unit, $a_0 + a_1x$ is also an unit. So inductively, we can conclude that $f(x) = a_0 + a_1x + \cdots + a_nx^n$ is also an unit in R. □

8. Prove that when F is a field, $F[x_1, x_2]$ is not a principal ideal ring.

Proof. We claim that (x_1, x_2) is not a principal ideal. For the sake of contradiction, assume that $(x_1, x_2) = (p)$ for some polynomial p in $F[x_1, x_2]$. Then there exists polynomials $q_1, q_2 \in F[x_1, x_2]$ such that $pq_1 = x_1$, $pq_2 = x_2$. Note that from $pq_1 = x_1$, since F is a field, p must have non-zero coefficient of x_1 and from $pq_2 = x_2$, q_2 has non-zero constant term so that pq_2 has non-zero coefficient of x_1, which contradicts that $pq_2 = x_2$. Hence, (x_1, x_2) is not a principal ideal. □

9. Prove, completely, Lemma 3.11.2 and its corollary.

Proof. By the definition of Unique Factorization Domain(in short, UFD), for any non-unit $a, b \in R$,

$$\begin{aligned} a &= q_1q_2 \cdots q_n, \\ b &= q_1'q_2' \cdots q_m' \end{aligned}$$

where q_i, q_j's are irreducibles in R. Now we re-order the irreducibles of a and b such that

$$\begin{aligned} a &= (q_1q_2 \cdots q_k) \cdot q_{k+1} \cdots q_n, \\ b &= (q_1'q_2' \cdots q_k') \cdot q_{k+1}' \cdots q_m' \end{aligned}$$

where each $q_i, 1 \leq i \leq k \leq \min\{n, m\}$ is associate with q_i', and none of $q_i, i \geq k+1$ is associate with $q_j', j \geq k+1$. Let $d = q_1q_2 \cdots q_k$. We claim that $d = (a, b)$. It is clear that $d \mid a$ and $d \mid b$. Suppose c is also a common divisor of a and b. As R is an UFD, c is also a product of irreducibles of R. Suppose $c \nmid d$. Then there exists an irreducible y such that y divides one of $q_i, i \geq k+1$ and $q_j', j \geq k+1$. This forces us to conclude that y is either an unit or q_i and q_j are not irreducibles. But either of the cases leads to contradiction. Hence, $c \mid d$ and d is the required greatest common divisor of a and b.
Now suppose a and b are relatively prime and $a \mid bc$. Since none of irreducible factors of a are associates with b, it must divide c(or in associate with some irreducible factors of c). Thus, it forces us that $a \mid c$.
Now we prove the corollary. If a is an irreducible element and $a \mid bc$, then either $(a, b) = 1$ or $(a, b) = a$. If former was the cases, then $a \mid c$. If later was the case, $a \mid b$. □

10. a) If R is a unique factorization domain, prove that every $f(x) \in R[x]$ can be written as $f(x) = ag_1(x)$, where $a \in R$ and where $f_1(x)$ is primitive.

Proof. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots a_nx^n$ where $a_i \in R$. Define $a = (a_0, a_1, \cdots, a_n)$. Then

$$f(x) = a(b_0 + b_1x + b_2x^2 \cdots + b_nx^n) = af_1(x)$$

where $(b_0, b_1, \cdots b_n) = 1$. Hence $f_1(x)$ is primitive and $f(x) = af_1(x)$. □

b) Prove that the decomposition in part (a) is unique (up to associates).

Proof. Suppose $f(x) = af_1(x) = bf_2(x)$ for some primitive polynomials $f_1(x), f_2(x) \in R[x]$. Let $c(f)$ denote the content of the polynomials. Then

$$\begin{aligned}
&c(f) = c(af_1) = c(bf_2) \\
&(a_0, a_1, \cdots a_n) = a \cdot c(f_1) = a = b \cdot c(f_2) = b
\end{aligned}$$

so that a and b are also greatest common divisors of coefficients of $f(x)$. But since every gcd's are associates, so does a and b, and hence $af_1(x)$ and $bf_2(x)$. □

11. If R is an integral domain, and if F is its field of quotients, prove that any element $f(x)$ in $F[x]$ can be written as $f(x) = (f_0(x)/a)$, where $f_0(x) \in R[x]$ and where $a \in R$.

Proof. Let $f(x)$ be a polynomial in $F[x]$ such that

$$f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x^n$$

where $a_i \in R$, $b_i \neq 0 \in R$. We set $a = b_0b_1 \cdots b_n \in R$. Then

$$\begin{aligned}
f(x) &= \frac{a_0b_1 \cdots b_n}{a} + \frac{a_1b_0b_2 \cdots b_n}{a}x + \cdots + \frac{a_nb_0b_1 \cdots b_{n-1}}{a}x^n \\
&= \frac{a_0b_1 \cdots b_n + a_1b_0b_2 \cdots b_nx + a_nb_0 \cdots b_{n-1}x^n}{a} \\
&= \frac{f_0(x)}{a}
\end{aligned}$$

for some $f_0(x) = a_0b_1 \cdots b_n + a_1b_0b_2 \cdots b_nx + a_nb_0 \cdots b_{n-1}x^n \in R[x]$. □

12. Prove the converse part of Lemma 3.11.4.

Proof. Suppose $f(x) \in R[x]$ is primitive and irreducible as an element of $F[x]$. If $f(x)$ is not irreducible in $R[x]$,

$$f(x) = g(x)k(x)$$

for some non constant $g(x), k(x) \in R[x]$. But each $g(x)$ and $k(x)$ can be viewed as elements in $F[x]$. Thus $f(x) = g(x)k(x)$ in $F[x]$, which contradicts that $f(x)$ is irreducible in $F[x]$. Hence, $f(x)$ is also irreducible in $R[x]$. □

13. Prove Corollary 2 to Theorem 3.11.1.

Proof. Note that $F[x_1]$ is always an Unique Factorization Domain. Applying the Corollary 1, $F[x_1, x_2, \cdots, x_n]$ is also an Unique Factorization Domain. Hence proved. $\square$

14. Prove that a principal ideal ring is a unique factorization domain.

Proof. We can show that every PID is a GCD closed domain, following the proof of Lemma 3.7.1 by just changing the word "Euclidean ring" by "PID". Also, Lemma 3.7.5 and Lemma 3.7.6 assure us that irreducibles of PID are primes(and in fact, vice versa), so that Theorem 3.7.2 is valid. Hence, PID is also an UFD. $\square$

15. If J is the ring of integers, prove that $J[x_1, x_2, \cdots, x_n]$ is a unique factorization domain.

Proof. Note that J is an Euclidean ring with unit element so that it is an PID, and hence, UFD. Consequently, $J[x_1]$ is also an UFD. Induction shows that $J[x_1, x_2, \cdots, x_n]$ is an UFD. $\square$