Ingram Algebraic Number Theory Course Solutions (Appendix)

Emily Pillmore

September 14, 2019

Exercise 1 (A.9)**.** *Let R be a (commutative) ring (with identity), and let $\mathfrak{a}, \mathfrak{b} \subseteq R$ be ideals. Show that*

$$\mathfrak{a} + \mathfrak{b} =_{def} \{a + b : a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

Is an ideal of R.

Proof. By definition, $\mathfrak{a} + \mathfrak{b}$ is an ideal of R if it forms an additive subgroup of R, (i.e. if $(\mathfrak{a} + \mathfrak{b}) \pm (\mathfrak{a} + \mathfrak{b}) \subseteq \mathfrak{a} + \mathfrak{b}$) and if it is closed under (left) multiplicative actions $r\mathfrak{a} \subseteq \mathfrak{a}$ for all $r \in R$. The former is proven by noting that distributivity inherited by R yields the following for all $r \in R$: $r(\mathfrak{a} + \mathfrak{b}) = r\mathfrak{a} + r\mathfrak{b} = \mathfrak{a} + \mathfrak{b}$. Hence $\mathfrak{a} + \mathfrak{b}$ is closed under (left) multiplicative actions. We must now show the former requirement holds.

Let $k, k' \in \mathfrak{a} + \mathfrak{b}$. Note that k has the form $k = a + b$ as defined above. Therefore, $k + k' = (a + b) + (a' + b') = (a + a') + (b + b') \in \mathfrak{a} + \mathfrak{b}$ using associativity inherited by additivity in R, with $0 = 0 + 0$. A similar proof is given for subtraction, hence $\mathfrak{a} + \mathfrak{b}$ is closed under the additive group operation of R, and is therefore an ideal of R. □

Exercise 2 (A.11)**.** *Show that if $a, b \subseteq R$ are ideals, then so is $\mathfrak{a}\mathfrak{b}$, defined as the set of all finite sums of elements of the form ab with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ (including the "empty sum" 0). Show also that this is the smallest ideal containing all elements of the form ab (with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$).*

Proof. Note that each element $ab \in \mathfrak{a}\mathfrak{b}$ takes the form $\sum_{i,j=0}^{n-1} a_i b_j$ where $a \in \mathfrak{a}, b \in \mathfrak{b}$. Must check closure under left multiplicative actions by elements in R, and that these elements are closed under the additive group action of R. Let's first check multiplicativity:

$$\begin{aligned}
rab &= r(\sum_{i,j} a_i b_j) \\
&= \sum_{i,j} r a_i b_j \\
&= \sum_{i,j} a_i b_j \qquad (ra \in \mathfrak{a} \text{ for all } r \in R)
\end{aligned}$$

Hence, finite formal sums are closed under left multiplicative actions by elements of R. Now, we check that it is closed under addition:

$$\begin{aligned}
ab + a'b' &= \sum_{i,j}^{n} a_i b_j + \sum_{k,l}^{m} a'_k b'_l \\
&= \sum_{t=i+k, u=j+l}^{n+m} a_t b_u
\end{aligned}$$

Where $t < n$ enumerates the indices i with $t >= n$ enumerates k, likewise for u. Hence, the sum of finite formal sums of elements $a, a' \in \mathfrak{a}, b, b' \in \mathfrak{b}$ is again a finite formal sum of elements in $\mathfrak{a}$ and $\mathfrak{b}$. The proof is similar for subtraction, with extra steps noting that $\mathfrak{a}$ and $\mathfrak{b}$ are closed under subtraction themselves:

$$\begin{aligned}
ab - a'b' &= \sum_{i,j}^{n} a_i b_j - \sum_{k,l}^{m} a'_k b'_l \\
&= \sum_{i,j}^{n} a_i b_j + (-1) \sum_{k,l}^{m} a'_k b'_l \\
&= \sum_{i,j}^{n} a_i b_j + \sum_{k,l}^{m} (-1) a'_k b'_l \\
&= \sum_{i,j}^{n} a_i b_j + \sum_{k,l}^{m} a''_k b'_l \\
&= \sum_{t=i+k, u=j+l}^{n+m} a_t b_u
\end{aligned}$$

Hence, $\mathfrak{ab}$ is an ideal of R. □

Exercise 3 (A.12)**.** *Let $a, b \in R$. Show that $(a)(b) = (ab)$ (i.e., the product of two ideals means what you think it does for principal ideals). Note again that the product operation does not turn the ideals of R (or even the non-zero ideals of R) into a group.*

Proof. Let $(a) = aR, (b) = bR$ be principal ideals of R. We must show that $(a)(b) = (ab)$ is again a principle of R. Consider $(a)(b)$:

$$
\begin{aligned}
(a)(b) &= aRbR \\
&= abRR \qquad \text{(commutativity of multiplication in } R\text{)} \\
&= abR \qquad\qquad\qquad\qquad\qquad \text{(closure under } \times\text{)} \\
&= (ab)
\end{aligned}
$$

Hence, (ab) is again a principal ideal of R. This is not a group in general for obvious reasons when considering (0), but also in the case of non-zero ideals. Let a and b be zero elements such that $ab = 0$. Then $(b) = (1)(b) = (a^{-1}a)(b) = (a^{-1})(a)(b) = (a^{-1})(ab) = (a^{-1})(0) = (0)$ yields a contradiction. This holds, in fact, even for arbitrary ideals $\mathfrak{ab}$ (via a similar proof).Hence ideals can't form a group under multiplication in the presence of zero elements which may not be 0. $\square$

Exercise 4 (A.15 (optional))**.** *If R is a commutative ring with identity and $\mathfrak{a} \subseteq R$ is an ideal, then $R/\mathfrak{a}$ is a commutative ring with multiplicative identity $1 + \mathfrak{a}$ and additive identity $a = 0 + a$.*

Proof. This is equivalent to noting that for any other ring Q, $R/\mathfrak{a}$ is the coequalizer of the parallel pair $Q \rightrightarrows R$:

$$
\begin{tikzcd}
Q \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & R \arrow[r, "h"] \arrow[d, "\phi"'] & S \\
& R/\mathfrak{a} \arrow[ur, dotted, "\exists! q"'] &
\end{tikzcd}
$$

Hence, $R/\mathfrak{a}$ is a quotient object in $CRng$. (this is a mechanical proof) $\square$

Exercise 5 (A.18)**.** *Let F be a field, and let $R = F[X]$. Prove that every non-zero ideal in R is principal. You may use the division algorithm for polynomials, which says that if $a, b \in F[X]$, with $b \neq 0$, then there exist $q, r \in F[X]$ such that $a = bq + r$, and $0 \leq deg(r) < deg(b)$.*

Proof. $\square$