In today’s 11:20 class, Karen Kelley asked two questions that I couldn’t answer immediately. Here are some answers:

The first question was from the text, Exercise 16.29: Must every ring with a prime number of elements be commutative? We saw immediately that if \((R, +, \cdot)\) is a ring for which \(|R|\) is a prime number, then \((R, +)\) is a cyclic group. But the question is whether the multiplication \(\cdot\) has to be commutative. I claim that it does, because \(\cdot\) is distributive over \(+\). To see this, let \(a\) be a generator of the additive cyclic group \(R\). I contend that the entire multiplication table for \(\cdot\) is determined by the choice of the product \(a \cdot a\), and that it turns out to be commutative: Every element of \(R\) has the form \(na = a + a + \cdots + a\) \((n\text{ terms})\) for some positive integer \(n\) (from 1 up to the prime order of \(R\), to be exact, but we don’t use that here). Now

\[
(na) \cdot (ma) = (a + a + \cdots + a) \cdot (a + a + \cdots + a) \quad (n \text{ and } m \text{ terms})
\]

\[
= a \cdot a + a \cdot a + \cdots + a \cdot a \quad (mn \text{ terms})
\]

\[
= nm(a \cdot a) = mn(a + a) = (ma) \cdot (na) ,
\]

where we have used the fact that multiplication of integers is commutative. Therefore \(\cdot\) is commutative, i.e., \(R\) is a commutative ring.

The second question may be in the text, but I can’t find it. The question was: Find an example of a ring \(R\) and an ideal \(I\) in it, and an ideal \(J\) of \(I\) that is not an ideal in \(R\). The example that I’ve come up with seems to me much harder than it should be, but at least it works. Let \(R = \mathbb{R}[x, Q^+ \cup \{0\}]\), the “semigroup ring of \(Q^+ \cup \{0\}\) over \(\mathbb{R}\)”, i.e., all polynomials in \(x\) with coefficients in \(\mathbb{R}\), but allowing any nonnegative rational number as an exponent. We get polynomials that look like, for example, \(2 + x^{1/2} + 5x^2 - 3x^{10/3}\). Now let:

\[
S = \{q \in \mathbb{Q} : q \geq 1\} \quad \text{and} \quad T = \{1\} \cup \{q \in \mathbb{Q} : q \geq 2\}.
\]

The set of elements with exponents in \(S\) is an ideal of \(R\) — the product of a polynomial with lowest-degree term at least \(x^1\) and any other polynomial in \(R\) is another with lowest-degree term at least \(x^1\). And the set \(J\) of polynomials with exponents in \(T\) is an ideal in \(I\) — in fact, the product of any two elements of \(I\) is in \(J\), because its lowest degree term is at least \(x^2\). But \(J\) is not an ideal in \(R\); \(x^{1/2} \in R\) and \(x^1 \in J\), but \(x^{1/2} \cdot x^1 = x^{3/2} \notin J\). There must be a simpler example.

P.S.: Here is another example; whether it qualifies as simpler is up to you: Let \(R\) be the set of polynomials in \(x\) with terms \(ax^n\) where \(a\) is a real number and \(n = 2r + 3s\) for some nonnegative integers \(r, s\) — so the exponents can be any element of \(\mathbb{N} \cup \{0\}\) except 1. (In the terms of the last example, this \(R\) is the semigroup ring of the “numerical semigroup generated by 2 and 3”.) Now let \(I\) be the set of elements of \(R\) with zero coefficients in the \(x^0\) (i.e., constant) and \(x^2\) terms, and let \(J\) be the set of elements of \(R\) with zero coefficients in the \(x^0\), \(x^2\), and \(x^5\) terms. The product of any two elements of \(I\) has lowest exponent at least 6, so it is in \(J\); so \(J\) captures multiplication in \(I\) and hence is an ideal there. But \(J\) is not an ideal in \(R\), because \(x^3 \in J\) and \(x^2 \in R\) but \(x^5 \notin J\).