Fields were intended to capture our intuitions from \( \mathbb{Q} \). What about \( \mathbb{Z} \)?

**Definition 8.** A commutative ring is a set equipped with two binary operations + and \( \times \) which satisfy all the field axioms except M4 (the existence of multiplicative identities). A not-necessarily-commutative ring also omits axiom M3, and also beefs up axiom M1 to say \( 1a = a = a1 \) for all \( a \) and beefs up axiom AM1 to say \( a(b + c) = ab + ac \) and \( (b + c)a = ba + bc \). In this class, we will almost entirely be concerned with commutative rings, and when I say ‘ring’ without qualification (something I’ll try to avoid doing), I mean ‘commutative ring’. (The book, by contrast, means not-necessarily-commutative ring.)

(Remark: sometimes people omit the axiom M1 from the ring axioms, and call rings that satisfy it ‘rings with unit’. For us, though, all rings have unit.)

**Proposition 9.** All the facts in Proposition 2 (lecture 5) are all true for any ring, not just any field.

**Proof.** A quick examination of the proof of Proposition 2 reveals we never used axiom M4. \( \square \)

On the other hand, the proof of Proposition 5 (which said that if \( ab = 0 \) then either \( a = 0 \) or \( b = 0 \)) did use axiom M4. Thus the conclusion of Proposition 5 need not be true in an arbitrary ring.

**Definition 10.** Let \( R \) be a commutative ring. If it is the case that whenever \( a, b \in R \) satisfy \( ab = 0 \), then we can conclude that \( a = 0 \) or \( b = 0 \), then we say \( R \) is an integral domain (or just domain for short).

**Example 11.** Every field is of course an example of a domain (e.g \( \mathbb{R}, \mathbb{C}, \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R} \)).

**Example 12.** The integers \( \mathbb{Z} \) form a commutative ring, which is even a domain.

**Example 13.** The collection of 2 by 2 matrices forms a not-necessarily-commutative ring.

**Example 14.** The collection of polynomials with real coefficients form a commutative ring. This ring is denoted by something like \( \mathbb{R}[X], \mathbb{R}[T], \mathbb{R}[x] \) or \( \mathbb{R}[t] \), depending on which letter we are using to denote the variable of the polynomial. In fact, this is a domain; if \( p(x)q(x) = 0 \), then we can write \( p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \) and \( q(x) = bmx^m + b_{m-1}x^{m-1} + \cdots + b_0 \), where \( a_n \) and \( b_m \) are not 0. Then we can work out that \( p(x)q(x) = a_nb_mx^{n+m} + \cdots \), which is not zero (as \( a_nb_m \neq 0 \)).

**Example 15.** Similarly, we can construct rings \( \mathbb{Q}[T] \) (polys with rational coeffs) and \( \mathbb{C}[T] \). In fact, we can do this for any field. (The result will still always be a domain; why?) Thus, for instance, if \( F \) is the ‘mystery field’ from the first lecture, then \( F[X] \) makes sense and is a domain.

**Example 16.** Suppose \( R_1 \) and \( R_2 \) are commutative rings (possibly, both the same ring). We can cook up another ring \( R_1 \times R_2 \) out of them as follows. The elements of \( R_1 \times R_2 \) consist of pairs \((r_1, r_2)\) where \( r_1 \in R_1 \) and \( r_2 \in R_2 \). We multiply and add using the formulas

\[
(r_1, r_2) \times (r_1', r_2') = (r_1 \times r_1', \ r_2 \times r_2') \quad \text{multiply in } R_1 \times \text{multiply in } R_2
\]

\[
(r_1, r_2) + (r_1', r_2') = (r_1 + r_1', \ r_2 + r_2') \quad \text{add in } R_1 \times \text{add in } R_1
\]

It is easy to check that this gives us a ring structure.\(^1\) But, this is not a domain, even if \( R_1 \) and \( R_2 \) were domains.

\(^1\)In fact, this would work with not-necessarily-commutative rings too.