RINGS

Vocabulary: ring, commutative ring, zero ring, ring homomorphism, units .

Definition. A ***ring*** is a set R with two operations:

- $+\colon R \times R \to R$ (called ***addition***) and
- $*\colon R \times R \to R$ (called ***multiplication***)

and elements 0_R and 1_R satisfying[a] [b] the following axioms:

R1: $(R, +, 0_R)$ is an abelian group,
R2: $*$ is associative: $r * (s * t) = (r * s) * t$ for all $r, s, t \in R$,
R3: multiplication is both left and right distributive with respect to addition: for all $r, s, t \in R$ we have $r * (s + t) = r * s + r * t$ (called ***left-distributivity***) and $(s + t) * r = s * r + t * r$ (called ***right-distributivity***), and
R4: $1_R * r = r * 1_R = r$ for all $r \in R$.

[a] Some people do not impose that a ring has a multiplicative identity, but in this course all rings will have a multiplicative identity. See Poonen, "Why all rings should have a 1", `https://math.mit.edu/~poonen/papers/ring.pdf` for an argument.

[b] A ring without an identity is sometimes referred to as a ***rng***. A ring without negatives is sometimes called a ***rig***.

We will almost always drop the symbol $*$ and write ab for $a * b$; similarly, we will write 0 and 1 for 0_R and 1_R. A ring is said to be ***commutative*** provided that its multiplicative operation is commutative. A ***zero ring*** is a ring with one element.

(1) Suppose R is a ring. Show $\mathrm{Mat}_{n\times n}(R)$ is a ring with respect to matrix multiplication. When is it commutative?
(2) Let G be a group and k a ring. The ***group ring*** kG is defined to be the set of sums of the form $\sum_{g\in G} a_g g$, where the a_g are in k and all but finitely many a_g are 0, with the "obvious" addition and multiplication. Spell out what the "obvious" definitions are and check that they are a ring.
(3) Let A be an abelian group. Let $R = \mathrm{Hom}_{\mathrm{grp}}(A, A)$, and define operations $+$ and $*$ on R by $(r_1 + r_2)(a) = r_1(a) + r_2(a)$ and $(r_1 * r_2)(a) = r_1(r_2(a))$. Show that R is a ring.

This ring is called the ***endomorphism*** ring of A and denoted $\mathrm{End}(A)$.

(4) Why did we require that A was abelian in the previous problem?
(5) Suppose R is a ring. Show that $0_R * x = x * 0_R = 0_R$ for all $x \in R$.
(6) Suppose that R is a ring with $0_R = 1_R$. Show that R is the zero ring.

Definition. Suppose that R is a ring. An element $u \in R$ is called a ***unit*** if there is an element u^{-1} with $u * u^{-1} = u^{-1} * u = 1_R$. The set of units of R is denoted $R^\times$.

(7) Show that $R^\times$ is a group with respect to $*$.
(8) Give an example of a ring R with elements u and v such that $u * v = 1_R$ but $v * u \neq 1_R$.

Definition. Suppose $(R, +_R, *_R, 1_R)$ and $(S, +_S, *_S, 1_S)$ are two rings. A function $f\colon R \to S$ is called a ***ring homomorphism*** provided[a] that

- $f(a +_R b) = f(a) +_S f(b)$ for all $a, b \in R$,
- $f(a *_R b) = f(a) *_S f(b)$ for all $a, b \in R$, and
- $f(1_R) = 1_S$

The set of ring homomorphisms from R to S is denoted $\mathrm{Hom}(R, S)$ or $\mathrm{Hom}_{\mathrm{ring}}(R, S)$.

[a] Some people do not impose that $f(1_R) = 1_S$. These people call f ***unital*** when $f(1_R) = 1_S$. In this course, we define homorphisms to be unital, and say "non-unital homomorphism" on the rare occasions that we need this concept.

(9) Let $R = \mathbb{Z}/15\mathbb{Z}$ and let $S = \mathbb{Z}/3Z$. What is $\mathrm{Hom}_{\mathrm{ring}}(R, S)$? What about $\mathrm{Hom}_{\mathrm{ring}}(S, R)$? What if we allow non-unital homomorphisms?
(10) We defined a group ring above. For those who know what a monoid and/or a category are: Can you define a ***monoid ring***? What about a ***category ring***?