WORKSHEET 1.1: BASICS OF RINGS

A *ring* $(R,+,\cdot)$ is an abelian group $(R,+)$ together with a multiplication $(\cdot)$ and a multiplicative identity element $1_R \in R$ satisfying the following axioms:

(i) (Multiplicative Identity): $1_R \cdot a = a \cdot 1_R = a$ for all $a \in R$,

(ii) (Associativity): $a\cdot(b\cdot c) = (a\cdot b)\cdot c$ for all $a,b,c \in R$, and

(iii) (Distributivity): $a\cdot(b+c) = (a\cdot b)+(a\cdot c)$ and $(b+c)\cdot a = (b\cdot a)+(c\cdot a)$ for all $a,b,c \in R$.

As a warning some people will not include condition (i) in the definition of a ring, but this is rare to unheard of in modern commutative algebra. (See the historical remark at the end of this worksheet.) As is often the case once we are familiar with these operations we will normally just drop some of the notational baggage and just write ab for $a\cdot b$ and 1 for 1_R.

A ring R is *commutative* if and only if $ab = ba$ for all $a,b \in R$. As the name of the course suggests we will primarily be interested in commutative rings in this course. To the point we shall adopt the following convention: Throughout this course, "ring" means *commutative* ring with unity. Commutative algebra broadly can be thought of as the study of rings and their associated objects. At a high level we will study rings from four perspectives: 1) element-wise, 2) homomorphisms, 3) ideals, and 4) modules. You hopefully have some familiarity with 1, 2, and 3, but today we will review and remember what it is like working with these objects.

An element $u \in R$ is a *unit* if there exists $v \in R$ such that $uv = vu = 1$, in which case we will often denote v by u^{-1}. A nonzero element $a \in R$ is a *zero divisor* if there exists a nonzero element $b \in R$ such that $ab = 0$. A non-zero element, which is not a zero divisor is a *non-zero divisor*.

(1) Let R be a ring and consider $R[[t]]$ the ring of formal power series with coefficients in R. The goal of this exercise is to prove that:

$$(R[[t]])^\times = \left\{ u + tf(t) \;\middle|\; u \in R^\times,\ f(t) \in R[[t]] \right\}.$$

   (a) Elements of $R[[t]]$ can be written as $f = \sum_{k=0}^{\infty} f_k t^k$ for $f_k \in R$. We call f_0 the constant term of f. If $f = \sum_{k=0}^{\infty} f_k t^k$ and $g = \sum_{k=0}^{\infty} g_k t^k$ then find a formula for the constant term of fg.

   (b) Using the formula from 1a prove that if f is a unit then $f_0 \in R^\times$.

   (c) Find a formula for the coefficient of t^k appearing in fg.

   (d) Assume that $f_0 \in R^\times$. Prove that f is a unit by explicitly constructing an element $g \in R[[t]]$ such that $fg = 1$. (Hint: The condition that $fg = 1$ places constraints on each coefficient of fg. Use the constraints together with part 1c to recursively solve for the coefficients of g.)

A non-empty subset $I \subset R$ is an *ideal* if it is closed by outside multiplication by elements of R and is closed under addition. Precisely, $I \subset R$ is a non-empty subset satisfying:

(i) if $a \in I$ then $ra \in I$ for all $r \in R$ and

(ii) if $a, b \in I$ then $a + b \in I$.

Note this immediately implies that an ideal always contains 0 and is an abelian group with respect to addition. Given elements $a_1, \ldots, a_t \in R$ we write $\langle a_1, \ldots, a_t \rangle \subset R$ for the the smallest ideal containing $a_1, \ldots, a_t$. Concretely, we may describe this as the set of all R-linear combinations of $a_1, \ldots, a_t$:

$$\langle a_1, \ldots, a_t \rangle = \left\{ r_1 a_1 + \cdots + r_t a_t \;\middle|\; r_1, \ldots, r_t \in R \right\}.$$

An ideal $I \subset R$ is *principal* if there exists an element $a \in R$ such that $I = \langle a \rangle$.

---

(1) (a) Prove that an element $u \in R$ is a unit if and only if the principal ideal $\langle u \rangle = R$.

(b) Prove that if ab and b are units, then a is a unit.

(c) Prove that if u is a unit and $a \in R$, then a and ua generate the same principal ideal.

(d) In the ring $\mathbb{Z}/\langle 12 \rangle$, determine which elements are units.

Let R and S be rings. A ring homomorphism from R to S is a function $\phi : R \to S$ such that:

(i) (Multiplicative): $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$,

(ii) (Additive): $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$, and

(iii) (Preserves Unit): $\phi(1_R) = 1_S$.

Notice that condition (ii) implies that $\phi(0_R) = 0_S$, so ϕ is a homomorphism of the underlying abelian groups. It will turn out that condition (iii) is very useful as the following exercise demonstrates. There are two important sets associated to any ring homomorphism $\phi : R \to S$ the kernel and image of ϕ:

$$\ker(\phi) := \left\{ a \in R \;\middle|\; \phi(a) = 0 \right\} \subset R \qquad \text{and} \qquad \operatorname{img}(\phi) := \left\{ \phi(a) \in S \;\middle|\; a \in R \right\} \subset S.$$

More succinctly, $\ker(\phi) = \phi^{-1}(\{0\})$ and $\operatorname{img}(\phi) = \phi(R)$. One checks that $\ker(\phi)$ is an ideal of R, and that $\operatorname{img}(\phi)$ is a subring of S; however, it need not be an ideal of S.

---

(1) Given two rings R and S we let $\mathrm{Hom}_{\mathbf{comRing}}(R, S)$ be the set of ring homomorphisms from R to S. When there is little room for confusion we will often drop the subscript **comRing** and simply write $\mathrm{Hom}(R, S)$.

(a) Prove or disprove: If R and S are rings, then $\mathrm{Hom}(R, S)$ is a ring under point-wise multiplication and point-wise addition.

(b) Give an explicit description of the hom-sets below:

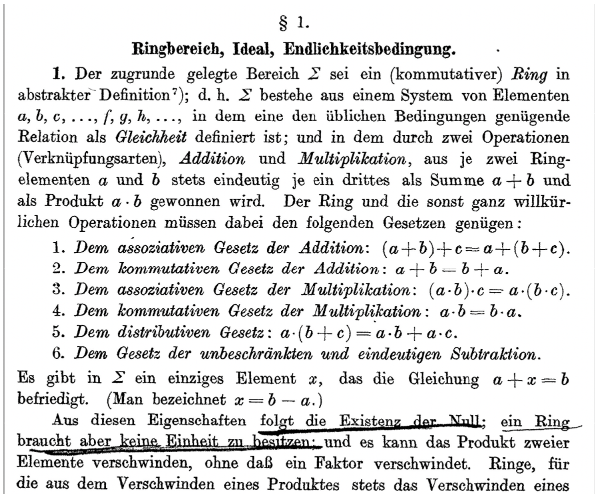
  (i) $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z})$
  (ii) $\mathrm{Hom}(\mathbb{Z}/\langle 2\rangle, \mathbb{Z})$
  (iii) $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/\langle 2\rangle)$
  (iv) $\mathrm{Hom}(\mathbb{Z}, \mathbb{C}[x])$

(c) Based on part 1b state and prove a characterization of $\mathrm{Hom}(\mathbb{Z}, R)$ for any ring R.

(2) Let $\phi : R \to S$ be a ring homomorphism.

  (a) Prove that if $J \subset S$ is an ideal then $\phi^{-1}(J) \subset R$ is an ideal.
  (b) Assuming ϕ is injective, give a nice description of $\phi^{-1}(J)$ for an ideal $J \subset S$.
  (c) Find a counterexample showing that if $I \subset R$ is an ideal, then $\phi(I)$ need not be an ideal.
  (d) Prove that if ϕ is surjective then $\phi(I)$ is an ideal of S.
  (e) Let $I \subset R$ be an ideal. Prove that if $\ker(\phi) \subset I$, then $\phi^{-1}(\phi(I)) = I$.
  (f) Is the assumption that $\ker(\phi) \subset I$ needed in part 2e?

As a small historical remark, despite it being common practice to include the existence of a multiplicative identity in the definition of a ring, in her original definition of a ring Emmy Noether did not do this. In E. Noether's 1921, article *Idealtheorie in Ringbereichen* – which can reasonably be viewed as the birth of commutative algebra – she says, "*Aus diesen Eigenschaften folgt die Existenz der Null; ein Ring braucht aber keine Einheit zu besitzen...*"; roughly translating to, "From these properties the existence of the zero element follows; however a ring is not required to possess a unit".



§ 1.

Ringbereich, Ideal, Endlichkeitsbedingung.

1. Der zugrunde gelegte Bereich Σ sei ein (kommutativer) *Ring* in abstrakter Definition[7]); d. h. Σ bestehe aus einem System von Elementen $a, b, c, \ldots, f, g, h, \ldots,$ in dem eine den üblichen Bedingungen genügende Relation als *Gleichheit* definiert ist; und in dem durch zwei Operationen (Verknüpfungsarten), *Addition* und *Multiplikation*, aus je zwei Ringelementen a und b stets eindeutig je ein drittes als Summe $a + b$ und als Produkt $a \cdot b$ gewonnen wird. Der Ring und die sonst ganz willkürlichen Operationen müssen dabei den folgenden Gesetzen genügen:

1. *Dem assoziativen Gesetz der Addition*: $(a+b)+c = a+(b+c)$.
2. *Dem kommutativen Gesetz der Addition*: $a + b = b + a$.
3. *Dem assoziativen Gesetz der Multiplikation*: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
4. *Dem kommutativen Gesetz der Multiplikation*: $a \cdot b = b \cdot a$.
5. *Dem distributiven Gesetz*: $a \cdot (b + c) = a \cdot b + a \cdot c$.
6. *Dem Gesetz der unbeschränkten und eindeutigen Subtraktion.*

Es gibt in Σ ein einziges Element x, das die Gleichung $a + x = b$ befriedigt. (Man bezeichnet $x = b - a$.)

Aus diesen Eigenschaften folgt die Existenz der Null; ein Ring braucht aber keine Einheit zu besitzen; und es kann das Produkt zweier Elemente verschwinden, ohne daß ein Faktor verschwindet. Ringe, für die aus dem Verschwinden eines Produktes stets das Verschwinden eines

---