Abstract Algebra. Math 6310. Bertram/Utah 2022-23.
Rings

Definition. A *commutative ring with* 1 $(R,+,\cdot)$ is a set R with operations:

$$+ : R\times R\to R \ \text{ and } \ \cdot : R\times R\to R \text{ satisfying}$$

(i) $(R,+)$ is an abelian group (with identity 0 and additive inverse $-r$)

(ii) $(R,\cdot)$ is associative with multiplicative identity $1\neq 0$ and commutative, and

(iii) For each $r\in R$, the map:

$$r:(R,+)\to(R,+);\ r(s)=r\cdot s \text{ is a homomorphism}$$

i.e. multiplication distributes with addition (and it follows* that $r\cdot 0=0$).

In other words, R satisfies the field axioms except for multiplicative inverses.

Examples. (i) The model examples are the fields k and $(\mathbb{Z},+,\cdot)$ the ring of integers.

(ii) Direct products (but not infinite direct sums!) of commutative rings with 1.

(iii) Given a commutative ring R with 1, then the ring of *polynomials*:

$$(R[x],+,\cdot)$$

is a commutative ring with 1, as are the rings of *power series* and *Laurent series*:

$$R[[x]]=\left\{\sum_{d=0}^{\infty} r_d x^d \mid r_d\in R\right\} \text{ and } R((x))=\left\{\sum_{d=e}^{\infty} r_d x^d \mid r_d\in R, e\in\mathbb{Z}\right\}$$

Note. If k is a field, then $k((x))$ (but not $k[[x]]$) is also a field*.

Examples. The ring $\mathbb{C}[[z]]$ contains the subrings:

$$\mathbb{C}[z]\subset \mathcal{H}ol(\mathbb{C})\subset\mathcal{H}ol(U)\subset\mathcal{H}ol_0\subset\mathbb{C}[[z]]$$

of entire holomorphic functions, holomorphic functions on an open set $0\in U\subset\mathbb{C}$, and holomorphic functions in *some* neighborhood of 0. The inclusions are strict*.

Before we move to ideals, we visit a few non-commutative rings.

The Group Ring. Let R be a commutative ring with 1 and $(G,*)$ be a group, Then:

$$R[G]=\{\sum_{i=1}^n r_i g_i\}$$

the set of (formal) finite sums of elements in G with coefficients in R is a ring with:

$$\sum r_i g_i+\sum s_i g_i=\sum (r_i+s_i)g_i \text{ and}$$

$$\left(\sum r_i g_i\right)*\left(\sum s_j h_j\right)=\sum_i\sum_j r_i s_j (g_i * h_j)$$

Note that $(R[G],+,*)$ is commutative if and only if G is abelian. For example,

$$R[\mathbb{Z}]=\left\{\sum_{d=-e}^{e} r_d x^d \ |e\in\mathbb{Z}\right\}$$

is the ring of *Laurent polynomials*, and for a finite cyclic group $(C_n,*)$,

$$R[C_n]=\{r_0+r_1x+\cdots+r_{n-1}x^{n-1}\mid x^n=1\}$$

where $x\in C_n$ is a generator (as in the case of the infinite cyclic group above).

Endomorphism Rings. Let A be an abelian group. Then the *ring of endomorphisms*:

$$\mathrm{End}_{\mathrm{ab}}(A) = \{f : A \to A\}$$

(of A as an abelian group) is a ring with *composition* as the product, since:

$$(f \circ (g+h))(a) = f(g(a)+h(a)) = (f \circ g)(a) + (f \circ h)(a)$$

(but composition rarely commutes). Recall that the ring of k-linear endomorphisms:

$$M_{n\times n}(k) = \mathrm{End}_{\mathrm{vs}}(k^n)$$

is the ring of $n \times n$ matrices with matrix addition and multiplication.

Quaternions. The vector space $\mathbb{R}^4$ with basis $\{1, i, j, k\}$ and multiplication:

$$i^2 = j^2 = k^2 = -1, ij = k = -ji, jk = i = -kj, ki = j = -ik$$

is the ring $\mathbb{H}$ of quaternions. It is not commutative, but:

$$(a+bi+cj+dk)(a-bi-cj-dk) = \ (a^2+b^2+c^2+d^2)$$

is a nonzero real number whenever $a + bi + cj + dk \neq 0$, and so, like a field, every non-zero element of $\mathbb{H}$ has a (unique) multiplicative inverse. A non-commutative ring with (left and right) multiplicative inverses is called a *division ring.*

Definition. A map $f : R \to S$ of rings with 1 is a *ring homomorphism* if:

(i) $f(r_1 + r_2) = f(r_1) + f(r_2)$ for all $r_1, r_2 \in R$ and $f(0) = 0$ (linear)

i.e. f is a homomorphism of additive abelian groups, and

(ii) $f(r_1 r_2) = f(r_1)f(r_2)$ for all $r_1, r_2 \in R$ and $f(1) = 1$ (multiplicative)

Examples. (i) Evaluation at $x = r$ is a ring homomorphism:

$$ev_r : R[x] \to R;\ ev_r(f) = f(r)$$

and in the special case $r = 0$, we can extend this to the formal power series ring:

$$ev_0 : R[[x]] \to R;\ ev_0(r_0 + r_1 x + \cdots) = r_0$$

If we think of polynomials as functions from R to R, then this generalizes. Let S be an nonempty set, and let

$\mathcal{F}un(S, R) = \{f : S \to R\}$ with pointwise addition and multiplication of functions.

Then $ev_p(f) = f(p)$ defines an evaluation homomorphism to R.

(ii) The map from integers to the commutative ring:

$$(\mathbb{Z}/n\mathbb{Z}, +, \cdot) \text{ of integers mod } n$$

given by $f(r) = r \pmod{n}$ is a (surjective) ring homomorphism.

Nonexamples. (i) The derivative: $d : \mathcal{C}^1(0,1) \to \mathcal{C}(0,1)$ is linear (and $\mathbb{R}$-linear) but not multiplicative (because of the Leibniz rule for products).

(ii) The *determinant* $\Delta : \mathrm{End}(k^n) \to k$ is multiplicative but not linear.

Image. The image $f(R)$ of a homomorphism of commutative rings with 1 satisfies:

(a) if $s_1, s_2 \in f(R)$, then $s_1 + s_2 \in f(R)$ and $-s_i \in f(R)$ (so $0 \in f(R)$)

(b) also, $s_1 s_2 \in f(R)$ and (by assumption) $1 \in f(R)$.

In other words, the image of a homomorphism is a *subring (with* 1*).*

And of course, conversely, any subring with 1 of a commutative ring R is the image of a homomorphism, namely the inclusion mapping (of the subring). As a bonus, therefore, every subring of R is the image of a *mono*morphism.

Kernel. The kernel $I = f^{-1}(0)$ of a morphism of commutative rings with 1 satisfies:

(a) if $s_1, s_2 \in I$, then $s_1 + s_2 \in I$ and $-s_i \in I$ (so $0 \in I$) and

(b) if $r \in R$ and $s \in I$, then $rs \in I$ (but $1 \notin I$ unless $I = R$).

Conversely, we make the following definition.

Definition. A subset $I \subset R$ is an *ideal* if it satisfies (a) and (b) above

Examples. (i) $n\mathbb{Z} \subset \mathbb{Z}$ (for any n) is an ideal.

(ii) if $S \subset R$ is a subset, then $\langle S \rangle = \{\sum_{i=1}^n r_i s_i \mid r_i \in R, s_i \in S\}$ is the *ideal generated by* S. In particular, what we've been calling $n\mathbb{Z}$ could also be called $\langle n \rangle$.

Notice that subrings (with 1) are **NOT** ideals and vice versa. This distinguishes commutative rings from abelian groups or vector spaces, in which all kernels are images and vice versa. Thus the cokernel of a ring homomorphism is not defined.

Definition/Proposition. Given an ideal $I \subset R$ in a commutative ring, then:

$$r \sim r' \text{ if and only if } r - r' \in I$$

is an equivalence relation on R, whose equivalence classes are denoted by:

$$r + I := \{r' \in R \mid r \sim r'\}$$

and the set of equivalence classes R/I inherits a *well-defined* pair of operations:

$$(r + I) + (s + I) := (r + s) + I \text{ and } (r + I)(s + I) = rs + I$$

making R/I into a commutative ring with 1 equipped with a canonical *epimorphism*:

$$f : R \to R/I;\ f(r) = r + I$$

i.e. a surjective ring homomorphism.

Proof (of well-definedness). If $r - r' \in I$ and $s - s' \in I$, then:

$$(r + s) - (r' + s') = (r - r') + (s - s') \in I \text{ and}$$

$$(rs - r's') = (rs - r's) + (r's - r's') = (r - r')s + r'(s - s') \in I$$

so the operations are well-defined by properties (a) and (b) of an ideal, respectively.

Note: When adapting this to a non-commutative setting, one needs to distinguish left multiplication from right multiplication. The definition above gives a *left ideal*, in which multiplication by R happens on the left, but a *right ideal* flips (b) to (b'): $sr \in I$ for all $s \in I$ and $r \in R$. The kernel of a homomorphism is a both-sided ideal and conversely, a quotient ring by a both-sided ideal is constructed as above. A (non-commutative) ring with no non-trivial both-sided ideals is *simple*. For example* the matrix ring $\text{End}(k^n)$ is simple.

Commutative Rings in the Wild. Every number field K has a *ring of integers* $\mathcal{O}_K \subset K$. Class field theory is the study of these rings. Complex algebraic geometry is concerned with the rings $\mathbb{C}[x_1, ..., x_n]/I$ and arithmetic algebraic geometry, a blend of number theory and algebraic geometry, is about the rings $\mathcal{O}_K[x_1, ..., x_n]/I$.