Honors Algebra II, Courant Institute, Spring 2021

http://www.math.nyu.edu/faculty/goodman/teaching/HonorsAlgebraII2021/HonorsAlgebraII.html

Basic definitions and concepts of commutative algebra.

It came up in the first class that the Algebra I class did not cover rings very much or at all. These notes give the basic definitions. Please think through anything that is unfamiliar to you. This may take a while. All this material is in each of the three textbooks (Artin, Judson, Herstein). It might help to see the concepts described more systematically in those books.

Some domains

I use the word *domain* to mean any algebraic object, or algebraic setting. The technical term is *category*. There is a category of groups, a category of rings, etc. A mathematician might say: "this theorem holds is the category of rings" to mean that it is true about any ring. We won't use category theory in this class, but the word might slip out once or twice.

integers $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, \cdots\}$

rationals $\mathbb{Q} =$ fractions $r = \frac{a}{b}$ where a and b are integers.

reals $\mathbb{R} =$ the set of real numbers

complex numbers $\mathbb{C} =$ the set of complex numbers $z = x + iy$ with $x \in \mathbb{R}$ and $y \in \mathbb{R}$.

polynomials $D[x]$ = the set of formal polynomials with coefficients in the "domain" D. A *polynomial* $f \in D[x]$ is an expression $a_0 + a_1 x + \cdots + a_n x^n$. The a_k are elements of D. The powers x_k are just formal expressions that help us define the *operations* on polynomials.

Operation

The "domains" of abstract algebra are *groups*, *rings*, *fields*, *algebras*, etc. Each type of domain is defined by the *operations* that are defined on it. If D is a domain, an operation is a function $F\colon D \times D \mapsto D$. This means that for any pair (x, y) with $x \in D$ and $y \in D$, there is $z = F(x, y) \in D$. An operation is usually written "as an operation", $z = x \circ y$ means that $z = F(x, y)$. The operations in this course are called *addition*, where $\circ$ is $+$ or *multiplication*, where $\circ$ is $\cdot$ or $\times$ or just left out. An operation is assumed to be *associative*, which means that any $x, y, z \in D$ have

$$(x \circ y) \circ z = x \circ (y \circ z) \ .$$

In function notation, this is

$$F(F(x, y), z) = F(x, F(y, z)) \ .$$

The expression using F shows that the associative property is non-trivial. It also demonstrates that it can be more clear to use operator notation. An operation is *commutative* (also called *abelian*) if $F(x,y) = F(y,x)$ (which is the same as $x \circ y = y \circ x$) for all $x, y \in D$.

Inverse

The *identity* element for operation $\circ$ is $e \in D$ with $e \circ x = x$ and $x \circ e = x$ for all $x \in D$. If $\circ$ is addition, the identity is called the *additive identity* and is often denoted by 0. That means $0 + x = x + 0 = 0$ for all $x \in D$. The *multiplicative identity* is often denoted by 1, and $1 \cdot x = x \cdot 1 = x$ for all $x \in D$. An *inverse* of $x \in D$ for operation $\circ$ is $y \in D$ with $x \circ y = y \circ x = e$. An *additive inverse* of $x \in D$ is often denoted by $-x$, so $x + (-x) = (-x) + x = 0$. A *multiplicative inverse* of x is denoted by x^{-1}, so $\left(x^{-1}\right) \cdot x = x \cdot \left(x^{-1}\right) = 1$. These notations assume that an inverse is unique, which it usually is.

Group

A *group* G is a domain with a single operation. It is assumed that there is an identity element and every $x \in G$ has a unique inverse with respect to the operation. In this class, some groups are commutative and others (particularly Galois groups) need not be. The group operation is usually written multiplicatively, and generally without the $\cdot$. That means $x \circ y$ is written xy. If the group is abelian, the operation is sometimes written *additively*, so $x \circ y$ is written as $x + y$. All of the example domains above are groups if the operation is addition. The domain $\mathbb{Q}^*$ is $\mathbb{Q}$ with 0 removed (non-zero rational numbers). This $\mathbb{Q}^*$, with the operation of multiplication, is also a group. The multiplicative groups $\mathbb{R}^*$ and $\mathbb{C}^*$ are defined in the same way. You have seem other groups where the operation is neither addition nor multiplication, such as S_n (the group of permutations of n objects) and the group of rotations and translations of euclidean space.

Semi-group

A *semi-group* is a domain with an operation that has an identity element but not necessarily inverses. Any group is a semi-group. Some semi-groups that are not groups are $\mathbb{Z}$ and $D[x]$.

Ring

A *ring* R is a domain with two operations, one written additively and one written multiplicatively. The ring is a group with respect to the additive operation and a semi-group with respect to "multiplication" (the operation written multiplicatively). In this class, the operations in a ring are always assumed to be commutative. In *commutative algebra*, all operations are assumed to be commutative except group operations. (Galois theory is part of commutative algebra.)

The operations are related by the *distributive law*, which is

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z) \ .$$

All the domains above are rings, except possibly $D[x]$. This becomes a ring if the *coefficients* a_k are in an abelian semi-group (or a ring). A *zero divisor* in a ring is an $x \neq 0$ so that there is a $y \neq 0$ with $xy = 0$. A ring without zero divisors is an *integral domain*, sometimes just called *domain*.

Field

A *field* $\mathbb{F}$, is a ring where every $x \in \mathbb{F}$ except $x = 0$ has a multiplicative inverse. Examples are $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. The integers and polynomial rings are not fields because many elements do not have multiplicative inverses. Polynomial rings are unlikely to be fields. The *degree* of a polynomial is the largest n with $a_n \neq 0$ (assuming D is a ring). We write $n = \deg(f)$. If $\deg(f) > 0$, and if the coefficient ring (where the coefficients a_j live) has no zero divisors, then there is no g with $fg = 1$.

Homomorphism (mapping)

A *homomorphism* is a map $\phi\colon D \mapsto E$ from one domain to another domain that respects the operations of the domains. This means that whatever operations exist in D also exist in E and $\phi(x \circ_D y) = \phi(x) \circ_E \phi(y)$ for all $x, y \in D$. The notation $\circ_D$ means the operation in D. For groups, a homomorphism has to respect the group operation. For rings and fields, it has to respect both addition and multiplication. An example is what the textbook calls the polynomial *evaluation map*. If R is a ring and $D = R[x]$ (the polynomial ring), and for $c \in R$, there is a map that evaluates a polynomial $f(x)$ at the point c

$$\phi_c\colon R[x] \mapsto R \ \ , \ \ f \overset{\phi_c}{\rightsquigarrow} f(c) = a_0 + a_1 c + a_2 c^2 + \cdots + a_n c^n \ .$$

A homomorphism is an *injection*, (also called *into* if no to elements are mapped to the same element (no loss of information). That is $x \neq y \implies \phi(x) \neq \phi(y)$. A homomorphism is a *surjection* (also called *onto*, "sur" is "on" in French) if it covers all of its target (also called range). For every $y \in E$, there is an $x \in D$ with $\phi(x) = y$. A homomorphism is a *bijection* if it is both into and onto. In algebra, a bijection is necessarily an *isomorphism*, which means that the *inverse map* defined by $\phi^{-1}(y) = x$ if $\phi(x) = y$ is well defined and also is a homomorphism. You should verify this for yourself: ϕ^{-1} preserves the operations.

Two domains (two groups, or two rings, etc.) are *isomorphic* if there is an isomorphism between them. People think of isomorphic objects as being the same, but that doesn't mean that isomorphisms are obvious or trivial. An *automorphism* is an isomorphism from a domain to itself. There can be many automorphisms that are not the identity automorphism. Galois theory as about certain kings of automorphisms of fields.

The *image* of a homomorphism is the set of $\phi(x)$ for all x. The *kernel* of a group homomorphism is the set of $x \in G$ with $\phi(x) = \mathrm{id}$. (The identity element in a group is often called id). The kernel of a ring or field homomorphism is the set of $x \in R$ or $x \in \mathbb{F}$ that map to the additive identity: $\phi(x) = 0$.

Polynomials and rational functions

A polynomial ring can have more than one "variable". For example, $\mathbb{Q}[x, y]$ is the set of polynomials in two variables with rational coefficients. Elements of $\mathbb{Q}[x, y]$ have the form

$$f = \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} x^i y^j \ .$$

You add and multiply multi-variable polynomials in the usual way. A *rational function* is a quotient of polynomials. The set of rational functions in one variable with coefficients in $\mathbb{F}$ is written $\mathbb{F}(x)$. Round parentheses mean rational functions and square braces mean polynomials. A rational function $r \in \mathbb{F}(x)$ has the form

$$r(x) = \frac{f(x)}{g(x)} \ , \quad f, g \in \mathbb{F}[x] \ , \ g \neq 0 \ .$$

The denominator is not allowed to be the zero polynomial, but it may have zeros. The zeros of a polynomial or rational function are elements $a \in \mathbb{F}$ with $f(a) = 0$ or $r(a) = 0$. A *pole* of a rational function is an $a \in \mathbb{F}$ so that $g(a) = 0$ and $f(x) \neq 0$. If $f(a) = 0$ and $g(a) = 0$, then you simplify f and g by dividing out the common factor $(x - a)$.

Ideal

An *ideal* is a subset of a ring, $I \subset R$. An ideal is an additive subgroup of R: if $x \in I$ and $y \in I$, then $x + y \in I$. An ideal is *closed under multiplication* by any element of R. If $a \in R$ and $x \in I$, then $ax \in I$. For any $a \in R$, there is the *principal ideal*, written (a), that consists of all multiples of a by elements of R:

$$(a) = \{ax \mid x \in R\} \ .$$

A *principal ideal domain* is a ring in which every ideal is a principal ideal. Some of the most basic rings, such as $\mathbb{Z}$ and $\mathbb{F}[x]$ (a polynomial ring over a field) are principal ideal domains. Fancier rings may not be.

It is possible that $S \subset R$ is a sub-ring but not an ideal. A sub-ring is a set that is a subgroup under addition and a sub-semigroup under multiplication. That means that if $x \in S$ and $y \in S$, then xy and $x+y$ and $-x$ are in S. It does not require that $ax \in S$ if $a \notin S$. For example, $\mathbb{Z} \subset \mathbb{Z}[x]$ is a sub-ring but not an ideal. The product of two integers is an integer, but the product of an integer $x \in S = \mathbb{Z}$ with a polynomial $a \in R = \mathbb{Z}[x]$ is not an integer if $\deg(a) > 0$.

Quotient ring

The quotient of a ring R by an ideal I is written R/I. It is something like a quotient group under the operation of addition, but that is not the whole story because R/I is a ring with addition and multiplication, not just a group with addition. If $I \subset R$ is an ideal and $a \subset R$ is an element, then the *coset* of a is

$$\overline{a} = \{a + x \mid x \in I\} \ .$$

You "remember" (look it up if you don't remember) from group theory that cosets $\overline{a}$ and $\overline{b}$ either are disjoint or are identical. If $c \in \overline{a}$ and $x \in \overline{b}$, then $\overline{c} = \overline{a} = \overline{b}$. You also know that if $c = a + b$ then $\overline{c} = \overline{a + b}$. That implies that the $+$ operation can be defined on cosets as $\overline{a} + \overline{b} = \overline{a + b}$ and this is well defined. That would be true if I were only an additive subgroup. If I is an ideal and $c = ab$, then $\overline{c} = \overline{ab}$. Threfore $\overline{a} \cdot \overline{b} = \overline{ab}$ can define multiplication of multiplication of cosets. This makes the set of cosets into a ring, which is the quotient R/I.

You should check these claims to see how the verifications work. You might want to warm up with the special case where $R = \mathbb{Z}$ and $I = (n)$. In this case $a' \in \overline{a}$ is the same as $a \equiv a' \mod n$. (Check that you believe this.) You need to check that if $a \equiv a' \mod n$ and $b \equiv b' \mod n$ then $a + b \equiv a' + b' \mod n$ and $ab = a'b' \mod n$.

Exercises

These exercises are "routine verifications" that illustrate how the definitions work. That doesn't mean you can easily "get" all of them. Please ask for hints if you get stuck, and/or look in a textbook. You should also make sure you can verify the many claims above.

1. Suppose $R \overset{\phi}{\mapsto} S$ is a ring homomorphism. Show that $I = \ker(\phi)$ is an ideal in R.

2. Suppose $R = \mathbb{C}[x]$ and $\lambda \in \mathbb{C}$ with $\lambda \neq 0$. Consider the *scaling map* $f_\lambda(x) = f(\lambda x)$. Show that this defines an automorphism of $\mathbb{C}[x]$. Call this automorphism $S_\lambda : \mathbb{C}[x] \mapsto \mathbb{C}[x]$. Consider the *translation map* $f^a(x) = f(x + a)$. Show that this is an automorphism and call it T_a.

3. The set of automorphisms of a domain is called $\text{aut}(D)$. Show that this is a group "under composition". That means that if $\phi \colon D \mapsto D$ and $\psi \colon D \mapsto D$ are two automorphisms of D, then $\phi\psi$ is another automorphism defined by $(\phi\psi)(x) = \phi(\psi(x))$.

   (a) Show that $S_\lambda S_\mu = S_{\lambda\mu}$.

   (b) Show that $T_a T_b = T_{a+b}$.

   (c) Show that the composition operation in $\text{aut}(D)$ is associative, find the identity of this group, and show that every element has an inverse.

(d) Show that an automorphism group does not have to be abelian ever if the underlying domain is abelian. Specifically, show that $S_\lambda T_a \neq T_a S_\lambda$.

4. A *proper* ideal is $I \subset R$ with $I \neq R$. Show that (0) is the only proper ideal of a field.

5. Let $R = \mathbb{F}[x]$ be the one variable polynomial ring and $I = \{f \in R \mid f(0) = 0\}$.

   (a) Show that I is the principal ideal generated by the polynomial $x \in \mathbb{F}[x]$.

   (b) Show that R/I is isomorphic to $\mathbb{F}$. *Hint*: For $f \in \mathbb{F}[x]$, define $\phi f = f(0)$ (an evaluation map). Show that if $f' \in \overline{f}$, then $\phi(f') = \phi(f)$. This implies that the number $\phi(\overline{f})$ is well defined. That makes ϕ a map from $R/$ to $\mathbb{F}$. Show that this ϕ is a homomorphism, that it is into and onto.

6. Let $R = \mathbb{R}[x, y]$ be the ring of polynomials in x and y with real coefficients. Let $I \subset R$ be the set of polynomials that vanish at the origin, which is $f(0, 0) = 0$. Show that I is not a principal ideal. *Hint.* If $I = (f)$ (a principal ideal generated by the polynomial f), then $x = u(x, y)f(x, y)$ for some polynomial $u(x, y)$ and $y = v(x, y)f(x, y)$ for some other polynomial $v(x, y)$. Let $f(x, y) = f_{00} + f_{10}x + f_{01}y + f_{20}x^2 + \cdots$, and similarly for u and v. The x equation is $x = u_{00}f_{00} + (u_{10}f_{00} + u_{00}f_{01})x + \cdots$. This implies that $u_{00} = 0$ or $f_{00} = 0$ or both. If $u_{00} = 0$ then $u_{10}f_{00} = 1$, so $f_{00} \neq 0$. If $f_{00} = 0$, then $u_{00}f_{10} = 0$, so $f_{10} \neq 0$. Keep going like this until you find a contradiction.

Corrections

- January 31, exercise 2 corrected to replace $\mathbb{S}[x]$ by $\mathbb{C}[x]$.