A

Review of commutative algebra

This appendix collects definitions and results from basic algebraic geometry which will be freely referenced in the course. In some cases being familiar with them is required to follow the lecture; in other cases they are used to illustrate how real algebraic geometry differs from its complex counterpart. Many texts on commutative algebra may be consulted for proofs and more details. For example, [DF04] is a comprehensive resource.

Ring and field. A *ring* $\mathcal{R}$ in this course will always be commutative and come with a multiplicative unit 1. A *unit* in $\mathcal{R}$ is an element which has a multiplicative inverse and if every non-zero element is a unit, then $\mathcal{R}$ is a *field*. An element $a \in \mathcal{R} \setminus \{0\}$ is a *zero divisor* if there is a $b \in \mathcal{R} \setminus \{0\}$ such that $a \cdot b = 0$. It is *nilpotent* if b can be chosen as a power of a. No unit can be a zero divisor.

Characteristic and prime field. The presence of $1_{\mathcal{R}}$ lets us define a canonical ring homomorphism $\mathbb{Z} \to \mathcal{R}$ which sends $1_{\mathbb{Z}}$ to $1_{\mathcal{R}}$. If this homomorphism is injective, then $\mathcal{R}$ is said to have *characteristic* 0. Otherwise there is a smallest positive integer d whose image under this homomorphism is $0_{\mathcal{R}}$ and this integer is then the *characteristic* of $\mathcal{R}$. The characteristic of a field is either 0 or a prime. There is a unique smallest field inside every field which is its *prime field*. There is precisely one prime field per characteristic: $\mathbb{F}_p$ for prime characteristic $p > 0$ and $\mathbb{Q}$ in case of characteristic zero.

Fraction field. If $\mathcal{R}$ has no zero divisors, then it is an *integral domain*. In this case, we may define its *fraction field* $\mathsf{ff}(\mathcal{R})$. This is a ring whose elements are the classes of formal fractions a/b with $a, b \in \mathcal{R}$ and $b \neq 0$ modulo the equivalence relation

$$\frac{a}{b} \sim \frac{c}{d} \;:\Leftrightarrow\; ad = bc.$$

Addition and multiplication are defined as usual for fractions. Since every non-zero element a/b has an inverse b/a, $\mathsf{ff}(\mathcal{R})$ is a field and we have a canonical ring embedding $\mathcal{R} \hookrightarrow \mathsf{ff}(\mathcal{R})$ via $a \mapsto a/1$.

Field extension and algebraic closure. Two fields in inclusion $\mathbb{F} \subseteq \mathbb{F}'$ form a *field extension*. This is also written as $\mathbb{F}'/\mathbb{F}$. If $a \in \mathbb{F}'$ is a root of some polynomial $0 \neq f \in \mathbb{F}[x]$, then a is *algebraic* over $\mathbb{F}$; otherwise it is *transcendental*. If a is algebraic, then among all polynomials f of which a is a root, there is a unique monic and irreducible one which is the *minimal polynomial* of a over $\mathbb{F}$. Any extension $\mathbb{F}'$ is also a vector space over $\mathbb{F}$ whose dimension is the *extension degree*. The algebraic extension $\mathbb{F}(a)$ is finite and its degree is the degree of the minimal polynomial of a.

Theorem A.1: Primitive element theorem. Let $\mathbb{F}$ be a perfect field. Then every finite extension $\mathbb{F}'/\mathbb{F}$ has a primitive element, i.e., $a \in \mathbb{F}'$ such that $\mathbb{F}' = \mathbb{F}(a)$.

A field is *perfect* if it has characteristic zero (which is the case relevant in this course) or if has characteristic p and every element is a p^{th} root.

A field is *algebraically closed* if it has no proper algebraic extension. An algebraically closed and algebraic extension of a field $\mathbb{F}$ is an *algebraic closure*.

Theorem A.2: Algebraic closure. Every field $\mathbb{F}$ has an algebraic closure. The algebraic closure is unique up to unique $\mathbb{F}$-isomorphism.

The proof of this theorem requires a useful lemma from poset theory:

Zorn's lemma. Let $(P, \leq)$ be a poset in which every chain has an upper bound. Then $(P, \leq)$ has a maximal element.

Ideal and variety. A set $\{\,0\,\} \subseteq \mathcal{I} \subseteq \mathcal{R}$ is an *ideal* if $\mathcal{I} + \mathcal{I} \subseteq \mathcal{I}$ and $\mathcal{R} \cdot \mathcal{I} \subseteq \mathcal{I}$ where the operations are performed pairwise for all the elements of either set. Notice how ideals generalize the notion of "zero" in a ring. The quotient structure $\mathcal{R}/\mathcal{I}$ consisting of all cosets of $\mathcal{I}$ in $\mathcal{R}$ has again a well-defined ring structure.

Theorem A.3: Homomorphism theorem. Let $\varphi : \mathcal{R} \to \mathcal{R}'$ be a ring homomorphism. Then $\mathcal{I} = \ker \varphi$ is an ideal in $\mathcal{R}$ and we have $\mathcal{R}/\mathcal{I} \cong \operatorname{im} \varphi$.

For every ideal $\mathcal{I}$ in $\mathcal{R}$ we have the canonical homomorphism $\mathcal{R} \to \mathcal{R}/\mathcal{I}$ whose kernel is exactly $\mathcal{I}$. Hence, ideals are nothing but kernels of ring homomorphisms.

A ring is *noetherian* if every chain of ideals eventually stabilizes. This ensures that every ideal is finitely generated.

Theorem A.4: Hilbert's basis theorem. A polynomial ring over a noetherian ring is noetherian. In particular, every ideal in $\mathbb{F}[x_1, \ldots, x_n]$ is finitely generated.

To an ideal $\mathcal{I} \subseteq \mathbb{F}[x_1, \ldots, x_n]$ we associate the *variety*

$$\mathcal{V}(\mathcal{I}) \coloneqq \{\, a \in \mathbb{F}^n : f(a) = 0 \text{ for all } f \in \mathcal{I} \,\}.$$

Conversely, the *vanishing ideal* of any subset of $V \subseteq \mathbb{F}^n$ is

$$\mathcal{I}(V) \coloneqq \{\, f \in \mathbb{F}[x_1, \ldots, x_n] : f(a) = 0 \text{ for all } a \in V \,\}.$$

Theorem A.5: Hilbert's Nullstellensatz. Let $\mathbb{F}$ be algebraically closed and $\mathcal{I}$ an ideal in $\mathbb{F}[x_1, \ldots, x_n]$. Then $\mathcal{I}(\mathcal{V}(\mathcal{I})) = \sqrt{\mathcal{I}} \coloneqq \{\, f \in \mathbb{F}[x_1, \ldots, x_n] : \exists m \geq 0 : f^m \in \mathcal{I} \,\}$.

The ideal $\sqrt{\mathcal{I}}$ appearing in this theorem is the *radical* of $\mathcal{I}$. It can be formed by apply $\mathcal{I}(\mathcal{V}(-))$ to an ideal. The operation $\mathcal{V}(\mathcal{I}(-))$ applied to a subset $V \subseteq \mathbb{F}^n$ is referred to as *Zariski closure* and further explained below.

Theorem A.6: Alternatives in algebraic geometry. Let $\mathbb{F}$ be any field and $f_i, g_j \in \mathbb{F}[x_1, \ldots, x_n]$. Then exactly one of the following two cases occurs:

(a) There exists a point $a \in \mathsf{acl}(\mathbb{F})^n$ with $f_i(a) = 0$ and $g_j(a) \neq 0$ for all i and j.
(b) There exist $h_i \in \mathbb{F}[x_1, \ldots, x_n]$ and $m \geq 0$ such that $\sum_i f_i h_i = \left(\prod_j g_j\right)^m$.

The condition (b) in the above theorem is equivalent to $0 \in \mathcal{I} + \mathcal{U}$, i.e., the element-wise sum of the ideal $\mathcal{I}$ generated by the f_i and the multiplicative monoid $\mathcal{U}$ generated by the g_j in $\mathbb{F}[x_1, \ldots, x_n]$. However, $0 \in \mathcal{I} + \mathcal{U}$ is absurd when the solution space is non-empty, for every point in the solution space evaluates to zero on every element of $\mathcal{I}$ and to non-zero on every element of $\mathcal{U}$. This shows that either there exists a point in the solution set of the polynomial system all of whose coordinates are algebraic numbers over $\mathbb{F}$ or there exists an algebraic proof of the unsolvability of the system in the form of a polynomial in $\mathcal{I} \cap \mathcal{U}$ which has coefficients in $\mathbb{F}$.

Irreducible variety. The varieties in $\mathbb{F}^n$ form the closed sets of the *Zariski topology*. Every closed set has an essentially unique decomposition has a union of *irreducible* varieties. A variety is irreducible if and only if its vanishing ideal $\mathcal{I}$ is *prime*, i.e., whenever $ab \in \mathcal{I}$ already $a \in \mathcal{I}$ or $b \in \mathcal{I}$. Clearly, $\mathcal{I}$ is prime if and only if $\mathcal{R}/\mathcal{I}$ is an integral domain. The *dimension* if an irreducible variety is the maximal length of a chain of irreducible varieties inside it. For a reducible variety, the dimension is the maximum over its irreducible components.