ALGEBRAIC GEOMETRY

DE-QI ZHANG (OWNER OF COPYRIGHT)

(Professor of Mathematics; Office: S17-0608)

12th June 2021

Contents

1 Assessment: HWs, Presentations, Final Exam; References; Syllabus

Assessment

1. Homeworks ??, ??, ??, ?? and ?? to be submitted one week after being assigned **[40%].**

2. Each one presents a topic in §?? **[20%].**

3. Final examination **[40%].**
   Can bring in one $A4$-size double-sided handwritten or typed help sheet (**but might be open-book zoom exam**).

References: (1) - (4) are main, while (5) - (15) are extra.

1. Miles Reid, Undergraduate Algebraic Geometry, London Math.Society, Student Texts **12**. (QA1 Lmss 12)

2. Miles Reid, Chapters on Algebraic Surfaces, in:
   http://homepages.warwick.ac.uk/ masda/surf/ParkC/
   or preprint available at: https://arxiv.org/abs/alg-geom/9602006

3. R. Hartshorne, Algebraic Geometry, GTM 52, 1977.

4. H. Matsumura, Commutative ring theory, Cambridge studies in advanced mathematics 8, 1986.

5. Iitaka, Algebraic Geometry, an Introduction to Birational Geometry of Algebraic Varieities, GTM 76, 1982.

6. J. Kollar and S. Mori, Birational Geometry of Algebraic Varieties, Cambridge University Press, 1998.

7. Y. Kawamata, K. Matsuda and K. Matsuki, Introduction to the Minimal Model Problem, in: Advanced Studies in Pure Mathematics, 1987: 283-360 (1987), available at: https://doi.org/10.2969/aspm/01010283

8. James E. Humphreys, Linear Algebraic Groups, Ch I : Algebraic Geometry, GTM 21, 1981

9. W. Fulton, Algebraic Curves: an introduction to algebraic geometry, Addison-Wesley Pub. Co., Advanced Book Program, 1989.

10. A. Beauville, Complex Algebraic Surfaces, Cambridge, New York, Cambridge University Press: 1996. 2nd ed.

11. Yu. I. Manin, Cubic form : Algebra, geometry, arithmetic, North-Holland, 2nd ed, 1986.

12. W. Barth, K. Hulek, C. Peters and A. Van de Ven, Compact complex surfaces, 2nd ed., Springer-Verlag, Berlin, 2004.

13. M. F. Atiyah and I. G. Macdonald, Introduction to commutative algebra, Addison-Wesley Pub. Co . 1969.

14. Thomas W. Hungerford, Algebra, GTM73, Springer

15. J. A. Dieudonné, History of algebraic geometry : an outline of the history and development of algebraic geometry Monterey, Calif. : Wadsworth Advanced Books & Software , c1985.

Prerequisites:

MA2202 Algebra I (Basics of group theory) is fully assumed.

MA3201 Algebra II, MA5203 Graduate Algebra I, or MA5204 Graduate Algebra IIA will be assumed.

1. MA2202 module description: This course introduces basic concepts in group theory such as the notion of subgroups, permutation groups, cyclic groups, cosets, Lagranges theorem, quotient groups and isomorphism theorems. Major topics: Divisibility, congruences. Permutations. Binary operations. Groups. Examples of groups including finite abelian groups from the study of integers and finite non-abelian groups constructed from permutations. Subgroups. Cyclic groups. Cosets. Theorem of Lagrange. Fermat's Little Theorem and Euler's Theorem. Direct products of groups. Normal subgroups. Quotient groups. Isomorphism Theorems.

2. MA3201 module description: The objective of this module is to provide the essentials of ring theory and module theory. Major topics: rings, ring isomorphism theorems, prime and maximal ideals, integral domains, field of fractions, factorization, unique factorization domains, principal ideal domains, Euclidean domains, factorization in polynomial domains, modules, module isomorphism theorems, cyclic modules, free modules of finite rank, finitely generated modules, finitely generated modules over a principal ideal domain.

3. MA5203 module description: This module is designed for graduate students in both pure and applied mathematics. It covers topics from the five basic areas of groups, rings, modules, fields and multi-linear algebra, including group actions, Sylow theorems, Jordan-Holder theorem, semisimple modules, chain conditions, bimodules, tensor products and localizations, algebraic, separable and normal field extensions, algebraic closures, multilinear forms, quadratic forms, symmetric and exterior algebras.

4. MA5204 module description: This module is a basic introduction to commutative and homological algebra. It covers the following topics: prime spectrum of a commutative ring, exact sequences, projective, injective and flat modules, Ext and Tor, integral ring extensions, Noether's normalization and Hilbert's Nullstellensatz, Noetherian and Artinian rings and moduels, dimension theory,

Dedekind domains and discrete valuation ring.

Module syllabus:

MA5208 Algebraic Geometry, Module description (from Math Dept website):

This module is a first course in algebraic geometry, introducing the basic objects (varieties) and basic geometric constructs and notions (products, fibers of morphisms, dimensions, tangent spaces, smoothness) with applications to curves and surfaces. It is suitable for students who intend to work in number theory, representation theory, algebraic geometry and topology and geometry in general.

2 Some History of Algebraic Geometry

Bernard Riemann (**1826** $\sim$ **1866**) classified one dimensional complex manifolds, which are now called *Riemann surfaces* (over $\mathbb{R}$). There are many things named after him: Riemann Mapping Theorem, Riemann Hypothesis (one of the six remaining Clay Mathematics Institute Millennium Prize Problems) and also Riemann-Roch Theorem, one of its version was proved by F. Hirzebruch (a **Fields Medalist**).

Other well known concepts: Dedekind domain, Kronecker's field extension theorem, Max Noether formula, Picard number and group, Lefschetz fixed point theorem (see also the M. Atiyah (a **Fields Medalist**) - Singer holomorphic version), Poincaré duality, E. Cartan matrix, Hilbert's 23 problems (the fourteen's problem was negatively solved by M. Nagata). André Weil's conjecture on generating functions = local zeta functions, was proved by Bernard Dwork (1960) for the rationality, Alexander Grothendieck (1965), a **Fields Medalist**, on the function equation, and Pierre Deligne (1974), a **Fields Medalist**, on the analogue of the Riemann hypothesis.

The Italian school ($\sim$ **1920**), led by Enriques, Castelnuovo, Severi, Fano, classified 2-dimensional algebraic manifolds. The classification of two dimensional complex manifolds was finished by K. Kodaira (**Fields Medalist**) in 1950's. The Kodaira dimension (defined by his student S. Iitaka) is a very important birational/bimeromorphic invariant in the minimal model program (MMP) (see Ch **??**).

Oscar Zariski first went to Italy to learn Algebraic Geometry, with the supervisor being Guido Castelnuovo. He realized the necessity to make the foundation of algebraic geometry more solid. He defined, around **1940**'s, the so called *Zariski topology* and built every thing of Algebraic Geometry upon **commutative rings**. He was the one who established the foundation of Algebraic Geometry. See also André Weil's "Foundations of Algebraic Geometry". Zariski also nurtured a lot of PhD students (18 PhD students and 1954 descendants according to Mathematics

Genealogy as of 3rd June 2021) including S. Abhyankar (resolved singularities of 3-dimensional spaces defined over the field of characteristic $p > 5$), M. Artin (former President of the American Math. Soc), R. Hartshorne (the author of the bible-like GTM 52: Algebraic Geometry), H. Hironaka (**Fields Medalist** who resolved the singularities of complex spaces), D. Mumford (**Fields Medalist** and the former President of the International Congress of Mathematicians).

J. Lerray invented the notion of *Sheaf*, which was further developed by H. Cartan and J.-P. Serre (**Fields Medalist**). J.-P. Serre also discovered the one-to-one correspondence between objects in Algebraic Geometry and Complex Geometry (the GAGA principle).

A. Grothendieck (**Fields Medalist**) introduced, around 1957, the new concept of *Scheme*, which is a union of affine subspaces as Zariski open subsets. The affine spaces $\mathbf{C}^n$ and the projective spaces $\mathbf{P}^n$ are important schemes.

S. Mori (**Fields Medalist**, and student of Nagata) made the breakthrough by establishing the existence of flips for threefolds, in Journ. Amer. Math. Soc. Vol. 1 (**1988**))), thus completing the **Minimal Model Program** (= **MMP**, or Mori's program) in dimension ≤ 3, the contribution of which also comes from Y Kawamata, J Kollár, Miles Reid, V V Shokurov et al. Precisely, the MMP conjectures (a theorem in dimension ≤ 3) that every complex algebraic variety X is either birational to some X' with a Fano fibration $X' \to Y$ (with $\dim Y < \dim X$) or has a minimal model X' such that the canonical divisor $\mathcal{O}(K_{X'}) \simeq \det(T_{X'})^\vee$ is numerically effective, i.e., $\deg \mathcal{O}(K_{X'})|_C \geq 0$ for every curve C on X'.

Andrew Wiles (the only silver-plaque winner awarded so far, by the Fields Medal committee) proved the Fermat's last theorem in 1994 asserting that every rational solution of the equation $X^n + Y^n = Z^n$ satisfies $XYZ = 0$, based on the works of G. Faltings (**Fields Medalist**), G. Shimura, K. Ribet, et al.

In some different aspect, **S.T. Yau** (**Fields Medalist**) solved in 1980's the Calabi Conjecture: the existence of Kähler-Einstein metric on manifolds with trivial canonical divisor. The Miyaoka-Yau inequality saying that $c_1^2 \leq c_2$ for general type

surface (with also higher dimensional analogues) is due to Yau and Y. Miyaoka independently in 1977. Now the study of Calabi-Yau manifolds is very active among physicists (who predict the number of rational curves ($\cong \mathbf{P}^1$) of any given degree, on complex spaces like quintic threefolds) and Algebraic Geometers (who prove rigorously). A little bit later, S. Donaldson (**Fields Medalist**) identified the concept of anti-self dual connections in the study of Yang-Mills fields (Physicist and Nobel Prize Laureate, and his PhD student) with the concept of stable bundles in Algebraic Geometry, and defined Donaldson invariant to distinguish smooth 4-manifolds (over $\mathbb{R}$), which was further extended by Seiberg and Witten (**Fields Medalist**).

Recently, **Caucher Birkar** (the only twice Fields medalist 2018, the first medal being stolen), and P. Cascini, C. Hacon, and J. McKernan [Existence of minimal models for varieties of log general type, J. Amer. Math. Soc. 23 (2010), 405-468], built on fundamental work of **V. V. Shokurov**, have made big breakthrough in proving the existence of KLT flips in any dimension, the finite generation of canonical ring and generalizing Mori's result to higher dimensions (the analytic approach is by Y. T. Siu); see §**??** for details.

The relation between algebra and geometry is very close as demonstrated in the recently solved **Yau-Tian-Donaldson** conjecture, due to Chen-Donaldson-Sun and Tian, asserting the equivalence of existence of Kähler-Einstein metric on Fano manifolds and K-stability in algebraic language. The papers are: [X. Chen, S. K. Donaldson, and S. Sun, Journal of the American Mathematical Society, 28 (2015) 183–278; [Tian, G., K-stability and Kähler-Einstein metrics. Communications on Pure and Applied Mathematics, 68 (2015) pp.1085–1156.

Very recently, Caucher Birkar, has solved the Borisov-Alexeev-Borisov (**BAB**) conjecture claiming that Fano varieties of fixed dimension with at most ϵ-lc singularities are in a bounded family, thus earning him the Fields medal. His papers are published as: Singularities of linear systems and boundedness of Fano varieties, Ann. of Math, 193, No. 2 (2021), 347–405; Anti-pluricanonical systems on Fano varieties, Ann. of Math. Vol. 190, No. 2 (2019), pp. 345–463; the MMP for generalized pairs,

used in solving BAB, was developed in the early paper (solving Iitaka's conjecture of 1970): Effetivity of Iitaka fibrations and pluricanonical systems of polarized pairs, Pub. Math. IHES., 123 (2016), 283–331 (Joint with De-Qi Zhang).

For the latest developement/advancement on MMP, see [Hacon and Liu, Existence of flips for generalized lc pairs, arXiv:2105.13590]

3 Quick Revision of Basics of Commutative Algebra

Some basic knowledge of **ring theory, field theory, module theory, and general toplology** will be assumed without proof. In this section, we **quickly** recall some basic things in commutative algebra to be used in the sequel of the course, including:

Artinin ring/module, Cohen-Macaulay ring/module, Depth of a module, Embedding dimension, Height of a prime idea, Hilbert basis theorem, Krull dimension, Local ring, Localization, Nakayama lemma, Noether's normalizaiton, Noetherian ring/module, Normal ring, Regular ring, Regular sequence of a module, Serre's normality criterion.

Definition 3.1. (**Group**) A set G together with an operation $*$:

$$* : G \times G \to G,$$

$$(g_1, g_2) \mapsto g_1 * g_2 (= g_1 g_2)$$

is called a *group* if the following are satisfied:

(a) (the existence of identity) there is an element $e = e_G \in G$ such that

$$ge = eg = g, \quad \forall \ g \in G;$$

(b) (the inverse) for each $g \in G$, there is an inverse $g^{-1} \in G$ such that

$$g^{-1}g = e = gg^{-1}; \text{ and}$$

(c) (associativity) for all $g_i \in G$, one has

$$(g_1 g_2)g_3 = g_1(g_2 g_3).$$

We use $(G, *)$ to denote the group G with the operation $\times$.

Definition 3.2. (**Abelian group**) A group $(G, *)$ is *abelian* (or *commutative* or *additive*) if

$$g_1 * g_2 = g_2 * g_1, \quad \forall \ g_i \in G;$$

if this is the case, we may use

$$(G, +, 0), \quad \text{or} \quad (G, +)$$

to denote the abelian group with the addition operation "+" and the additive identity 0 (the additive inverse of g is denoted by $-g$, called the *negative* of g); thus,

$$g + 0 = 0 + g,$$
$$g + (-g) = 0,$$
$$(g_1 + g_2) + g_3 = g_1 + (g_2 + g_3).$$

Example 3.3.

(a) The set $\mathbf{Z}$ of integers, the set $\mathbf{Q}$ of rational numbers, the set $\mathbf{R}$ of real numbers and the set $\mathbf{C}$ of complex numbers all have additive group structures with the natural addition operation "+".

(b) The sets

$$\mathbf{Q}^* := \mathbf{Q} \setminus \{0\}, \ \mathbf{R}^* := \mathbf{R} \setminus \{0\}, \ \mathbf{C}^* := \mathbf{C} \setminus \{0\}$$

with the natural multiplication $''\times''$, are commutative (= abelian) multiplicative groups.

Definition 3.4. (**Ring**) A set R with a plus operation $+$ and a multiplication operation $\times$ is a *ring* and denoted as $(R, +, \times)$, if:

(a) $(R, +, 0)$ is an additive group,

(b) (associativity for the multiplication)

$$(r_1 r_2) r_3 = r_1 (r_2 r_3), \quad \forall \ r_i \in R, \quad \text{and}$$

(c) (distribution law)

$$(r_1 + r_2)r_3 = r_1r_3 + r_2r_3,$$
$$r_1(r_2 + r_3) = r_1r_2 + r_1r_3, \ \forall \ r_i \in R.$$

Definition and Exercise 3.5. *(***Commutative ring with** 1*)*

(a) $(R, +, \times)$ *is a ring with* $1 = 1_R$ *if* $1 \neq 0$ *and*

$$1\, r = r\, 1 = r, \ \ \forall \ r \in R.$$

Show that such 1_R *is unique.*

(b) A ring R *is commutative if*

$$r_1r_2 = r_2r_1, \ \forall \ r_i \in R.$$

Example 3.6. $(\mathbf{Z}, +, \times)$, $(\mathbf{Q}, +, \times)$, $(\mathbf{R}, +, \times)$ and $(\mathbf{C}, +, \times)$ are all commutative rings with 1, where $+$ and $\times$ are the natural operations.

Definition 3.7. (**Field**) A commutative ring $(R, +, \times)$ with 1 is a *field* if $(R^*, \times)$ is a multiplicative group, where $R^* = R \setminus \{0\}$.

Definition and Exercise 3.8. *(***Polynomial ring; Fraction field***)*

(a) $\mathbf{Q}$, $\mathbf{R}$ *and* $\mathbf{C}$ *are all fields. But* $\mathbb{Z}$ *is not a field (why?)*

(b) Let R *be a commutative ring with* 1*. Then the polynomial ring*

$$R[x_1, \ldots, x_n]$$

over R *in* n*-variables* $x_1, \ldots, x_n$*, is again a commutative ring with* 1*.*

(c) Let k *be a field. Then one can define the fraction field* $k(x_1, \ldots, x_n)$ *(which is a field) of the polynomial ring* $k[x_1, \ldots, x_n]$ *as*

$$k(x_1, \ldots, x_n) =$$
$$\{f/g \,|\, f,\, g \,\in k[x_1, \ldots, x_n],\, g \neq 0\}.$$

In general, if R is an integral domain (see below), one can define the fraction field $Q(R)$ of R as

$$Q(R) = \{r_1/r_2 | r_i \in R, r_2 \neq 0\}.$$

Definition 3.9. (**Module**) A (left) R-**module** (or a **module** over R) is an additive abelian group M together with a binary **scalar multiplication** (or **scalar action**)

$$R \times M \to M$$

$$(r, m) \mapsto rm.$$

such that for all $r, s \in R$ and all $u, v \in M$, the following axioms are satisfied.

(1) (distributive law)

$$r(u + v) = ru + rv,$$

$$(r + s)u = ru + su.$$

(2) (associativity)

$$r(su) = (rs)u.$$

(3) for the unity $1 = 1_R \in R$, we have

$$1u = u.$$

If in addition, R is a division ring (or a field) an R-module M is called a (left) **vector space**.

Remark 3.10.

(1) *In this section we consider only left R-module. The theory of right R-module is similar.*

(2) If R is commutative, a left R-module M has a natural $R - R$ **bimodule** structure, by simply defining the right scalar action as $vr := rv$ for $r \in R$, $v \in M$.

Example 3.11. Every additive abelian group M is a $\mathbb{Z}$-module in a natural way. So the study of abelian groups is part of that of modules.

Example 3.12. Let I be a (two-sided) ideal in R (see below for definition). Then the quotient ring $M := R/I$ has a natural R-module structure, if we define the scalar multiplication as follows:

$$R \times R/I \to R/I$$
$$(r, \bar{s}) \mapsto \overline{rs}.$$

Example 3.13. If R is a ring, then R has a natural left R-module structure by defining the scalar action of $r \in R$ to $x \in R$ as the natural product rx.

From now on until the end of this section, by a ring R, we mean (unless specified) that R is a commutative ring with 1.

Definition and Exercise 3.14. *(***Ideal***) A subset J of a ring R is an ideal if:*

$$j_i \in J \implies j_1 \pm j_2 \in J,\ j_1 j_2 \in J$$
$$j \in J,\ r \in R \implies rj \in J.$$

Show that $J = R \Leftrightarrow 1_R \in J$.

Definition 3.15. (**Finitely generated ideal; Principal ideal; Unit**)

(a) Fix $r_1, \ldots, r_s \in R$. Then

$$\begin{aligned}&(r_1, \ldots, r_s)\\ &= Rr_1 + \cdots + Rr_s\\ &= \{\sum x_i r_i \,|\, x_i \in R\}\end{aligned}$$

is an ideal and called the *ideal generated* by $r_1, \ldots, r_s$.

(b) Fix an $r \in R$. Then

$$(r) = Rr = \{xr \,|\, x \in R\}$$

is called the *principal* ideal generated by r.

(c) $u \in R$ is a *unit* if $uv = 1$ for some $v \in R$.

Exercise 3.16. (1) Show: $u \in R$ is a unit $\Longleftrightarrow (u) = R$.

(2) If $u \in R$ is a unit then $(ur) = (r)$ for any $r \in R$. Conversely if R is an integral domain and $(ur) = (r)$ for some $r \neq 0$, then $u \in R$ is unit.

Definition 3.17. (**Homomorphism; Isomorphism**) A map

$$f : R_1 \to R_2$$

between rings is a *ring-homomophism* if:

(a) (preserve addition)

$$f(r_1 + r_2) = f(r_1) + f(r_2), \quad \forall \ r_i \in R_1;$$

(b) (preserve multiplication)

$$f(r_1 r_2) = f(r_1) f(r_2), \ \forall \ r_i \in R_1; \ \text{and}$$

(c) (preserve the identity)

$$f(1_{R_1}) = 1_{R_2}.$$

Note that (c) follows from (a) and (b) if R is an integral domain and $f \neq 0$.

A ring-homomophism $f : R_1 \to R_2$ is an *isomorphism* if it is bijective.

Exercise 3.18. Show that a ring-homomorphism $f : R_1 \to R_2$ is an isomorphism if and only if

$$g \circ f = \mathrm{id}_{R_1}, \qquad f \circ g = \mathrm{id}_{R_2}$$

for some ring-homomorphism $g : R_2 \to R_1$. If this is the case, $g = f^{-1}$ (the inverse of f) is also a ring-isomorphism.

Definition and Exercise 3.19. *Let $J \ (\neq R)$ be an ideal of a ring $(R, +, \times)$. Define a relation $\sim$ on R:*

$$r_1 \sim r_2 \Longleftrightarrow r_1 - r_2 \in J.$$

Show that $\sim$ is an equivalence relation.

Denote by

$$\overline{r} = r + J = \{r + j \,|\, j \in J\}$$

the equivalence class (or the coset) containing r. Let

$$R/J := \{\overline{r} \,|\, r \in R\}$$

be the set of all equivalence classes.

Define two operations $+, \times$ on R/J:

$$\overline{r}_1 + \overline{r}_2 := \overline{r_1 + r_2}, \quad \overline{r}_1 \overline{r}_2 := \overline{r_1 r_2}.$$

Exercise 3.20. (**Quotient ring**)

(a) Show that $+, \times$ are well defined on R/J (independent of the choice of the representative r_i of the class $\overline{r}_i$).

(b) Show that $(R/J, +, \times)$ is a ring with 1, called the *quotient ring* of R modulo the ideal J. Setting $\bar{R} := R/J$, one has

$$0_{\bar{R}} = \overline{0_R}, \qquad 1_{\bar{R}} = \overline{1_R}.$$

(c) Show that in $\bar{R}$ we have:

$$\overline{r} = 0_{\bar{R}} \iff r \in J,$$
$$\overline{r_1} = \overline{r}_2 \iff r_1 - r_2 \in J.$$

(d) Show that

$$\gamma : R \to R/J$$
$$r \mapsto \overline{r}$$

is a ring-homomorphism (called the *quotient map*).

Definition and Exercise 3.21. *(***Ideal and Kernel***)*

(a) If $f : R_1 \to R_2$ is a ring-homomorphism then the kernel

$$\operatorname{Ker} f := f^{-1}(0) = \{r \in R_1 \mid f(r) = 0\}$$

is an ideal of R_1.

(b) For the quotient map $\gamma : R \to R/J$ in 3.19, one has $\operatorname{Ker}\gamma = J$.

(c) By (a) and (b), for a ring R, one has

$$\{\textit{ideals} \subseteq R\} = \{\operatorname{Ker} f\,;\, f : R \to \ \textit{(a ring) is a hom.}\}.$$

Theorem 3.22. (Fundamental Theorem of Ring Theory). *Let $f : R_1 \to R_2$ be a ring-homomorphism. Then there is a ring-isomorphism*

$$\overline{f} : R_1/(\operatorname{Ker} f) \ \cong\ \operatorname{Im} f\ (\subseteq R_2)$$

such that

$$f \ = \ \overline{f} \circ \gamma$$

where

$$\gamma : R_1 \ \longrightarrow\ R_1/(\operatorname{Ker} f)$$

is the quotient map (see 3.19*).*

Definition 3.23. (**Integral domain**) A ring R is an *integral domain* if

$$r_1 r_2 = 0 \implies r_1 = 0, \ \text{ or } \ r_2 = 0.$$

Exercise 3.24. (**Integral domain means cancellation law**) Show the following:

(1) R is an integral domain if and only if the concellation law holds:

$$rx = ry,\ r \neq 0 \implies x = y.$$

(2) Any field is an integral domain.

Definition and Exercise 3.25. *(***Prime ideal***) An ideal P of a ring R is a prime ideal if the following equivalent conditions are satisfied:*

(a) R/P is an integral domain;

(b) $p_1 p_2 \in P \Longrightarrow p_1 \in P$, or $p_2 \in P$.

Show that (a) and (b) are equivalent.

Definition and Exercise 3.26. *(***Maximal ideal***) An ideal M of a ring R is a maximal ideal if the following equivalent conditions are satisfied:*

(a) R/M is a field (called the residue field); and

(b) $M \neq R$, and there is no any ideal J such that

$$M \subset J \subset R.$$

(1) Show that (a) and (b) are equivalent.

(2) Show that a maximal ideal is a prime ideal.

Exercise 3.27. (**Irreducible v.s. Prime v.s. Maximal**)

(a) Let k be a field. Then the polynomial ring $k[x_1, \ldots, x_n]$ is an integral domain. In general, if R is an integral domain, then so is the polynomial ring $R[x_1, \ldots, x_n]$ over R. Hint: induction on n.

(b) Let $f \in k[x_1, \ldots, x_n]$ be a non-constant polynomial. Then (f) is a prime ideal if and only f is *irreducible* (i.e., f is non-constant and $''f = f_1 f_2'' \Rightarrow ''f_i \in k^* = k \setminus \{0\}''$ for $i = 1$ or 2). Hint: $k[x_1, \ldots, x_n]$ is UFD (cf. 3.34).

(c) If $n \geq 2$, then (x_1) is a prime ideal of $k[x_1, \ldots, x_n]$ but not a maximal ideal.

(d) For $J = (f) \subseteq k[x]$, one has:

$$f \text{ is irreducible } \Longleftrightarrow$$

$$J \text{ is prime } \Longleftrightarrow$$

$$J \text{ is maximal .}$$

(e) Is (d) true for $J = (f(x)) \subseteq k[x, y]$?

Definition 3.28. (**Euclidean domain**) An integral domain R is a *Euclidean domain* if there is a *valuation*

$$\nu : R \setminus \{0\} \longrightarrow \mathbf{Z}_{\geq 0}$$

satisfying:

(a) For any a, $b \in R$ with $b \neq 0$, there are q, $r \in R$ such that

$$a = bq + r$$

where

$$r = 0, \text{ or } \nu(r) < \nu(b); \text{ and}$$

(b) For all non-zero $a, b \in R$,

$$\nu(a) \leq \nu(ab).$$

Exercise 3.29.

(a) Let k be a field. Then both k and $k[x]$ are Euclidean domains.

Hint: Define $\nu(f) := \deg(f)$.

(b) The Gaussian integer ring

$$\mathbf{Z}[i] = \{a + bi \,|\, a, b \in \mathbf{Z}\}$$

is an Euclidean domain, where $i = \sqrt{-1}$.

Hint: Define (cf. [Fraleigh, Th 6.8]):

$$\nu(a + bi) := a^2 + b^2.$$

Definition 3.30. (**PID**) An integral domain R is a PID (*principal ideal domain*) if every ideal J of R is principal : $J = (r)$.

Exercise 3.31.

$$\text{Euclidean} \implies \text{PID}.$$

In particular, $k[x]$ and $\mathbf{Z}[i]$ are PID.

Definition 3.32. (**UFD**) An integral domain is a UFD (*unique factorization domain*) if:

(a) (*factorization*) for any nonzero and non-unit $r \in R$, one has a *prime decomposition* (or *irreducible decomposition*; see 3.33 below):

$$r = p_1 \cdots p_n$$

with p_i *prime* (i.e., (p_i) is a prime ideal); and

(b) (*uniqueness*) when

$$r = q_1 \cdots q_m$$

is another prime decomposition, one has, after relabelling, $m = n$ and $(q_i) = (p_i)$ so that

$$q_i = p_i \times (\text{a unit}).$$

A nonzero and non-unit element $r \in R$ is *irreducible* if

$$r = r_1 r_2 \implies r_1, \text{ or } r_2 \text{ is a unit.}$$

An element $r \in R$ is *prime* if the principal ideal (r) is a prime ideal of R.

Exercise 3.33. (**Irreducible = Prime in a UFD**)

(1) Show that for a non-zero and non-unit element p in a UFD R,

$$p \in R \text{ is prime} \iff p \text{ is irreducible.}$$

Give an example to show the necessity of assuming R to be UFD in the assertion above.

(2) Show that (a) $\Rightarrow$ (b) in Definition 3.32.

Exercise 3.34.

(a) PID $\Longrightarrow$ UFD.

(b) R is UFD $\Longrightarrow$ $R[x]$ is UFD (cf. [Fraleigh, Th 6.3]).

(c) In particular, every polynomial ring $k[x_1, \ldots, x_n]$ over a field k is a UFD.

Definition 3.35. (**Integral elements**) Let $R \subseteq S$ be integral domains. An element $s \in S$ is *integral over* R if there is a *monic* polynomial $f(x)$ (i.e., the leading coeffcient of $f(x)$ is 1)

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

such that $f(s) = 0$.

Definition and Exercise 3.36. *(***Integral closure; Normal ring***) Show that*

$$\widetilde{R}_S := \{s \in S \,|\, s \text{ is integral over } R\}$$

is a subring of S (cf. [Matsumura, Th 9.1]) and called the integral closure of R in S. Note that

$$R \subseteq \widetilde{R}_S \subseteq S.$$

For an integral domain R with fraction field $Q(R)$, let

$$\widetilde{R} := \{t \in Q(R) \,|\, t \text{ is integral over } R\}$$

be the integral closure of R in its fraction field $Q(R)$. Then we have

$$R \subseteq \widetilde{R} \subseteq Q(R).$$

An integral domain R is normal if $\widetilde{R} = R$.

Exercise 3.37.

$$R \text{ is } \text{ UFD } \Longrightarrow R \text{ is normal.}$$

In particular, every polynomial ring $k[x_1, \ldots, x_n]$ over a field k, is normal.

Theorem 3.38. *(***Ring of fractions***) Let R be a commutative ring and let D be a set with $\emptyset \neq D \subseteq R \setminus \{0\}$ which does not contain any zero divisors and is closed under multiplication (i.e., $a, b \in D \Rightarrow ab \in D$). Then there is a commutative ring $Q = D^{-1}R$ with 1 such that:*

(1) Q contains R as a subring.

(2) Every element of D is a unit in Q.

(3) Every element of Q is of the form $r\, d^{-1}$ for some $r \in R$ and $d \in D$.

Remark 3.39.

(1) In $D^{-1}R$, when $d \in D$, we usually denote

$$r\, d^{-1} := \frac{r}{d} = r/d.$$

(2) The addition $+$ and multiplication $\times$ in $Q = D^{-1}R$ are given as follows

$$\begin{aligned} r_1/d_1 \,+\, r_2/d_2 \;&=\; (r_1 d_2 + r_2 d_1)/(d_1 d_2), \\ (r_1/d_1)\,(r_2/d_2) \;&=\; (r_1 r_2)/(d_1 d_2). \end{aligned}$$

(3) The multiplicative identity

$$1_Q = d/d$$

for any $d \in D$.

(4) The inclusion $R \to D^{-1}R$ is given by

$$\begin{aligned} R \;&\to\; D^{-1}R \\ r \;&\mapsto\; rd/d \end{aligned}$$

for any $d \in D$, noting $rd/d = rd_1/d_1$ for any $d, d_1 \in D$.

Definition 3.40. (**Ring of fractions**)

(1) The ring $Q = D^{-1}R$ in Theorem 3.38 is called the **ring of fractions of D with respect to R.**

(2) (**Fraction field of an integral domain**) If R is an integral domain and $D = R \setminus \{0\}$ we call $D^{-1}R$ the **fraction field of** R and denoted as $Q(R)$. Namely,

$$Q(R) = D^{-1}R.$$

Corollary 3.41.

(1) Suppose that R is a nonzero subring of a field F. Then the fraction field $Q(R)$ of R is the subfield of F generated by R. Namely,

$$Q(R) = \{\alpha \in F \,|\, \alpha = \frac{r_1}{r_2},\, r_i \in R, r_2 \neq 0\}.$$

(2) More generally, suppose R is an integral domain and $Q = Q(R)$ its fraction field. If $\sigma : R \to F$ is an injective ring homomorphism to a field F, then σ extends to an injective homomorphism

$$\sigma' : Q(R) \to E =: \{\alpha \in F \,|\, \alpha = \frac{\sigma(r_1)}{\sigma(r_2)},\, r_i \in R, r_2 \neq 0\} \subseteq F.$$

Here $E = Q(\sigma(R))$ is the fraction field of the integral domain $\sigma(R)$ and is the subfield of F generated by $\sigma(R)$.

Definition 3.42. (**Local ring**) A commutative ring R with $1 \neq 0$, is called a **local ring** if it has a unique maximal ideal (say M).

Example 3.43.

$$R = \{m/n \,|\, m, n \in \mathbb{Z}; 2 \not| n\}$$

is a subring of $\mathbb{Q}$.

$$M = (2)$$

is the unique maximal ideal of R. Hence R is a local ring.

Example 3.44. (**Localisation**) Let R be an integral domain and P a prime ideal. Then $D := R \setminus P$ satisfies the condition of Theorem 3.38. Denote by

$$R_P := D^{-1}R$$

which is called the **localisation of** R **at** P. Then

$$PR_P = \{a/d \,|\, a \in P,\, d \notin P\}$$

is the only maximal ideal in R_P so that R_P is a local ring. Here note that $d \in D$ if and only if $d \notin P$.

For instance, if $R = F[x]$ is the polynomial ring over a field F and $P = (x)$, then

$$R_P = \{f(x)/g(x) \,|\, g(0) \neq 0\}$$

and

$$P\,R_P = xR_P = \{f(x)/g(x) \,|\, f(0) = 0, g(0) \neq 0\}.$$

Here $f(0) = 0$ means the constant term of $f(x)$ is zero.

Definition 3.45. (**ACC; DCC**) Let M and N modules under the (left, right or two-sided) scalar actions of some ring.

(1) M is said to satisfy the **Ascending Chain Condition** (ACC) on submodules (or to be **Noetherian**) if for every chain

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

of submodules of M, there is an integer $n \geq 1$ such that $M_i = M_n$ for all $i \geq n$.

(2) N is said to satisfy the **Descending Chain Condition** (DCC) on submodules (or to be **Artinian**) if for every chain

$$N_1 \supseteq N_2 \supseteq N_3 \supseteq \cdots$$

of submodules of N, there is an integer $m \geq 1$ such that $N_i = N_m$ for all $i \geq m$.

Definition 3.46. (**(Left/right) Noetherian; (Left/right) Artinian**)

(1) R is left (resp. right) **Noetherian** if R satisfies the Ascending Chain Condition (ACC) on left (resp . right) ideals.

R is said to be **Noetherian** if R is both left and right Noetherian.

(2) R is left (resp. right) **Artinian** if R satisfies the Descending Chain Condition (DCC) on left (resp . right) ideals.

R is said to be **Artinian** if R is both left and right Artinian.

Definition 3.47. (**Maximal/Minimal element**) Let $(C, \leq)$ be a partially ordered set.

- $a \in C$ is a **maximal** element if for every $c \in C$ which is comparable to a, we have $c \leq a$.
- Note: it is not necessarily true that $c \leq a$ for all $c \in C$.
- **Minimal elements** can be defined similarly.
- C may contain many maximal or minimal elements or none at all.

Definition 3.48. (**Maximum/Minimum condition**) (cf. [Hungerford, ChVIII, Theorem 1.4]) A module M is said to satisfy the **maximum condition** (resp. **minimum condition**) on submodules if every nonempty set of submodules of M contains a maximal (resp. minimal) element (with respect to set theoretic inclusion).

Below is a variation of **Zorn's lemma** and follows from the **Axiom of Choice**. It will be frequently used.

Theorem 3.49. *(**ACC/DCC = Maximum/Minimum condition**)(cf. [Hungerford, ChVIII, Theorem 1.4]) A module M satisfies the Ascending (resp. Descending) Chain Condition on submodules if and only if M satisfies the maximal (resp. minimal) condition on submodules.*

Theorem 3.50. *(**Hilbert's Basis Theorem**)* (cf. [Matsumura, Th 3.3])

(a) If R is Noetherian then so is $R[x]$.

(b) Every polynomial ring $k[x_1, \ldots, x_n]$ over a field k is Noetherian.

(c) Every algebra finitely generated over a field k is Noetherian.

Definition and Remark 3.51. *(CM =* **Cohen-Macaulay ring, Depth, Regular sequence***)*

(1) An integral ring R is normal if and only if the localization R_m is normal for every maximal ideal m of R, if and only if R_p is normal for every prime ideal p of R. See Matsumura book or [Iitaka GTM76, page 103, Corollary].

In the following assume R is a Noetherian local ring (see definition below) with maximal ideal m_R.

(2) **Serre's normality criterion***: R is normal if and only if it satisfies $R_1 + S_2$, i.e., regular in codimension 1 (i.e., the local ring R_p is regular for every height 1 prime idea p of R) and the length of a maximal m_R-regular sequence is at least 2. See below and Matsumura book.*

(3) R is reduced if and only if it satisfies R_0 and S_1.

(4) R is called being **Cohen-Macaulay** *(CM) if satisfies $\operatorname{depth}(R) = \dim R$, i.e., the depth of R equals the Krull-dimension of R (see below for definitions). One has a similar definition for CM (finite) R-modules M.*

In general, we have $\operatorname{depth}(M) \leq \dim M := \dim R/\operatorname{Ann}_R(M)$.

*Recall that a sequence $r_1, \ldots, r_s \in R$ of length s is an M-***regular sequence** *if r_{i+1} is not a zero divisor of the quotient module $M/(r_1, \ldots, r_i)M$. Our $\operatorname{depth}(M)$ is the maximal length of such regular sequence.*

Definition 3.52. (**Height**) Let R be an integral domain and $P \subset R$ a prime divisor. The *height* $\operatorname{ht}(P)$ of P is defined as the maximal $s \geq 0$ labelling the chain of prime ideals (between (0) and P) as follows:

$$(0) \subset P_1 \subset \cdots \subset P_s = P.$$

Exercise 3.53. Let $R = k[x_1, \ldots, x_n]$ be the polynomial ring over a field k, and let $P = (x_1 - a_1, \ldots, x_n - a_n)$ be a maximal ideal. Show that $\operatorname{ht}(P) = n$.

Definition 3.54. (**Krull dimension**) Let R be an integral domain. Define the Krull dimension of R as:

$$\dim R = \max\{\mathrm{ht}(P) \mid P \text{ is a maximal ideal of } R\}.$$

Remark and Question 3.55. *(***Catenary ring***) A Noetherian local integral domain R (cf. 3.57), is called catenary if*

$$\mathrm{ht}\, P + \dim(R/P) = \dim R$$

for every prime ideal $P \subset R$. (In general, LHS $\leq$ RHS). A regular local ring (cf. 3.59) is Cohen Macaulay; Cohen Macaulay rings and their quotients are catenary; every normal ring of dimension ≤ 2 is catenary; see [Matsumura, 17.8, 17.9, 23.8, 31.4].

Nagata constructed a Noetherian local integral domain R which is not catenary; thus it has two 'saturated' chains between (0) and the maximal ideal with different lengths.

If M_1, M_2 are two maximal ideals of a (Noetherian) ring, is it true that $\mathrm{ht}\, M_1 = \mathrm{ht}\, M_2$*?*

*The answer is yes for every polynomial ring $k[x_1, \ldots, x_n]$ with $k = \bar{k}$ by the Nullstellensatz in §**??**.*

Exercise 3.56. Show that the Krull dimension $\dim k[x_1, \ldots, x_n] = n$, for the polynomial ring $k[x_1, \ldots, x_n]$ over a field.

Definition 3.57. (**Embedding dimension**) Recall that a ring R with only one maximal ideal P is called a *local ring*. Then the quotient R-module P/P^2 can be regarded as a $k := R/P$ module. We call

$$\mathrm{emb}\dim(R) := \dim_k P/P^2$$

the **embedding** dimension of R (cf. **??** for the geometric meaning of it).

In particular, if R is Noetherian (and hence $P = Rp_1 + \cdots + Rp_m$ for some $p_i \in P$) then $P/P^2 = k\overline{p_1} + \cdots + k\overline{p_m}$ and $\mathrm{emb}\dim(R) \leq m$.

Theorem 3.58. *(***Nakayama's lemma***) (cf. Matsumura book) Let R be a commutative ring with 1_R. The* **Jacobson radical** *$J(R) = \cap_{P:maximal} P$ is the intersection of all maximal ideals of R. Let M be a finite R-module. Then we have:*

(1) Let I be an ideal in R. If $I\,M = M$, then there exists an $r \in R$ with $r = 1$ (mod I) such that $rM = 0$.

(2) If $J(R)M = 0$ then $M = 0$.

(3) If N is a submodule of R such that $M = N + J(R)M$, then $M = N$.

(4) If the images of elements $m_1, \ldots, m_s$ of M in $M/J(R)M$ generate quotient module $M/J(R)M$ as an R-module, then $m_1, \ldots, m_s$ also generate M as an R-module.

Definition and Exercise 3.59. *(***Regular local ring***) Let (R, P) be a Noetherian local ring. Then* $\operatorname{emb\,dim}(R)$ *is the smallest number of elements needed to generate P as an R-module (you may need to use the Nakayama's lemma).*

In general, for a Noetherian ring R, we have (cf. [Matsumura, Th 13.4]):

$$\dim R \leq \operatorname{emb\,dim} R.$$

In particular, $\dim R$ *is finite (cf. 3.57).*

A Noetherian local ring R is a regular local ring if

$$\dim R = \operatorname{emb\,dim} R$$

i.e., the Krull dimension of R equals the embedding dimension of R.

Exercise 3.60. For the polynomial ring $R = k[x_1, \ldots, x_n]$ over a field and

$$P = (x_1 - a_1, \ldots, x_n - a_n)$$

a maximal ideal of R, the subring (called the localization of R at P)

$$R_P := \{r/s \,|\, s \in S := R \setminus P\}$$

of $Q(R)$ has a single maximal ideal

$$\begin{aligned} PR_P :&= \{pr \,|\, p \in P,\, r \in R_P\} \\ &= \{p/s \,|\, p \in P,\, s \in S := R \setminus P\} \end{aligned}$$

so that (R_P, PR_P) is a local ring. Show that R_P is regular.

Conversely, we have **Cohen's structure theorem** below:

Theorem 3.61. (cf. [Hartshorne, Ch I, Th 5.4A, Th 5.5A]). *Let (R, P) be a Noetherian local ring and let*

$$\hat{R} = \varprojlim R/P^n$$

be the completion. Then there is a natural inclusing $R \subseteq \hat{R}$ so that $\hat{R}$ is a local ring with $\hat{P} := P\hat{R}$ its only maximal ideal. Further, we have:

(1) R is a regular ring if and only if so is $\hat{R}$.

(2) Suppose that (A, P) is a Noetherian complete local ring (like $\hat{R}$ above) containing a field. Then A is a regular ring if and only if

$$A \cong k[[x_1, \ldots, x_n]]\, (= k[\widehat{x_1, \ldots, x_n}])$$

(the ring of formal power series) where $n = \dim A$ and $k = A/P$ (the residue field).

Remark 3.62. (**Regular v.s. UFD. v.s. Normal**) *Auslander-Buchsbaum* proved that a regular local ring is UFD (cf. [Matsumura, Th 20.3]). Thus for a local ring R, we have (cf. 3.35):

$$R \text{ is regular } \Rightarrow \text{ R is UFD } \Rightarrow \text{ R is normal.}$$

When $\dim R = 1$,

$$R \text{ is normal } \Rightarrow \text{ R is regular.}$$

The above is not true when $\dim R \geq 2$.

Theorem 3.63. (cf. [Fraleigh, Th 8.14]) *(***Primitive element theorem***) Let $F \subset E$ be a finite field extension which is separable (or with* $\operatorname{char} F = 0$*). Then there is some $a \in E$ such that*

$$E = F(a) = F[a].$$

Theorem 3.64. (cf. [Reid, UAG, 3.13, 3.17]) (**Noether's normalization theorem**) Let k be a field with $|k| = \infty$, and $A = k[a_1, \ldots, a_n]$ a finitely generated k-algebra. Then there are $y_1, \ldots, y_m \in A$ for some $m \leq n$, such that

(1) $y_1, \ldots, y_m$ are algebraically independent over k, i.e., $k[y_1, \ldots, y_m]$ is isomorphic to the polynomial ring in m variables;

(2) A is a finite $R := k[y_1, \ldots, y_m]$-algebra, i.e., $A = \sum_{i=1}^{s} Rb_i$ for some $b_i \in A$; and

(3) the fraction field

$$Q(A) = k(y_1, \ldots, y_{m+1})$$

for some $y_{m+1} \in A$.

The $m := \operatorname{trans\,deg}_k A$ is called the *transcendence degree* of A over k.