# A REFRESHER IN COMMUTATIVE RING THEORY

Algebraic number theory uses a lot of algebra. You will need to have fresh in mind everything you learned in your graduate course(s) of algebra, especially the basic theory of commutative ring ideals and modules, and the theory of field extensions, including basic Galois theory.

This refresher is a sequence of questions and exercises intended to help you review part the basic material of algebra that we will use all the time in this class. Most of them are very simple – if you know well the relevant definitions. A few could take more thinking.

## 1. Basic notions

(1) Define (mentally) the following notions and answer (mentally) the following questions:
A commutative ring $R$;
a unit in $R$ (= an element of $R^*$);
the group of unitd in $R$;
the relation of divisiblity $a|b$ for $a|b$ in $R$; is this relation an order ?
an irreducible element in a ring; what are the irreducible elements in $\mathbb{Z}$?
a domain; the fraction field of a domain;
a module $M$ over $R$; a sub-module $N$ of $M$; A module quotient $M/N$; an ideal of $R$ (that is a sub-module of $R$); a set of generators of a module; a free module; Show that if $I$ is an ideal of $R$, $R/I$ has a natural structure of commutative ring.
For two ideals $I$ and $J$, define the ideald $I+J$, $IJ$, $I \cap J$. Show that $IJ \subset I \cap J$. Give an example where this inclusion is (resp. is not) an equality.
A maximal ideal; every ideal is included in a maximal ideal (Krull's lemma);

In what follows $R$ is a commutative ring and $I$ is an ideal of $R$.

(2) A very important trivial fact : the map $J \mapsto J/I$ is a *bijection* between the set of ideals of $R$ containing $I$ and the set of ideals of $R/I$.

(3) Show that $R$ is a field if it has no ideal excepted $(0)$ and $R$; Deduce (using 2) that $I$ is maximal if and only if $R/I$ is a field.

(4) $I$ is a *prime* if for $x, y \in R$, $xy \in I$ implies that $x \in I$ or $y \in I$. Show that $R$ is domain if and only if $(0)$ is a prime ideal. Show that $I$ is prime if and only if $R/I$ is a domain.

(5) Show that a maximal ideal is prime (combine 3 and 4 – you can also give a direct proof).

(6) What are the prime and maximal ideal of $\mathbb{Z}$. Is the converse of 5) true?

(7) Let $f : R \to R'$ be a morphism of commutative rings. Let $\mathfrak{p}$ be a prime ideal of $R'$. Show that $f^{-1}(\mathfrak{p})$ is prime. Special case (why is it a special case ?) : If $R \subset R'$, and $\mathfrak{p}$ is a prime ideal of $R'$, then $\mathfrak{p} \cap R$ is a prime ideal of $R$.

Show by an example that $\mathfrak{p}$ can be maximal without $f^{-1}(\mathfrak{p})$ being maximal.

(8) Show that if $\mathfrak{p}$ is a prime of $R$ and $I_1, \ldots, I_n$ are ideals of $R$ such that $\mathfrak{p} \supset I_1 \ldots I_n$, then $\mathfrak{p} \supset I_k$ for some $k$.

(9) Two ideals $I$ and $J$ of $R$ are said relatively prime if $R = I + J$. Show that if this holds $R/(I \cap J) \simeq R/I \times R/J$. Generalise with $n$ pairwise relatively prime ideals (Chinese remainder theorem).

## 2. Principal ideals

(10) An ideal is *principal* if it is generated by one element. A ring is a *Principal Ideal Domain* (PID) if it is a domain whose all ideals are principal. Show that if $R$ is a PID, then every prime ideal is either (0) or a maximal ideal. (The converse is not true - we will meet many counter-examples)

(11) If $R$ is a commutative ring, $R[X]$ is a PID if and only if $R$ is a field. (Hint: To show that if $R[X]$ is a PID, then $R$ is a field, consider the ideal $(r, X)$ for $r$ a non zero element of $R$, and using that this ideal is principal, prove that $r$ is invertible.)

(12) Show that the ring $\mathbb{Z}$ is a PID

(13) review mentally or with a book the theory of finite (that is finitely generated) modules over a principal ring.

## 3. Noetherian rings

(14) Show that in a ring $R$ the following properties are equivalent
   (i) Every increasing sequences of ideal of $R$ is stationary.
   (ii) Every set of ideals of $R$ has a maximal element.
   (iii) Every ideal of $R$ is finitely generated.

   Such a ring is called Noetherian.

(15) Try to prove Hilbert's Theorem : if $R$ is noetherian, so is $R[X]$. Or look it up in a book.

(16) Prove that if $R$ is noetherian, then so is any quotient ring $R/I$. Deduce that if $R$ is noetherian, ny finitely generated $R$-algebra is noetherian.

(17) If $R$ is noetherian, is any subring of $R$ noetherian?

(18) In a noetherian ring, show that any element is a product of irreducible elements.

(19) In a noetherian ring, show that any ideal contains a product of prime ideals.

(20) if $R$ is a noetherian ring, and $M$ a finitely generated (aka finite) module $M$ show that
  (i) Every increasing sequences of submodules of $M$ is stationary.
  (ii) Every set of submodules of $M$ has a maximal element.
  (iii) Every submodule of $M$ is finitely generated.

(21) Let $R$ be a noetherian ring, $M$ a finite $R$-module, and $f : M \to M$ a surjective map. Show that $f$ is injective. (Hint: consider the sequence $\ker f \subset \ker f^2 \subset \cdots \subset \ker f^n \subset \dots$).

(22) Show that the result of the preceding exercise is true without assuming $R$ noetherian. (This is harder. First assume that $M$ is free, and try to "reduce to the noetherian case").

(23) Let $R$ be a noetherian domain, $K$ its fraction field. A *fractional ideal* of $A$ is a finitely generated $A$-submodule of $K$. Show that all fractional ideals have the forms $x^{-1}I$ where $I$ is an ideal of $A$ and $x \in A - \{0\}$.

## 4. Modules over a domain

Let $R$ be a domain, $K$ its fraction field. Let $M$ be an $R$-module.

(24) Show that the kernel of the natural map $M \to M \otimes_R K$ is the torsion part of $M$. We define the (generic) *rank* of $M$ as the $K$-dimension of $M \otimes K$. Show that the rank is additive, namely if $N$ is a sub-module of $M$, the rank of $M$ is the rank of $N$ plus the rank of $M/N$.

(25) if $R$ is noetherian, show that an $R$-module that is finitely generated and torsion free is a submodule of finite free module.

(26) If $R$ is noetherian, and $M$ is an $R$-module, show that $M$ is a torsion free finite module of rank one if and only if $M$ is isomorphic as an $R$-module to a fractional ideal of $R$ (this is also true with *ideal* instead of*fractional ideal*)

Show that for such an $R$-module $M$, the fractional ideal to which it is isomorphic is well-determined up to multiplication by an element in $K^*$.

## 5. UFDs

(27) Look up or recall the precise definition of a UFD. Show that a PID is an UFD.

(28) Look up or redo the proof that if $A$ is an UFD, so is $A[X]$.

(29) Prove that in any ring $R$ a principal ideal that is prime is $R$ has an irreducible generator. Prove that if $R$ is an UFD, any ideal generated by an irreducible element is prime.

(30) Show that $\mathbb{C}[X,Y,Z]/(XY-Z^2)$ is not a UFD– though it is a domain.

## 6. Integral elements

(31) Let $A \subset B$ be two domains, and $x$ in $B$ Look up somewhere, or remember the definitions of $x$ being an integral element over $A$. Of the algebraic closure of $A$ in $B$. Of $A$ being integrally closed.

(32) Show that if a ring is an UFD, then it is integrally closed.

(33) Is the ring $k[X^2, X^3]$ integrally closed ($k$ a field)?

(34) Let $A$ be a domain, $K$ its fraction field, $L$ an algebraic field over $K$, and $B$ the algebraic closure of $A$ in $K$. Show that for every $x \in L$, there is an $a \in A$, $a \neq 0$ such that $ax \in B$.

(35) Let $A$ be a domain, $B$ a domain containg $A$ and integral over $A$, and $I$ a non zero ideal of $B$. Show that $I \cap A \neq 0$.

## 7. Localization

Let $A$ be a domain (for simplicity, and because that will be sufficient for our needs) with filed of fraction $K$, and $S$ a multiplicative subset of $A$ such that $0 \notin A$. Recall that we denote $S^{-1}A$ the subring of all elements that can be written $a/s$, $a \in A$, $s \in S$.

(36) Show that if $A$ is integrally closed, so is $S^{-1}A$.

(37) Show that there is a bijection $I \to S^{-1}I$ between proper ideals of $A$ that do not meet $S$, and proper ideals of $S^{-1}A$.

(38) Show that if $A$ is noetherian, so is $S^{-1}A$.

(39) Recall that if $\mathfrak{p}$ is prime, $S = A - \mathfrak{p}$ is multiplicative and we note $A_\mathfrak{p}$ for $S^{-1}A$. Show that $A_p$ is a local ring, with $\mathfrak{p}A_\mathfrak{p}$ as the unique maximal ideal.

(40) Let $M$ be a finite module over $A$, which we assume now to be a noetherian domain. Look up or recall the meaning of the following properties and the proof that they are equivalent:
- $M$ is flat;
- $M$ is projective;
- $M_\mathfrak{p} := M \otimes_A A_\mathfrak{p}$ is free for all primes $\mathfrak{p}$ of $A$