Algebra exam, M1 MF (3 hours)

D. Harari, K. Destagnol, P. Lorenzon

December 19, 2023

Every statement in the lecture notes (but not in the TD) can be used without proof. It is allowed to use the result of a question to solve a further question.

The symbol (*) stands for an a priori difficult question.

Exercise 1 : Index of a subgroup (6 points)

Let G be a group. Recall that the *index* $[G : H]$ of a subgroup H of G is the cardinality of the set G/H (we set $[G : H] = +\infty$ if this set is infinite).

a) Let N be a subgroup of G. Show that $[N : (N \cap H)] \leq [G : H]$.

b) Assume further $[G : H]$ finite. Show that we have equality in question a) if and only if $G = NH$, where NH is the set of all elements of G that can be written nh with $n \in N$ and $h \in H$.

c) Let $f : G \to G'$ be a morphism of groups. Let H' be a subgroup of G', set $H = f^{-1}(H')$. Show that if f is onto, then $[G : H] = [G' : H']$.

(*) d) Let p be a prime number. Let G be a p-group with $G \neq \{1\}$. Assume that G is not abelian. Show that G has a subgroup of index p (hint : proceed by induction on the cardinality of G).

e) Does the result of d) still stand if G is an abelian p-group ?

Exercise 2 : Dimension of a ring (5 points)

Let A be a non-zero commutative ring. Define the *dimension* of A as the upper bound (in $\mathbf{N} \cup \{+\infty\}$) of the integers $n \in \mathbf{N}$ such that there exists a strictly increasing sequence of prime ideals of A :

$$\wp_0 \subset \wp_1 \subset \ldots \subset \wp_n.$$

a) Show that A is of dimension zero if and only if every prime ideal of A is maximal.

b) Let k be a field and $n \in \mathbf{N}^*$. Find all prime ideals of $k[X]/(X^n)$, and deduce that $k[X]/(X^n)$ is of dimension zero.

c) Show that a principal ideal domain that is not a field is of dimension 1.

d) Show that if K is a field, then $K[X_1, ..., X_n]$ is of dimension at least n.

Exercise 3 : Modules of finite type (6 points)

Recall that if M is a module over a commutative ring A and I is an ideal of A, the piece of notation IM stands for the submodule of M generated by the elements of the form ax with $a \in I$ and $x \in M$. Let M be an A-module with $IM = M$. Let $w \in M$. Set $M' = M/(A.w)$ and assume that there exists $x \in I$ such that $(1 + x)M' = 0$.

a) Show that $(1+x)M \subset I.w$, where $I.w$ is the submodule of M consisting of the elements of the form $a.w$ with $a \in I$.

b) Choose $y \in I$ with $(1+x)w = yw$ (which is possible by a)). Show that $(1 + x - y)(1 + x)M = 0$.

c) Deduce that theres exists $z \in I$ such that $(1 + z)M = 0$.

(*) d) Let P be an A-module of finite type such that $IP = P$. Show that there exists $a \in A$ such that $aP = 0$ and $(a - 1) \in I$.

e) Assume further that for every maximal ideal J of A, we have $I \subset J$. Show that $P = 0$.

Exercice 4 : Galois theory (4 points)

An extension L/K of fields is said to be *abelian* (resp. *cyclic*) if it is finite, Galois, and has an abelian (resp. cyclic) Galois group.

a) Give an example of a finite Galois extension of $\mathbf{Q}$ which is not abelian.

b) Let L/K be a finite Galois extension. Let $K \subset F \subset L$ be an intermediate extension. Suppose L/K abelian ; are the extensions L/F and F/K always abelian ? Same question with cyclic instead of abelian.

(*) c) Let p be a prime number and $m \in \mathbf{N}^*$. Show that there exists a finite Galois extension L of $\mathbf{Q}$ with Galois group $\mathbf{Z}/p^m\mathbf{Z}$ (hint : consider a cyclotomic extension $\mathbf{Q}(\zeta)$, where ζ is a root of unity whose order in the multiplicative group $\mathbf{C}^*$ is a power of p).