Divers

Marc SAGE

Table des matières

1 Sur les idéux premiers et les localisés ;

Si a est un élément non nul d'un anneau (noethérien ?) A, existe-t-il un idéal premier minimal $\mathfrak{p}$ tel que a reste non nul dans le localisé $A_{\mathfrak{p}}$?

en fait c'est vrai ssi tout idéal premier associé de A (noetherien) est minimal. C'est le cas quand A est réduit, par exemple.

preuve : si c'est le cas et a est non nul, alors $\operatorname{Ann} a$ est contenu dans un idéal premier associé $\mathfrak{p}$, si bien que a reste non nul dans $A_{\mathfrak{p}}$, or $\mathfrak{p}$ est minimal. Réciproquement si $\mathfrak{p} = \operatorname{Ann} a$ est un idéal premier associé non minimal et $\mathfrak{q}$ est un idéal premier tel que a reste non nul dans $A_{\mathfrak{q}}$ alors forcément $\mathfrak{q}$ contient $\mathfrak{p}$ et $\mathfrak{q}$ ne peut être minimal.

2 SUr les idéeaux dans les anneaux

I remark that it is known that if every prime ideal is principal [resp. finitely generated], then every ideal is principal [resp. finitely generated]. How to prove this ?

I think we can drop the assumption on A being an integral domain, since this is implied by Tate's lemma (in a local version on $\operatorname{Sp} A$). Here is a sketch of proof :

A is Noetherian, since every prime is finitely generated. Let I be a non-zero ideal of A. Then there are finitely many prime overideals $\mathfrak{p}_1, ..., \mathfrak{p}_n$ of I. By a standard localization argument it suffices to assume that A is local (consider all the localizations of A at the $\mathfrak{p}_i$'s).

Now assume A be a Noetherian local non-trivial ring in which every prime is principal. For trivial reason we can assume that A be not a field and I is non-zero. Then, by Tate's lemma, A is an integral domain which implies that A is 1-dimensional. Denote by p the generator of the maximal ideal of A. Take some non-zero element i in I. Then the quotient ring ${}^{A}\!/_{iA}$ is artinian, such that there is some natural number $n > 0$ such that $p^n \in I$, but $p^{n-1} \notin I$. Thus ${}^{I}\!/_{p^n A}$ is a non-trivial submodule of the simple module ${}^{p^{n-1}A}\!/_{p^n A}$ over the field ${}^{A}\!/_{pA}$. Thus ${}^{I}\!/_{p^n A}$ is trivial or - in other words - $I = p^n A$.

3 The only complete archimedean fields are R and C

In brief, this starts by showing that one can assume that the complete archimedean field k contains $\mathbb{C}$, since if it does not, one can extend it to such a field.

Now suppose x is in k but not in $\mathbb{C}$.

Let c be the closest point of $\mathbb{C}$ to x.

Take $x - c$ in place of x.

Then $|x - z| \geq |x|$ for all z in $\mathbb{C}$.

Hence $|x^n - z^n| = |x - z|\,|x - \omega z|\,\left|x - \omega^2 z\right| \cdots \geq |x - z|\,|x|^{n-2}$ (where $\omega^n = 1$).

Choosing $|z| < 1$ and letting $n\infty$, it follows that $|x| \geq |x - z|$.

Hence $|x - z| = |x|$ and so (taking $x - z$ in place of x) $|x - 2z| = |x|$, and thus (repeating the argument) $|x - rz| = |x|$, contradicting the archimedean property.

4 Cardinalité des bases de clôtures algébriques

Il parait qu'il existe un théorème d'unicité du corps algébriquement clos de cardinalité fixé, mais j'aimerais savoir ce qu'il en est exactement (je suppose qu'il faut aussi fixer la caractéristique, n'est-ce vrai qu'en caractéristique nulle ?) et avoir une idée de comment cela se démontre (référence ?).

Précisément, les corps algébriquement clos (de caractéristique fixée) sont classifiés à isomorphisme près par le cardinal d'une base de transcendance sur le sous-corps premier k. (C'est facile : si l'on se donne une base de transcendance (x_i), ben le corps est une clôture algébrique de $k(x_i) \simeq k(X_i)$, et on est juste ramené à l'unicité de la clôture algébrique).

En cardinal dénombrable, on a donc plusieurs classe d'isomorphisme $(0, 1, 2, ..., \aleph_0)$, et une seule en un cardinal indénombrable quelconque.

Ils s'écrivent tous $F(p,I) := \left[F_p^{\text{alg}}(I)\right]^{\text{alg}}$ où p premier ou 0 et I cardinal (avec les conventions $F_0 = \mathbb{Q}$ et $K(I) := K\left((X_i)_{i\in I}\right)$)

Ma question est : y a-t-il des redondances ?

Evidemment si $L = F(p,I) \simeq F(p\prime, I\prime)$ alors $p = p\prime = car(L)$.

Mais si $L = F(p,I) \simeq F(p,I\prime)$, alors a-t-on $I = I\prime$?

On voit facilement que $\text{card}(F(p,I)) = \max(I, \aleph_0)$. Donc si $\text{card}(L) > \aleph_0$ alors $I = I\prime = \text{card}(L)$.

La question se réduit à : pour p fixé premier ou 0, les corps $F(p,I)$, $I \leq \aleph_0$ sont ils deux à deux non isomorphes ?

En tout cas le fait de savoir que $K -> (\text{car}(K), \dim \text{alg}_{F_p}(K))$ et $(p,I) -> F(p,I)^{F_0=Q}$ sont des bijections réciproques entre {classes d'isom de corps alg clos} et {nb premiers et 0}x{cardinaux} m'est très sympathique.

5 SUr les bases algébriques

Soit A une algèbre graduée sur un corps k de caractéristique 0.

On dit que $\{p_1, ..., p_k\}$est un système générateur minimal si il engendre A et si il est minimal pour l'inclusion. (ie $\{p_1, ..., p_k\}$ n'est pas générateur, etc).

Soit $\{p_1, ..., p_k\}$ et $\{p_1, ..., p_k\}$ deux systèmes générateurs minimaux de degrés respectifs $\{d_1, ..., d_k\}$ et $\{d'_1, ..., d'_k\}$. Alors :

- $k = k\prime$
- $d_i = d'_i$ pour tout i

Il me semble qu'il faut au moins que tu fasses les hypothèses suivantes :

* la partie de degré 0 de A est k

* les générateurs que tu considères sont homogènes sinon (à moins que je me sois trompé), c'est faux. Moyennant ces deux hypothèses, ça semble raisonnable.

6 Discriminant et Bézout

Est-ce qu'on sait quand une relation de Bezout entre deux polynômes de $\mathbb{Z}[X]$ reste dans $\mathbb{Z}[X]$?

En faisant l'hypothèse qu'un des polynômes est irréductible (et que les deux sont premiers entre eux et unitaires, ça ne pose pas de problème j'ai l'impression) et que l'anneau d'entiers du corps de nombres $Q[X]/(P)$ est égal à $\mathbb{Z}[\alpha]$, sauf erreur j'ai une équivalence entre l'existence d'une relation $UP + VQ = 1$ dans $\mathbb{Z}[X]$ et le fait que $Q(\alpha)$ soit une unité.

Si l'on a des polynômes unitaires, de façon que le déterminant de Sylvester se réduise comme on pense modulo p, ça veut juste dire que le résultant r de P et Q vaut 1 ou -1.

Dans ce cas-là, le critère donné par Pascal en début de thread est bien général. r est le produit des $Q(x_i)$ pour x_i les racines de P. Comme il vaut 1, ça impose que tous les $Q(x_i)$ soient des unités (dans l'anneau des entiers du corps de décomposition de P, ou bêtement dans l'anneau des entiers algébriques). Mais réciproquement, si tous ces trucs sont des

7 Trinômes sur corps fini

La question de comment factoriser les polynômes sur un corps fini fera l'objet d'un prochain texte : <URL : http ://www.dma.ens.fr/~madore/agreg/factor.pdf > (voir aussi <URL : http ://www.dma.ens.fr/~madore/mpri2006/mpri200
5.pdf >), mais bon, ici, y'a pas besoin d'aller chercher loin :

Dans le cas de la caractéristique 2, ce que tu veux est sans doute ceci : $z^2 + z + e = 0$ a une racine dans F_q (avec $q = 2^r$) si et seulement si $e + e^2 + e^4 + ... + e^{\frac{q}{2}} = 0$.

(Je laisse les détails en exercice. En bref : $e + e^2 + e^4 + ... + e^{\frac{q}{2}}$ ne peut valoir que 0 ou 1, il faut 0 si $e = z^2 + z$, et il y a $\frac{q}{2}$ éléments dans le sous-groupe de F_q image de $z \longmapsto z^2 + z$.)

Or j'ai déjà expliqué comment se ramener à $z^2 + z + e = 0$.

8 Polynôme annulateur d'une somme d'algébriques

En preparant un TD de DEUG1, nous nous sommes demandes si vous pouvions leur demander de prouver que la somme de deux nombres algebriques etait algebrique. Il s'agirait de trouver un polynome C qui annule a+b et qui s'exprime en fonction des polynomes A et B, A(a)=0, B(b)=0.

a+b est racine du polynome caracteristique de l'application lineaire "multiplication par a+b" de K(a,b) dans lui-meme. Or il se trouve que la matrice de cette application lineaire est particulierement simple dans la base de K(a,b) formee des a^i.b^j (en gros c'est plein de petites matrices compagnon dont les coefs sont ceux des polynomes de a et b), et le calcul de son polynome caracteristique est a la portee du premier DEUGard venu (enfin, si elle est pas trop grosse).

9 calcul des racines

pour calculer les racines d'un polynome, il est assez efficace de chercher les valeurs propres de sa matrice compagnon en utilisant des techniques du genre (?) Jacobi ; voir le bouquin de Ciarlet qui est a la bibli d'agreg.

10 Sur les composés de polynômes

On considere P et Q deux polynomes tels que

$$\begin{aligned} P &= X + a_1 X^2 + ... + a_n X^{n+1} \\ Q &= X + b_1 X^2 + ... + b_m X^{m+1} \\ P \circ Q &= X + c_1 X^2 + ... + c_{n+m+2} X^{m+n+2} \end{aligned}$$

Peut on montrer que, si $c_i = 0$ pour $i \leq m + n$, alors les a_i et les b_i sont nuls ?

Faux en carac 2, prendre $P = Q = X + X^2$. On a $n = m = 1$, et

$$P \circ P = X + X^2 + \left(X + X^2\right)^2 = X + X^2 + X^2 + X^4 = X + X^4.$$

11 polynômes irréductibles de tout degré

montrer que s'il existe un polynome irreductible de degre 3 sur un corps K donne, alors il existe des polynomes irreductibles de degre arbitrairement grand.
(bien sur K=R montre qu'on ne peut pas remplacer 3 par 2)

Par l'absurde : (supposons $\operatorname{car} K = 0$ pour simplifier). Si le degre des polynomes irreductibles sur K est borne par n , $\overline{K}$ est fini sur K (sinon contient une extension de degre $> n$ qui est monogene par le theoreme de l'element primitif, d'où un élément de poly min de degré $> n$).

Et ceci implique qu'en fait $K \hookrightarrow \overline{K}$ est de degre 2 (theoreme d'Artin-Lang), cf Algebra de Lang. Le point est que quand p est premier impair $X^p - a$ irreductible implique $X^{p^2} - a$ irreductible ce qui n'est pas vrai avec $p = 2$ ($X^2 + 4$ est irreductible sur $\mathbb{R}$ mais pas $X^4 + 4 = \left(X^2 + 2\right)^2 - 2X^2$).