Plan :

I) Notion de dénombrement

A) Ensemble fini
→ card des ens. + formule du crible + lemme des tiroirs
$|\mathcal{P}(E)| = 2^{|E|}$ ...

[VIG]

B) Parties d'un ensemble
→ p-liste, p-arrangement, permutation, combinaisons
prop. de $\binom{n}{k}$, binôme
...

C) Cardinal et fonctions :
injection, surjection ... ex

II) Dénombrement et algèbre

[ROM]

A) Théorie des groupes
→ action de groupe, orbites, stabilisateurs, éq. aux classes
Burnside

[PER]

[CAL]

B) Corps finis
$|Gl_n(\mathbb{F}_q)|$, $|Sl_n(\mathbb{F}_q)|$, symboles de legendre avec les prop. d'avant
+ $\boxed{\text{loi de réc. quad}}$ Dév ①
[CAL]

III) Fct arithmétiques :

[PER]

A) Indicatrice d'Euler
déf + prop ... + $[\mathbb{F}_q^*$ cyclique$]$

[FRA]

B) Fct de Möbius
↳ déf + premières prop. + $\boxed{\text{Formule d'inv + applic. au nbre de polyn irréd de } \mathbb{F}_q}$ dév 2 [FRA]

[FRA?]

C) Séries génératrices :
- explication séries ent ⇔ dénombrement + exemple
- déf Σ gén
- Nombre de Bell

Leçon [190] : Méthodes combinatoires et problèmes de dénombrements.

→ Rapport du jury :

- [x] Évoquer ≠ méthodes de dénombrement avec exemples
- [ ] Évoquer les ≠ domaines math. où il y a des Pb de dén.
- [x] Calculer des cardinaux classiques et probas
- [x] Connaître l'interprétation ensembliste de la somme des coeff bin.
- [x] Corps finis ⇔ lien avec alg. lin
- [ ] Fct de Möbius
- [x] Formule de Burnside

Dév

dénombremt polyn irréd de $\mathbb{F}_q$ + formule Möbius	Francinou - Gianella exercices maths agrégat° [FG]
Loi de récip. quad	H2G2 [Caldero]

[FG] + [CAL] + [PER] + [ROM]

[VIG] = Vigneron - Dénombrement et combinatoire

[COM] Combes, Algèbre et géométrie ?

[FRA] Algèbre 1 lequel ?

Plan détaillé [190] :

Dénombrement

I) Notion de dénombrement :

A) Ensemble fini :

On note E un ensemble fini à $n \in \mathbb{N}^*$ éléments.

[VIG] p.75

ROP$_1$: A, B parties de E

$A \subseteq E \Rightarrow card(A) \leq card(E)$

$card(A \cup B) + \bar{A} + A \setminus B + A \cup B \ldots$

THM$_2$: Formule du crible ~~de~~ ou de Poincaré

[VIG] p.76

op$_3$: Card d'une partit° d'un ens. fini

op$_4$: card d'un produit cartésien

op$_5$: $Card(\mathcal{P}(E)) = 2^{Card(E)} = 2^n$.

6 : exemples sur ensemble fini + calcul de probas...

p$_7$: (lemme des tiroirs) n+1 éléments répartis dans n ensembles ⇒ 1 ensemble (au -) contiendra ≥ 2 éléments.

pas de réf...

B) Parties d'un ensemble : E ensemble à $n \in \mathbb{N}^*$ éléments

[VIG] p.2-9

f$_8$: p-liste de E (↔ interprétat° tirage boule dans urne)

p$_9$: nbre de p-liste $= n^p$.

f$_{10}$: p-arrangement de E

m : exemple + ⚠ l'ordre compte + (interp. tirage sans remise)

p$_{11}$: nbre de p-arrangements : $A_n^p = \frac{n!}{(n-p)!}$ si $p \leq n$, 0 sinon

f$_{12}$ permutation = n-arrangement
rem: $A_n^n = n!$

f$_{13}$ Combinaison de p éléments de E + interprétat° tirage — interprét ens.!

p$_{14}$: C_n^p = nbre de comb. à p élément $\rightsquigarrow C_n^p = \binom{n}{p} = \frac{n!}{p!(n-p)!}$

p.9-11

M$_{15}$: nbre de suite strictemt ↗ de p éléments de $[\![1;n]\!]$, $= \binom{n}{p}$

op$_{16}$: propriétés de $\binom{n}{p}$ ... (avec formule de Pascal + Binôme + formule de Vandermonde)

$_{17}$: calcul de $card\{(x_1,\ldots,x_n) \in \mathbb{N}^n \mid x_1+\ldots+x_n = p\} \rightsquigarrow \binom{n+p-1}{p}$

[VIG] p 12

C) Cardinal et fonctions : $|E| = n$, $|F| = p$

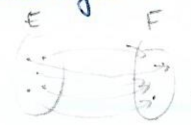
[VIG]

PROP$_{18}$: • nbre de fct de $F \to E$ = nbre de p-liste de E $= n^p$
• nbre d'inject° de $F \to E = A_n^p = \frac{n!}{(n-p)!}$

Rem$_{19}$: une permutation peut être vu comme une biject° de $E \to E$

Prop$_{19'}$: $n = p \Leftrightarrow \exists f : E \to F$ bijection.

Prop$_{20}$: Soit $f : E \to F$, f inj $\Rightarrow n \leq p$
surj $\Rightarrow n \geq p$
bij $\Rightarrow n = p$



Rem ⚠ réciproque fausse

Prop$_{21}$: Si $n = p$: [f injective ⟺ f surjective ⟺ f bijective]

Rem$_{22}$: Utile dans l'étude des morphismes de groupe fini + exemple

II) Dénombrement en algèbre

A) Groupes et actions de groupe : G groupe, X ensemble non vide

[ROM] p. 20-26

DÉF$_{23}$: Action de groupes

Rem$_{24}$: ⟺ avoir un morphisme de groupe de $G \to \mathfrak{S}_X$

Ex$_{25}$: ...

Déf$_{26}$: orbites de $x \in X$ noté $\mathcal{O}(x)$, forment une partition de X
exemple... + rem sur relat° d'équivalence $x \sim y \Leftrightarrow \mathcal{O}(x) = \mathcal{O}(y)$

Déf$_{27}$ Stabilisateurs de $x \in X \rightsquigarrow Stab(x)$

Rem$_{28}$: Stab(x) ss-grpe de G.

THM$_{29}$: $\varphi_x : \begin{cases} G/Stab(x) \longrightarrow \mathcal{O}(x) \\ g \longmapsto g \cdot x \end{cases}$ bien déf et bijective. Si G fini $\rightsquigarrow |\mathcal{O}(x)| = \frac{|G|}{|Stab(x)|}$

THM$_{30}$ $\boxed{\text{équation aux classes}}$

Applicat°$_{31}$: le centre d'un p-groupe est non trivial

Appli$_{32}$: tout groupe d'ordre p^2 est commutatif

THM$_{33}$: Formule de Burnside

[ROM] p 38 (exo 1.16)

B) Corps finis : Soit $n \in \mathbb{N}^*$, $q = p^r$ où p premier, $r \in \mathbb{N}^*$

On appelle $\mathbb{F}_q$ un corps à q éléments.

Prop$_{34}$: $Card(GL_n(\mathbb{F}_q)) = \prod_{m=0}^{n-1}(q^n - q^m)$; $Card(SL_n(\mathbb{F}_q)) = \prod_{m=0}^{n-2}(q^n - q^m) \times q^{n-1}$

[ROM] p.165

[PER] p 116 aller voir ici

II) B)

On note $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q \mid x = y^2\}$ [PER]

Prop 35 : $|\mathbb{F}_q^2| = \frac{q+1}{2}$, $|\mathbb{F}_q^{\times 2}| = \frac{q-1}{2}$ ← mettre plutôt card( ) — Aller voir dans [ROM]

Déf 36 : symbole de Legendre $\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{si } a \text{ carré dans } \mathbb{F}_p^\times \\ -1 & \text{si } a \text{ non carré dans } \mathbb{F}_p^\times \\ 0 & \text{si } a = 0 \end{cases}$ — [CAL] p 302 - 303

⚠ p premier impair

Prop 37 : $\forall a \in \mathbb{F}_p^\times$, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ ← dans $\mathbb{F}_p$ et dans $\mathbb{Z}$ car les 2 quantités sont dans $\{-1, 1\}$ — aller voir dans [ROM] ?

$a \in \mathbb{F}_p^\times \mapsto \left(\frac{a}{p}\right) \in \{-1, 1\}$ morphisme de groupe

Prop 38 : $p > 2$, 1er, $a \in \mathbb{F}_p^\times$, $\mathrm{Card}\left(\{x \in \mathbb{F}_p \mid ax^2 = 1\}\right) = 1 + \left(\frac{a}{p}\right)$ — [CAL] p 303

THM 39 : Loi de réciprocité quad. Dév 1 — [CAL] p 304

Ex ? (aller voir ROM ?)

Rem 40 : Preuve repose sur principe de double comptage très utilisé en dénombrement.

III) Fonctions remarquables - Fonctions arithmétiques.

A) Indicatrice d'Euler :

Déf 41 : fonction ind. Euler φ — [PER] p 15 - 16

Prop 42 : $\forall n \in \mathbb{N}^*$, $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

- $\forall p$ premier $\varphi(p) = p - 1$, $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$
- + autre prop. de φ

Thm 43 : Euler ⇝ $a \wedge n = 1$ $a^{\varphi(n)} \equiv 1 [n]$ — [PER] p 39 (exo)

Prop 44 : $\boxed{n = \sum_{d \mid n} \varphi(d)}$ — [PER] p 82

Appli 45 : Tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique — [PER] p 82

B) Fonction de Möbius : (normalement tout dans [ROM] + [FRA] (le vieux) qd $\ddot{m}$)

Déf 46 : fct de Möbius : μ — [ROM] p 389

Ex 47 : $\mu(5)$, $\mu(25)$, $\mu(6)$ ...

Lemme 46 : $\forall n \geq 1$, on note $\mathcal{D}_n = \{d \in \mathbb{N}^* \mid d \mid n\}$ — [ROM] p 390

$$\sum_{d \in \mathcal{D}_n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases}$$

Dév 2

THM 47 : Formule d'inversion de Möbius — [FRA] p 93 - 189

Appli 48 : Sur $\mathbb{F}_q$, $X^{q^n} - X = \prod_{d \in \mathcal{D}_n} \prod_{P \in A(n,q)} P$ (admis) où $A(n,q) = \{P \in \mathbb{F}_q[X] \mid P \text{ unit. irréductible de d}^\circ n\}$, $I(n,q) = \mathrm{Card}(A(n,q))$

$\boxed{I(n,q) = \frac{1}{n} \sum_{d \mid n} \mu(n/d) q^d}$ (éq ?)

C) Séries entières :

Rem 49 : L'unicité des coeff permet de dénombrer des ensembles en calculant de 2 façons ≠ la série ent. — pas de réf ...

Ex 50 : $(1+x)^n (1+x)^m = (1+x)^{n+m}$ ⇝ $\left(\sum_{k=0}^{n} \binom{n}{k} x^k\right)\left(\sum_{\ell=0}^{m} \binom{m}{\ell} x^\ell\right) = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k$

D'où $\binom{n+m}{k} = \sum_{\ell=0}^{k} \binom{n}{\ell}\binom{m}{k-\ell}$ "produit de Cauchy" ↳ $\sum_{k=0}^{n+m} \left(\sum_{\ell=0}^{k} \binom{n}{k}\binom{m}{k-\ell}\right) x^k$

Prop 51 Nombres de Bell — [FRAN] p 12 - 13

↳ B_n = nbre de partitions de $[\![1;n]\!]$, $B_0 = 1$ (convention), $\boxed{\forall n \in \mathbb{N}\ B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k}$

↳ la série entière $\sum \frac{B_n}{n!} z^n$ a un rayon de CV $R > 0$, en calculant sa somme, on en tire : $\boxed{B_k = \frac{1}{e} \sum_{n=0}^{+\infty} \frac{n^k}{k!}}$

Réf :

[VIG] Vigneron - Dénombrement et combinatoire (I)

[ROM] : Rombaldi - Mathématiques pour l'agrégation (II.A, II.B)

[PER] - Perrin - Cours d'Algèbre (II.B, III.A)

[CAL] - Caldero - Nouvelles histoires hédonistes. Algèbre tome 1 (II.B) dév 1

[FRA] - Francinou-Gianella - Exercices de mathématiques pour l'agrégation (III.B) dév2

[FRAA1] - Francinou... Oraux X-ENS Algèbre 1 (III.C) Nombres de Bell