Université de Genève
Section de Mathématiques

Algèbre I
Session de printemps 2009
Examen écrit, corrigé

Ex.1

Commençons par chercher une solution particulière n_0 sous la forme $n_1+101n_2+61\cdot 101n_3$ avec $n_1, n_2, n_3 \in \mathbb{Z}$.

On veut $n_0 \equiv n_1 \equiv 5 \pmod{101}$. On pose donc $n_1 = 5$.

On veut également $n_0 \equiv n_1 + 101n_2 \equiv 5 + 40n_2 \equiv 6 \pmod{61}$, ce qui est équivalent à $40n_2 \equiv 1 \pmod{61}$. Il faut donc inverser 40 modulo 61. Puisque ces nombres sont premiers entre eux, cela peut être fait en écrivant une relation de Bézout entre 40 et 61. On applique donc l'algorithme d'Euclide :

$$\begin{aligned} 61 &= 40 + 21 \\ 40 &= 21 + 19 \\ 21 &= 19 + 2 \\ 19 &= 9 \cdot 2 + 1, \end{aligned}$$

puis

$$\begin{aligned} 1 &= 19 - 9 \cdot 2 = 19 - 9(21 - 19) \\ &= -9 \cdot 21 + 10 \cdot 19 = -9 \cdot 21 + 10(40 - 21) \\ &= 10 \cdot 40 - 19 \cdot 21 = 10 \cdot 40 - 19(61 - 40) \\ &= -19 \cdot 61 + 29 \cdot 40. \end{aligned}$$

Cela donne donc $29 \cdot 40 \equiv 1 \pmod{61}$. On pose $n_2 = 29$.

On veut enfin $n_0 \equiv n_1 + 101n_2 + 61 \cdot 101n_3 \equiv 8 + n_3 \equiv 8 \pmod{11}$. On pose $n_3 = 0$.

Au final, $n_0 = 5 + 29 \cdot 101 = 2934$ est solution particulière.

De plus, les nombres 11, 61 et 101 sont tous les trois premiers donc deux à deux premiers entre eux ; d'après le théorème chinois, la différence entre deux solutions du système de congruence est un multiple de $11 \cdot 61 \cdot 101 > 2934$.

L'entier $n_0 = 2934$ correspond donc à la plus petite solution positive.

Ex.2

Par divisions euclidiennes successives, on a

$$\begin{aligned} 2265 &= 2 \cdot 1048 + 169 \\ 1048 &= 6 \cdot 169 + 34 \\ 169 &= 4 \cdot 34 + 33 \\ 34 &= 33 + 1. \end{aligned}$$

Ce qui donne $\operatorname{pgcd}(2265, 1048) = 1$. Et en remontant les calculs, on obtient :

$$\begin{aligned} 1 &= 34 - 33 = 34 - (169 - 4 \cdot 34) \\ &= -169 + 5 \cdot 34 = -169 + 5(1048 - 6 \cdot 169) \\ &= 5 \cdot 1048 - 31 \cdot 169 = 5 \cdot 1048 - 31(2265 - 2 \cdot 1048) \\ &= -31 \cdot 2265 + 67 \cdot 1048. \end{aligned}$$

Ex.3

(a),(b) Si deux anneaux sont isomorphes, alors ils possèdent le même nombre d'éléments inversibles. Or, puisque $200 = 2^3 5^2$,

$$\begin{aligned}
\#\Big(U\Big(\mathbb{Z}/200\mathbb{Z}\Big)\Big) &= \varphi(200) = 200(1-\frac{1}{2})(1-\frac{1}{5}) = 80;\\
\#\Big(U\Big(\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/50\mathbb{Z}\Big)\Big) &= \#\Big(U\Big(\mathbb{Z}/4\mathbb{Z}\Big)\Big)\cdot\#\Big(U\Big(\mathbb{Z}/50\mathbb{Z}\Big)\Big)\\
&= \varphi(4)\varphi(50)\\
&= 4(1-\frac{1}{2})\cdot 50(1-\frac{1}{2})(1-\frac{1}{5}) = 40;\\
\#\Big(U\Big(\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}\Big)\Big) &= \#\Big(U\Big(\mathbb{Z}/4\mathbb{Z}\Big)\Big)\cdot\#\Big(U\Big(\mathbb{Z}/5\mathbb{Z}\Big)\Big)\cdot\#\Big(U\Big(\mathbb{Z}/10\mathbb{Z}\Big)\Big)\\
&= \varphi(4)\varphi(5)\varphi(10)\\
&= 2\cdot 4\cdot 10(1-\frac{1}{2})(1-\frac{1}{5}) = 32.
\end{aligned}$$

Aucun de ces trois anneaux ne sont donc isomorphes entre eux.

(c) On a $200 = 8\cdot 25$ avec 8 et 25 premiers entre eux. Par le théorème chinois, on peut donc conclure que

$$\mathbb{Z}/200\mathbb{Z} \cong \mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/25\mathbb{Z}.$$

(d) Deux anneaux isomorphes possèdent le même nombre d'éléments. Or

$$\#\Big(\mathbb{Z}/200\mathbb{Z}\Big) = 200$$

mais

$$\#\Big(\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/11\mathbb{Z}\Big) = 3\cdot 5\cdot 11 = 165 \neq 200.$$

Ces deux anneaux ne sont donc pas isomorphes[1].

Ex.4

(a) Les entiers 7 et $10^{10} = 2^{10}5^{10}$ sont premiers entre eux ; d'après le théorème d'Euler, on a donc $7^{\varphi(10^{10})} \equiv 1 \pmod{10^{10}}$. Or $\varphi(10^{10}) = 10^{10}(1-\frac{1}{2})(1-\frac{1}{5}) = 4\cdot 10^9$. On a donc $7^{10^{11}} \equiv 7^{25\cdot 4\cdot 10^9} \equiv \left(7^{4\cdot 10^9}\right)^{25} \equiv 1^{25} \equiv 1 \pmod{10^{10}}$.

Or le reste de la division de $7^{10^{11}}$ par 10^{10} correspond au plus petit entier positif congru à $7^{10^{11}}$ modulo 10^{10}. D'après ce qui précède, cela donne 1.

(b) Cette fois, ce sont 53 et $72 = 2^3 3^2$ qui sont premiers entre eux et puisque

$$\varphi(72) = 72(1-\frac{1}{2})(1-\frac{1}{3}) = 24,$$

on a, toujours d'après le théorème d'Euler, $53^{24} \equiv 1 \pmod{72}$. Donc

$$53^{50} \equiv 53^{2\cdot 24+2} \equiv 53^2(50^{24})^2 \equiv (-19)^2 1^2 \equiv 361 \equiv 1 \pmod{72}.$$

[1] bien qu'ils possèdent pourtant le même nombre d'éléments inversibles

Sinon, on peut aussi directement constater que $53^2 \equiv 1 \pmod{72}$ et donc que, $53^{50} \equiv (53^2)^{25} \equiv 1 \pmod{72}$.

Ex.5

(a) Dans $\mathbb{Z}/6\mathbb{Z}$, on a $-3 = 3$. Les trois polynômes sont donc égaux à

$$(x+3)^2 = x^2 + 6x + 9 = x^2 + 3.$$

(b) Les anneaux $\mathbb{F}_{11}$ et $\mathbb{R}$ sont tous les deux des corps, les anneaux $\mathbb{F}_{11}[x]$ et $\mathbb{R}[x]$ sont donc tous les deux principaux, *i.e.* tous leurs idéaux sont engendrés par un unique polynôme unitaire.

Or les seuls diviseurs unitaires de $x+2$ sont 1 et $x+2$. Le générateur unitaire de $(x+2, x^2-2x+3)$ est donc l'un des deux. De plus, un polynôme est divisible par $x+2$ si et seulement si -2 est racine de ce polynôme.

Dans $\mathbb{F}_{11}$, -2 est racine de x^2-2x+3, on a donc $(x+2, x^2-2x+3) = (x+2)$.

Dans $\mathbb{R}$, ça n'est par contre pas le cas. On a donc $(x+2, x^2-2x+3) = (1) = \mathbb{R}[x]$.

Cette exercice peut également se résoudre en faisant des divisions euclidiennes de polynômes.

(c) Que ce soit par division euclidienne ou par factorisation évidente, on a

$$2x^3 - 11x^2 + 2x - 11 = (2x-11)(x^2+1).$$

Le plus grand diviseur commun unitaire de x^2+1 et $2x^3-11x^2+2x-11$ est donc x^2+1.

(d) Pour tout nombre premier p et tout polynôme unitaire $P \in \mathbb{F}_n[x]$ de degré $d \geq 1$, l'anneau $\mathbb{F}_p[x]/(P)$ contient p^d éléments. Dans notre cas, cela fait donc $3^2 = 9$ éléments.

De plus, avec les notations précédentes, $\mathbb{F}_p[x]/(P)$ est un corps si et seulement P est irréductible dans $\mathbb{F}_p[x]$. Dans notre cas, $P = x^2+1$, de degré 2, est irréductible si et seulement il ne possède pas de racine. Or, $P(0) = 1 \neq 0$ et $P(1) = P(2) = 2 \neq 0$. Ce qui précède s'applique donc et tous les éléments non nuls de $\mathbb{F}_3[x]/(x^2+1)$ sont donc inversibles. De fait, il y a $9-1 = 8$ éléments inversibles.

Soit $\mathbb{1}$ l'élément unité de $\mathbb{F}_3[x]/(x^2+1)$. Il est clair que $3 \cdot \mathbb{1}$ est égal à zéro. De plus, $\mathbb{1}$ n'est évidemment pas nul, et si $2 \cdot \mathbb{1}$ l'était, alors $\mathbb{1} = 3 \cdot \mathbb{1} - 2 \cdot \mathbb{1}$ le serait aussi. La caractéristique étant le plus petit entier strictement positif k tel que $k \cdot \mathbb{1} = 0$, on a donc $\mathrm{Car}\Big(\mathbb{F}_3[x]/(x^2+1)\Big) = 3$.

Ex.6

(a) $14\mathbb{Z} + 42\mathbb{Z} + 98\mathbb{Z} = \mathrm{pgcd}(14, 42, 98)\mathbb{Z} = \mathrm{pgcd}(14, 3 \cdot 14, 7 \cdot 14)\mathbb{Z} = 14\mathbb{Z}$.

(b) $4\mathbb{Z} \cdot 6\mathbb{Z} \cdot 8\mathbb{Z} = 4 \cdot 6 \cdot 8\mathbb{Z} = 192\mathbb{Z}$.

Ex.7

Vérifions que $I \cap J$ satisfait les axiomes des idéaux :

Non vide : Puisque I et J sont des idéaux, $0_A \in I$ et $0_A \in J$, donc $0_A \in I \cap J \neq \emptyset$.

Sous-groupe additif : Soit $x, y \in I \cap J$, alors x et y sont chacun dans I et dans J. Or ces derniers sont des idéaux, donc $x - y \in I$ et $x - y \in J$ et donc $x - y \in I \cap J$.

Stabilité par multiplication externe : Soit $x \in I \cap J$ et $a \in A$, alors x est dans I et dans J. Or ce sont des idéaux, donc ax et xa sont dans I et dans J. Au final, $ax, xa \in I \cap J$.

L'ensemble $I \cap J$ est donc bien un idéal de A.

L'ensemble $I \cup J$, par contre, n'a aucune raison d'être un idéal. Pour $A = \mathbb{Z}$, on pourra, par exemple, prendre $I = (2)$ et $J = (3)$. Alors, $2 \in I \cup J$, $3 \in I \cup J$ mais pourtant $3 - 2 = 1$ n'est ni dans I, ni dans J, donc pas dans $I \cup J$.

Ex.8

Les nombres de la forme $39x$, $-6y$, $54z$ et $102w$ avec $x, y, z, w \in \mathbb{Z}$ sont, respectivement et exactement, les éléments de (39), (6), (54) et (102). Les éléments de la forme $39x - 6y + 54z + 102w$ avec $x, y, z, w \in \mathbb{Z}$ sont donc exactement les éléments de $(39)+(6)+(54)+(102)$, qui est bien un idéal de $\mathbb{Z}$. On sait de plus que cet idéal est engendré par

$$\text{pgcd}(39, 6, 54, 102) = \text{pgcd}(3 \cdot 13, 3 \cdot 2, 3 \cdot 8, 3 \cdot 34) = 3.$$

Ex.9

Montrons que l'ensemble $B := \{a + b\sqrt{11} | a, b \in \mathbb{Z}\}$ satisfait les axiomes de sous-anneau :

Non vide : $0 = 0 + 0 \cdot \sqrt{11} \in B$.

Sous-groupe additif : Soit $a_1 + b_1\sqrt{11}, a_2 + b_2\sqrt{11} \in B$, alors

$$(a_1 + b_1\sqrt{11}) + (a_2 + b_2\sqrt{11}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{11} \in B.$$

Stabilité par multiplication interne : Soit $a_1 + b_1\sqrt{11}, a_2 + b_2\sqrt{11} \in B$, alors

$$(a_1 + b_1\sqrt{11})(a_2 + b_2\sqrt{11}) = (a_1a_2 + 11b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{11} \in B.$$

Unitaire : $1 = 1 + \cdot\sqrt{11} \in B$.

Au final, B est bien un sous-anneau de $\mathbb{C}$.

Ex.10

(a) $\forall n \in \mathbb{N}, 2^{2n+1} + 1 \equiv 2 \cdot (2^2)^n + 1 \equiv 2 \cdot 1^n + 1 \equiv 2 + 1 \equiv 0 \pmod 3$. L'entier $2^{2n+1} + 1$ est donc divisible par 3 pour tout $n \in \mathbb{N}$.

(b) Pour tout $n \in \mathbb{N}$, on pose $n = 3k + r$ le résultat de la division euclidienne de n par 3. L'entier $r \in \{0, 1, 2\}$ correspond donc à la valeur de n modulo 3. On a alors

$$n^3 \equiv (3k + r)^3 \equiv 27k^3 + 27k^2r + 9kr^2 + r^3 \equiv r^3 \pmod 9.$$

Notamment

si $r = 0$, alors $n^3 \equiv 0 \pmod 9$;
si $r = 1$, alors $n^3 \equiv 1 \pmod 9$;
si $r = 2$, alors $n^3 \equiv -1 \pmod 9$.