Number theory assignment 02

N'Dah Jean KOUAGOU

January 19, 2019

7. Let I and J be coprime ideals in a commutative ring R satisfying an equality of ideals $IJ = K^n$. Let's show that we have $I = (I+K)^n$ and $J = (J+K)^n$

• $(I+K)^n \subseteq I$

We have

$$(I+K)^n = \left\{ finite \sum (x_{i_1} + z_{i_1})(x_{i_2} + z_{i_2}) \dots (x_{i_n} + z_{i_n}) : (x_{i_j}, z_{i_j}) \in I \times K \right\}$$

Let $X = \sum (x_{i_1} + z_{i_1})(x_{i_2} + z_{i_2}) \dots (x_{i_n} + z_{i_n}) : (x_{i_j}, z_{i_j}) \in (I+K)^n$.
We have:

$$\begin{aligned} X &= \sum (x_{i_1} + z_{i_1})(x_{i_2} + z_{i_2}) \dots (x_{i_n} + z_{i_n}) : (x_{i_j}, z_{i_j}) \\ &= \sum (x_{i_1}x_{i_2} + x_{i_1}z_{i_2} + z_{i_1}x_{i_2} + z_{i_1}z_{i_2})(x_{i_3} + z_{i_3}) \dots (x_{i_n} + z_{i_n}) \\ &= \sum (\underbrace{x_{i_1}x_{i_2}}_{\in I^2 \subseteq I} + \underbrace{x_{i_1}z_{i_2}}_{\in I} + \underbrace{z_{i_1}x_{i_2}}_{\in I} + \underbrace{z_{i_1}z_{i_2}}_{\in K^2})(x_{i_3} + z_{i_3}) \dots (x_{i_n} + z_{i_n}) \\ &\vdots \\ &= \sum (\underbrace{x_{i_1}x_{i_2} \dots x_{i_n}}_{\in I^n \subseteq I} + \underbrace{x_{i_1}(\dots)}_{\in I} + \underbrace{x_{i_2}(\dots)}_{\in I} + \dots + \underbrace{x_{i_n}(\dots)}_{\in I} + \underbrace{z_{i_1}z_{i_2} \dots z_{i_n}}_{\in K^n = IJ \subseteq I}) \in I \end{aligned}$$

It follows that $X \in I$ and so $(I+K)^n \subseteq I$.

• $I \subseteq (I+K)^2$

Let $x \in I$. Since I and J are coprime ($I + J = R$), then there exist $x_0 \in I, y_0 \in J$ such that $x_0 + y_0 = 1$.
Then we have :

$$\begin{aligned} x &= x(x_0 + y_0) \\ &= xx_0 + \underbrace{xy_0}_{\in IJ = K^n} \\ &= (x(x_0 + y_0))x_0 + xy_0 \text{ substituting } x \text{ in the first term by } x(x_0 + y_0) \\ &= \underbrace{xx_0^2}_{\in I^3} + \underbrace{xy_0 + xx_0y_0}_{\in IJ = K^n} \\ &= (x(x_0 + y_0))x_0^2 + \underbrace{xy_0 + xx_0y_0}_{\in IJ = K^n} \text{ substituting } x \text{ in the first term by } x(x_0 + y_0) \\ &= \underbrace{xx_0^3}_{\in I^4} + \underbrace{xx_0^2y_0 + xy_0 + xx_0y_0}_{\in IJ = K^n} \\ &\vdots \\ &= \underbrace{xx_0^{n-1}}_{\in I^n} + \underbrace{xy_0(\dots)}_{\in IJ = K^n} \in I^n + K^n \end{aligned}$$

But we have $(I+K)^n = I^n + K^n + \sum_{i=1}^{n-1} \begin{pmatrix} n \\ i \end{pmatrix} I^i K^{n-i}$, where $\begin{pmatrix} n \\ i \end{pmatrix} = \frac{n!}{i!(n-i)!}$.
So $I^n + K^n \subseteq (I+K)^n$ and we conclude that $I \subseteq (I+K)^n$.
Therefore $\boxed{I = (I+K)^n}$ **and by symmetry we have** $\boxed{J = (J+K)^n}$.

8. We take $A = \mathbb{Z}[\sqrt{-6}]$.

(a) Let's determine the primes of A of norm ≤ 8

Let $x = a + b\sqrt{-6} \in A$. We have $N(x) = a^2 + 6b^2$
There is no element of A of norm $N \in \left\{2, 3, 5, 8\right\}$ because the equation $a^2 + 6b^2 = N$ does not have a solution in $\mathbb{Z} \times \mathbb{Z}$
for $N \in \left\{2, 3, 5, 8\right\}$.

- If $a^2 + 6b^2 = 1$, then $x = a + b\sqrt{-6} \in A^*$.
- If $a^2 + 6b^2 = 4$, then $a = \pm 2$ and $b = 0$.
  If $x = \alpha\beta$, with $\alpha, \beta \in A$ then

$$N(x) = N(\alpha\beta) = N(\alpha)N(\beta) = 4$$
$$\Rightarrow \begin{cases} N(\alpha) = 1 \\ N(\beta) = 4 \end{cases} or \begin{cases} N(\alpha) = 4 \\ N(\beta) = 1 \end{cases} or \begin{cases} N(\alpha) = 2 \\ N(\beta) = 2 \text{ impossible} \end{cases}$$

  . Then α is a unit or β is a unit. So 2 and -2 are primes of norm 4.
- If $a^2 + 6b^2 = 6 \times 1 = 2 \times 3$, then $a = 0$ and $b = \pm 1$ and since there is no element of norm 2 or 3 then $x = 6$ and $x = -6$ are primes of norm 6.
- If $a^2 + 6b^2 = 7 = 7 \times 1$, then $a = \pm 1$ and $b = \pm 1$. Using the same reasoning it comes that $x = -1 - \sqrt{-6}$, $x = -1 + \sqrt{-6}$, $x = 1 - \sqrt{-6}$ and $x = 1 + \sqrt{-6}$ are primes of norm 7.

Then all primes of A of norm ≤ 8 are $x = 2$, $x = -2$, $x = -6$, $x = 6$, $x = -1 - \sqrt{-6}$, $x = -1 + \sqrt{-6}$, $x = 1 - \sqrt{-6}$ and $x = 1 + \sqrt{-6}$.

(b)

Let's show that 15 has two distinct factorizations into irreducible elements in A.
We have:

$$15 = 3.5 = (3 + \sqrt{-6})(3 - \sqrt{-6})$$

- We have $N(3) = 9 \times 1 = 3^2$ and there is no element of norm 3. So if $3 = \alpha\beta$ then and α is a unit or β is a unit.Thus 3 is irreducible.
- Also $N(5) = 25 = 5^2$ and by the same reasoning, 5 is irreducible.
- We have $N(3 + \sqrt{-6}) = N(3 - \sqrt{-6}) = 15 = 3.5$ Then $3 + \sqrt{-6}$ and $3 - \sqrt{-6}$ are irreducible because there is no element of norm 3 or 5.

We conclude that 15 **has two distinct factorizations into irreducible elements in** A.

(c) Let's write $15A$ a sa product of prime ideals of A

We have $15A = (3A)(5A)$.
- In $\mathbb{Z}/3\mathbb{Z}$, $-6 = 0$, a square. So $3A = (3, \sqrt{-6})^2$.
- In $\mathbb{Z}/5\mathbb{Z}$, $-6 = 4$, a square. So $5A = (5, \sqrt{-6} - 2)(5, \sqrt{-6} + 2)$

Therefore $\boxed{15A = (3, \sqrt{-6})^2(5, \sqrt{-6} - 2)(5, \sqrt{-6} + 2).}$

9.

- $\alpha = 5 + i$

$$\begin{aligned} \alpha\bar{\alpha} &= 5^2 + 1^2 \\ &= 26 \\ \alpha\bar{\alpha} &= 2 \times 13. \end{aligned}$$

$$\begin{aligned} 2 &= 1^2 + 1^2 = (1+i)(1-i) \\ 13 &= 3^2 + 2^2 = (3+2i)(3-2i) \end{aligned}$$

$$\alpha\bar{\alpha} = (1+i)(1-i)(3+2i)(3-2i).$$

Let's find α.

* $(3+2i)$

$$\begin{aligned} \frac{(5+i)(3-2i)}{(3+2i)(3-2i)} &= \frac{15 - 10i + 3i + 2}{13} \\ &= \frac{17-7i}{13} \notin \mathbb{Z}[i]. \end{aligned}$$

$(3+2i)$ doesn't divide α. So $(3-2i)$ divides it.

$(1+i)$ and $(1-i)$ divide α.

$(3-2i)(1+i) = 3 - 2i + 3i + 2 = 5 + i$

Thus

$$\boxed{\alpha = 5 + i = (1+i)(3-2i)}$$

- $\beta = 239 + i$

$$\begin{aligned} \beta\bar{\beta} &= 239^2 + 1^2 \\ &= 57122 \\ \beta\bar{\beta} &= 2 \times 13^4. \end{aligned}$$

$$\begin{aligned} 13 &= 3^2 + 2^2 = (3+2i)(3-2i) \\ &= (1+i)(1-i)(3+2i)^4(3-2i)^4. \\ 2 &= 1^2 + 1^2 = (1-i)(1+i) \end{aligned}$$

Let's find β.

- $(3+2i)$

$$\begin{aligned} \frac{(239+i)(3-2i)}{(3+2i)(3-2i)} &= \frac{717 - 478i + 3i + 2}{13} \\ &= \frac{719-476i}{13}. \end{aligned}$$

$(3+2i)$ doesn't divide β but $(3-2i)$ divides it.
$(1+i)$ and $(1-i)$ divide β.
We have:

$$\begin{aligned}(3-2i)^4(1+i) &= (1+i)(3-2i)^2(3-2i)^2 \\ &= (1+i)(5-12i)(5-12i) \\ &= (1+i)(-119-120i) \\ \beta &= (3-2i)^4(1+i) = 1-239i\end{aligned}$$

So

$$\boxed{\beta = 239 + i = i(1+i)(3-2i)^4}$$

Let's find a relation between $(5+i)$ and $(239+i)$.

$$\begin{aligned}(5+i)^4 &= (1+i)^4(3-2i)^4 \\ &= (1+i)^3(1+i)(3-2i)^4 \\ &= (1+i)(1+i)^2(1+i)(3-2i)^4 \\ &= i(1-i)(1+i)^2(1+i)(3-2i)^4 \\ &= (1-i)(1+i)^2 i(1+i)(3-2i)^4 \\ &= (1-i)(1+i)^2(239+i) \\ &= (1-i)(1+i)(1+i)(239+i) \\ (5+i)^4 &= 2(1+i)(239+i)\end{aligned}$$

For every complex number $z = a+bi = re^{i\theta}$, with $\theta \notin \frac{\pi}{2} + \pi\mathbb{Z}$, we have: $\cos(\theta) = \frac{a}{r}$ and $\sin(\theta) = \frac{b}{r}$.
So $tan(\theta) = \frac{\sin(\theta)}{\cos(\theta)} = \frac{b}{a}$ and $\theta = arctan(\frac{b}{a})$.
Then we have:

$$\begin{aligned}Arg[(5+i)^4] = Arg[2(1+i)(239+i)] &\Leftrightarrow 4Arg(5+i) = Arg[2(1+i)] + Arg(239+i) \\ &\Leftrightarrow 4Arg(5+i) - Arg(239+i) = Arg(2+2i) \\ &\Leftrightarrow 4arctan\left(\frac{1}{5}\right) - \arctan\left(\frac{1}{239}\right) = \arctan\left(\frac{2}{2}\right) \\ &\Leftrightarrow 4\arctan\left(\frac{1}{5}\right) - \arctan\left(\frac{1}{239}\right) = \arctan(1) \\ &\Leftrightarrow 4\arctan\left(\frac{1}{5}\right) - \arctan\left(\frac{1}{239}\right) = \frac{\pi}{4} \\ &\Leftrightarrow 16\arctan\left(\frac{1}{5}\right) - 4\arctan\left(\frac{1}{239}\right) = \pi.\end{aligned}$$

11. Let A be a commutative ring and, $I, J \subset A$ two ideals.

(a) Let's show that $(I \cap J)(I+J) \subseteq IJ$

We have:

$$(I \cap J)(I+J) = \left\{ finite \sum x_i y_i : x_i \in I \cap J, y_i \in I+J \right\}$$

.
Let $X = \sum x_i y_i \in (I \cap J)(I+J)$.
We have for all $z \in I \cap J$ and $a+b \in I+J$, $z(a+b) = \underbrace{za}_{\in IJ} + \underbrace{xb}_{\in IJ} \in IJ$.
Since $(I \cap J)(I+J)$ is an ideal then a finite summation of all elements in the form $z(a+b) : z \in I \cap J, a+b \in I+J$

is an element of IJ. It follows that $X = \sum x_i y_i \in (I \cap J)(I+J)$.
Therefore $(I \cap J)(I+J) \subseteq IJ$.
- Case $A = \mathbb{Z}$.

There exist $n, m \in Z$ such that $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$.Then $IJ = mn\mathbb{Z}, I \cap J = lcm(m.n)\mathbb{Z}$ and $I + J = gcd(m,n)\mathbb{Z}$.
Let $l = pcm(m,n)$ and $d = gcd(m,n)$. We have $I \cap J = l\mathbb{Z}$, $I + J = d\mathbb{Z}$ and so $(I \cap J)(I+J) = ld\mathbb{Z}$.
Since $lcm(n,m) \times gcd(n,m) = n \times m$ for all integers n, m, then $ld = mn$.
We conclude that $(I \cap J)(I+J) = IJ$ in the case $A = \mathbb{Z}$.

(b)

Let $m \geq 1$, As $I + J = A$. Then there exists $x \in I$ and $y \in J$ such that $x + y = 1$.
Then

$$\begin{aligned} 1 &= (x+y)^{2m} \\ &= \sum_{k=0}^{2m} \binom{2m}{k} x^{2m-k} y^k \end{aligned}$$

$$= \binom{2m}{0} x^{2m} + \binom{2m}{1} x^{2m-1} y + \binom{2m}{2} x^{2m-2} y^2 + \cdots + \binom{2m}{2m-1} x y^{2m-1} + \binom{2m}{2m} y^{2m}$$

$$= \underbrace{\binom{2m}{0} x^{2m}}_{\in I^{2m} \subset I^m} + \underbrace{\binom{2m}{1} x^{2m-1} y}_{\in I^{2m-1} \subset I^m} + \underbrace{\binom{2m}{2} x^{2m-2} y^2}_{\in I^{2m-2} \subset I^m} + \cdots + \underbrace{\binom{2m}{m} x^m y^m}_{\in I^m} + \underbrace{\binom{2m}{m+1} x^{m-1} y^{m+1}}_{\in J^{m+1} \subset J^m} + \cdots + \underbrace{\binom{2m}{2m} y^{2m}}_{\in J^{2m} \subset J^m}$$

Then $1 \in I^m + J^m$.

. **We conclude that** $I^m + J^m = A$ **for all integer** $m \geq 1$**.**