Hilbert's Tenth Problem Seminar
Diophantine Sets over Some Rings of Algebraic Integers

Eduardo Gomezcaña

Exercise 1. Let K and L be number fields with $K \subset L$. Prove that

a) If R_1 and R_2 are Diophantine relations over O_L then $R_1 \wedge R_2$ and $R_1 \vee R_2$ are too.

Solution. We need to recall an exercise given by Jetze[1] on week 12 of the seminar. Bringing the result to our terms, it will imply that both, disjunction and conjunction of two Diophantine sets over $\mathcal{O}_L$ are Diophantine over $\mathcal{O}_L$, provided $\mathcal{O}_L$ is an integral domain and its fraction field not algebraically closed.

The ring $\mathcal{O}_L$ is indeed an integral domain as it is contained on a field. Additionally, we need to notice that L is the fraction field of $\mathcal{O}_L$ and because there is a polynomial over $\mathbb{Z}$ which have no roots on L, we must conclude L is not algebraically closed. As the comment made in the first paragraph, the desired result follows from here. □

b) The relation $x \neq 0$ is Diophantine over $\mathcal{O}_L$.

Solution. For this part we claim that

$$x \neq 0 \Leftrightarrow \exists y, v \in \mathcal{O}_L . xy = (2v-1)(3v-1).$$

If we assume the RHS, then, because $(2v-1)(3v-1)$ is never 0 and the fact that $\mathcal{O}_L$ is an integral domain, $x \neq 0$.

Assume now $x \neq 0$. Suppose for a moment that there are elements v and z of $\mathcal{O}_L$ such that $2v+xz=1$, then immediately we would have that $x|(2v-1)$ and thus $x|(2v-1)(3v-1)$; therefore there would be y in $\mathcal{O}_L$ with $xy = (2v-1)(3v-1)$; we suppose now there are no such numbers, then there must be an element t dividing both 2 and x and t not being a unit; we write in such a case $2 = pt$ and $x = qt$. We consider now the ideal I generated by px and 3 which will need to be generated by 1, otherwise we would obtain with that 2 and 3 have a common factor different than some unit. Thus there are elements v and z such that $3v + xz = 1$ to have that $x|(3v-1)$ and in consequence $x|(2v-1)(3v-1)$ which in turn means that there is y in $\mathcal{O}_L$ such that $xy = (2v-1)(3v-1)$.

□

[1] Proposition 1 in *Recursively enumerable sets of polynomials over a finite field* from Jeroen Demeyer.

c) If $\mathbb{Z}$ is Diophantine over $\mathcal{O}_K$ and if $\mathcal{O}_K$ is Diophantine over $\mathcal{O}_L$, then $\mathbb{Z}$ is Diophantine over $\mathcal{O}_L$.

Proof. By assumption, there is a polynomial Z over O_K such that

$$x \in \mathbb{Z} \Leftrightarrow \exists y_1, \ldots, y_m \in \mathcal{O}_K . Z(x, y_1, \ldots, y_m) = 0.$$

Because the coefficients of Z are in $\mathcal{O}_K \subset O_L$ and because $\mathcal{O}_K$ is Diophantine over O_L we have that the RHS is also Diophantine over O_L. But this just means that $\mathbb{Z}$ is Diophantine over $\mathcal{O}_L$ as desired. □

d) If $\mathbb{Z}$ is Diophantine over $\mathcal{O}_L$, then $\mathbb{Z}$ is Diophantine over $\mathcal{O}_K$.

Solution. We recall now that O_K and $\mathcal{O}_L$ are free of finite rank $\mathbb{Z}$-modules, we denote by $[\mathcal{O}_K : \mathbb{Z}]$ and $[\mathcal{O}_L : \mathbb{Z}]$ their rank, respectively. It is not hard to see that $[K : \mathbb{Q}] = [\mathcal{O}_K : \mathbb{Z}]$ and $[L : \mathbb{Q}] = [\mathcal{O}_L : \mathbb{Z}]$, and because $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module, we have

$$\begin{aligned} [L : K] &= [L : \mathbb{Q}]/[K : \mathbb{Q}] \\ &= [O_L : \mathbb{Z}]/[\mathcal{O}_K : \mathbb{Z}] \\ &= [\mathcal{O}_L : \mathcal{O}_K]. \end{aligned}$$

Meaning that $\mathcal{O}_L$ is finitely presented as a module over $\mathcal{O}_K$. Lets take $n = [\mathcal{O}_L : \mathcal{O}_K]$ and allow $B = \{b_1, \ldots, b_n\}$ be an $\mathcal{O}_K$-linear independent subset of $\mathcal{O}_L$ such that any element in $\mathcal{O}_L$ can written as a $\mathcal{O}_K$-linear combination of B. If x in an element of $\mathcal{O}_L$ we write $[x]_B = (x_1, \ldots, x_n) \in \mathcal{O}_K^n$ if $x = \sum_{k=1}^n x_k b_k$.
Finally, if $\mathbb{Z}$ is Diophantine over $\mathcal{O}_L$ there is a polynomial P over $\mathcal{O}_L$ such that

$$x \in \mathbb{Z} \Leftrightarrow \exists y_1, \ldots, y_m . P(x, y_1, \ldots, y_m) = 0.$$

By writing $(x_1, \ldots, x_m) = [x]_B$ and $(y_{i1}, \ldots, y_{im}) = [y_i]_B$, there are polynomials $P_1, \ldots, P_m$ over $\mathcal{O}_K$ such that

$$P(x, y_1, ..., y_n) = \sum_{k=1}^{m} P_1(x_1, \ldots, x_m, y_{11}, \ldots, y_{nm}) b_i.$$

Because the $\mathcal{O}_K$-linear independence of B, P will have a root if and only if a simultaneous root of the polynomials $P_1, \ldots, P_m$ exist. According to a) this will imply that $\mathbb{Z}$ is Diophantine over O_K because the system induced by the polynomials $P_1, \ldots, P_m$ is crafted through conjunction. □

Exercise 2. Let L be a number field and assume $\mathbb{Z}$ is Diophantine over $\mathcal{O}_L$. Prove that a relation is Diophantine over $\mathcal{O}_L$ if and only if is recursively enumerable.

Solution. We need to recall again that for any number field L, its ring of integers $\mathcal{O}_L$ is a free of finite rank $\mathbb{Z}$-module. We fix $B = \{b_1, \ldots, b_m\}$ as a $\mathbb{Z}$-linear independent subset of $\mathcal{O}_L$ such that any element of $\mathcal{O}_L$ can be written as a $\mathbb{Z}$-linear combination of B. Thanks to this, we use the injection

$$\begin{aligned} [\cdot]_B : \mathcal{O}_L &\to \mathbb{Z}^m \\ x &\mapsto (x_1, \dots, x_m), \end{aligned}$$

where $x = \sum_{i=1}^m x_i b_i$, to consider $\mathcal{O}_K$ as a subset of $\mathbb{Z}^m$.

With this we prove our result. Take $S \subset \mathcal{O}_K$ and assume first that S is Diophantine over $\mathcal{O}_L$, then there is a polynomial P with coefficients in $\mathcal{O}_L$ such that

$$x \in S \Leftrightarrow \exists y_1, \dots, y_n . P(x, y_1, ..., y_n) = 0.$$

By writing $(x_1, \dots, x_m) = [x]_B$ and $(y_{i1}, \dots, y_{im}) = [y_i]_B$, there are polynomials $P_1, \dots, P_m$ over $\mathbb{Z}$ such that

$$P(x, y_1, ..., y_n) = \sum_{k=1}^m P_1(x_1, \dots, x_m, y_{11}, \dots, y_{nm}) b_i.$$

Because of $\mathbb{Z}$-linear independence, P will have a root if and only if the system induced from the simultaneous roots of the polynomials $P_1, \dots, P_m$ has a solution. We know that in that case $[S]_B$ is Diophantine over $\mathbb{Z}$, and in consequence recursively enumerable by the DPRM-Theorem for $\mathbb{Z}$. We can conclude now S is recursively enumerable.

Assume now S is recursively enumerable. Then, by the DPRM-Theorem for $\mathbb{Z}$, $[S]_B$ is Diophantine over $\mathbb{Z}$, this means there is a polynomial Q over $\mathbb{Z}$ such that

$$(x_1, \dots, x_m) \in [S]_B \Leftrightarrow \exists y_1, \dots, y_n \in \mathbb{Z}. Q(x_1, \dots, x_m, y_1, ..., y_m) = 0.$$

and we have

$$x \in S \Leftrightarrow \exists x_1, \dots x_m, y_1, \dots, y_n \in \mathbb{Z}. \begin{pmatrix} Q(x_1, \dots, x_m, y_1, \dots, y_m) = 0 \\ x = x_1 b_1 + \dots + x_m b_m \end{pmatrix}.$$

By exercise 1 part a) and through the assumption of $\mathbb{Z}$ beign Diophantine over O_L, the RHS is Diophantine over $\mathcal{O}_L$. Thus S is Diophantine over $\mathcal{O}_L$.

$\square$