A PROBLEM IN ALGEBRAIC NUMBER THEORY

UROP+ FINAL PAPER, SUMMER 2017
CHRISTIAN ALTAMIRANO
MENTOR: ATTICUS CHRISTENSEN
PROJECT SUGGESTED BY: BJORN POONEN

ABSTRACT. In this paper, I investigate when an algebraic number can be expressed in terms of algebraic numbers of smaller degree. First, I describe an algorithm to decide, given an irreducible polynomial P in $\mathbb{Q}[x]$, whether one of its roots α can be expressed as $\beta + \gamma$, where β and γ are roots of polynomials in $\mathbb{Q}[x]$ of degree strictly less than the degree of α. Then, I turn to generalizations such as when α can be expressed as $\beta\gamma$, when α can be expressed as $P_1(\beta) + P_2(\gamma)$ where P_1 and P_2 are two given polynomials in $\mathbb{Q}[x]$ and similar with more variables.

CONTENTS

Date: August 31, 2017.

1. Introduction

The following notation will be used throughout this paper.
For an algebraic number z, let the degree of z, $\deg(z)$, be the degree of the minimal polynomial of z. This is the same as the degree of the extension $\mathbb{Q}(z)$ over $\mathbb{Q}$.
For a number field K, $I(K)$ will denote the set of all the fractional ideals in K.

In the second section I will describe when can α be written as a sum of β_i.
In the third section I will describe when can α can be written as $\beta\gamma$.
For these two sections I will first show that all the variables can be taken to be contained in the Galois closure of $\mathbb{Q}(\alpha)$.
In the fourth section I will show that that the same method will not work for the sum of polynomials case.

Acknowledgement

I would like to thank my mentor Atticus Christensen for teaching and for helping me with suggestions about the project. I would also like to thank Professor Bjorn Poonen for suggesting this project. Finally, I am thankful to the organizers of the UROP+ program for this amazing opportunity.

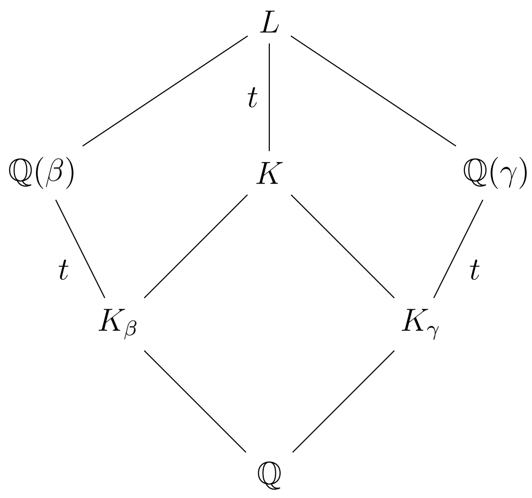
2. Sums of algebraic numbers

Given an algebraic number α, we describe an algorithm to decide whether or not α can be expressed as $\beta+\gamma$ where β and γ are algebraic numbers such that $\deg(\beta) < \deg(\alpha)$ and $\deg(\gamma) < \deg(\alpha)$.
To approach this problem, we will first show that if an algebraic number α has such property, then there exists a fixed field F (that only depends on α) such that there exist β and γ that satisfy $\alpha = \beta + \gamma$, $\deg(\beta) < \deg(\alpha)$ and $\deg(\gamma) < \deg(\alpha)$. Then, we will use linear algebra to describe α.

Theorem 2.1. *Let α, β, γ be algebraic numbers such that $\alpha = \beta+\gamma$, $\deg(\beta) < \deg(\alpha)$ and $\deg(\gamma) < \deg(\alpha)$. Let K be the Galois closure of $\mathbb{Q}(\alpha)$. Then, there exist β' and γ' such that $\alpha = \beta' + \gamma'$, $\deg(\beta') < \deg(\alpha)$, $\deg(\gamma') < \deg(\alpha)$ and β', $\gamma' \in K$.*

Lemma 2.2. *Let K be a Galois extension of $\mathbb{Q}$ and β be any algebraic number, then the minimal polynomial of β over K is the same as its minimal polynomial over $K \cap \mathbb{Q}(\beta)$*

Proof. Let $P \in K \cap \mathbb{Q}(\beta)[x]$ and $P' \in K[x]$ be the minimal polynomials of β over $K \cap \mathbb{Q}(\beta)$ and K respectively. Since $P(\beta) = 0$ and $P \in K \cap \mathbb{Q}(\beta)[x]$, which implies that $P \in K[x]$, then P is divisible by P' where both are monic and have the same degree because $[K(\beta) : K] = [\mathbb{Q}(\beta) : K \cap \mathbb{Q}(\beta)]$. Thus, $P = P'$. $\square$



Proof. Let $K_\beta = K \cap \mathbb{Q}(\beta)$ and $K_\gamma = K \cap \mathbb{Q}(\gamma)$, now we will show that there exist $\beta' \in K_\beta$ and $\gamma' \in K_\gamma$ that satisfy the property in the theorem.

Now, K and $\mathbb{Q}_\beta$ are extensions of $\mathbb{Q}$. Let $L = K\mathbb{Q}(\beta) = K(\beta)$, $K(\beta) = K(\gamma)$ because $\alpha \in K$ and $\beta + \gamma = \alpha$. Applying Lemma 2.2 to K and β

$$[L : K] = [K\mathbb{Q}(\beta) : K] = [\mathbb{Q}(\beta) : K \cap \mathbb{Q}(\beta)] = [K_\beta(\beta) : K_\beta]$$

Let $t = [L : K]$, $\beta' = Tr_K^L(\beta)/t$ and $\gamma' = Tr_K^L(\gamma)/t$ where Tr_K^L is the trace with respect to the extension L/K. Let $P(x) = x^t + a_{t-1}x^{t-1} + ... + a_0$ be the minimal polynomial of β in $K[x]$, then $Tr_K^L(\beta) = -a_{t-1}$ and $\beta' = Tr_K^L(\beta)/t = -a_{t-1}/t$. From Lemma 2.2, P is the minimal polynomial of β in K_β. Therefore, $P \in K_\beta[x]$, then $a_{t-1} \in K_\beta$ and $\beta' \in K_\beta$. Analogously, $\gamma' \in K_\gamma$. Also, since $\alpha \in K$ and $\beta + \gamma = \alpha$, $Tr_K^L(\beta) + Tr_K^L(\gamma) = Tr_K^L(\alpha)$, then $t\beta' + t\gamma' = t\alpha$, thus $\beta' + \gamma' = \alpha$.
Now, $\beta' \in K_\beta \subseteq \mathbb{Q}(\beta)$, therefore, $\deg(\beta') \leq \deg(\beta) < \deg(\alpha)$ and $\deg(\beta') < \deg(\alpha)$.
Analogously, $\deg(\gamma') < \deg(\alpha)$.
Hence, we have such β' and γ' that satisfy the theorem statement.

□

Now, the next step for this algorithm will be included in the following general case.

We now prove an analogous result for sums of n items.
Given an algebraic number α, we describe an algorithm to decide whether or not α can be expressed as $\beta_1 + \beta_2 + ... + \beta_n$ where the β_i are algebraic numbers such that $\deg(\beta_i) < \deg(\alpha)$ for all i.

Theorem 2.3. *Let α, β_1, β_2, ..., β_n be algebraic numbers such that $\alpha = \beta_1 + ... + \beta_n$ and $\deg(\beta_i) < \deg(\alpha)$ for all i. Then, there exist β'_1, β'_2, ..., β'_n such that $\alpha = \beta'_1 + ... + \beta'_n$, $\deg(\beta'_i) < \deg(\alpha)$ and β'_1, β'_2, ..., $\beta'_n \in K$ for all i from 1 to n where K is the Galois closure of $\mathbb{Q}(\alpha)$*

Proof. Let α, β_1, β_2, ..., β_n and K be as in the theorem. Let L be the extension of K containing β_1, β_2, ..., β_n. Let $t = [L : K]$ and for each β_i let $K_i = K \cap \mathbb{Q}(\beta_i)$.
Let $\beta'_i = Tr_K^L(\beta_i)/t$. From Lemma 2.2 the minimal polynomial of β_i over K is the same as its minimal polynomial over $K_i = K \cap \mathbb{Q}(\beta_i)$, as a result, $Tr_K^{K(\beta_i)}(\beta_i) = Tr_{K_i}^{\mathbb{Q}(\beta_i)}(\beta_i)$.

Now,

$$\beta_i' = Tr_K^L(\beta_i)/t = [L : K(\beta_i)]Tr_K^{K(\beta_i)}(\beta_i)/t = [L : K(\beta_i)]Tr_{K_i}^{\mathbb{Q}(\beta_i)}(\beta_i)/t$$

Clearly $Tr_{K_i}^{\mathbb{Q}(\beta_i)}(\beta_i) \in K_i$, then $\beta_i' \in K_i \subset K$. Now,

$$\alpha = \sum_{i=1}^{n} \beta_i$$

Taking the trace of L over K

$$Tr_K^L(\alpha) = Tr_K^L(\sum_{i=0}^{n} \beta_i) = \sum_{i=1}^{n} Tr_K^L(\beta_i)$$

Using that $\alpha \in K$ and replacing $Tr_K^L(\beta_i)$ by $t\beta_i'$, we get

$$t\alpha = \sum_{i=1}^{n} (t\beta_i')$$

Hence,

$$\alpha = \sum_{i=1}^{n} (\beta_i')$$

And we have that all $\beta_i' \in K$.

□

Now we will describe the algorithm to determine whether or not α can be written as $\sum_{i=1}^{n} \beta_i$ for some algebraic numbers β_i such that $\deg(\beta_i) < \deg(\alpha)$. Let K be the Galois closure of $\mathbb{Q}(\alpha)$. From Theorem 2.3, we know that if $\alpha = \sum_{i=1}^{n} \beta_i$, therefore, we can take $\beta_i \in K$.

Then, α can be the sum of β_i if and only if there exist n subfields K_i of K, that have dimension less than $\deg(\alpha)$ such that $\alpha \in \sum_i K_i$. Thus we must determine if α is in a finite list of computable sub $\mathbb{Q}$ vector spaces of K.

Let $m = [K : Q]$ and e_1, e_2, ..., e_m a basis for K and let $\alpha = \alpha_1 e_1 + ... + \alpha_m e_m$. Now, for every set of n subfields of K that have dimension less than $\deg(\alpha)$, let them be K_i, we will check if there exist $\beta_i \in K_i$ for all i such that satisfy $\alpha = \sum_{i=1}^{n} \beta_i$. Let one such set of n subfields of K that have dimension less than $\deg(\alpha)$ be K_1, K_2, ..., K_n and $b_{i1}, b_{i2}, ..., b_{il_i}$ be a basis for each K_i. Now, any number $\beta_i \in K_i$ can be written as $a_{i1}b_{i1} + a_{i2}b_{i2} + ... + a_{il_i}b_{il_i}$ and since β_{i_j} are all in K, each of them is a linear combination of $a_{i_1}, ..., a_{i_{l_i}}$.

Now, for $\alpha = \sum_{i=1}^{n} \beta_i$ to be true, the following equality should be true for each j from 1 to m:

$$\sum_{i=1}^{n} c_{ij} = \alpha_j$$

Therefore, α can be written as $\sum_{i=1}^{n} \beta_i$ if and only if the system of equations has a solution.

3. Products of algebraic numbers

Given an algebraic number α, we describe an algorithm to decide whether or not α can be expressed as $\beta\gamma$ where β and γ are algebraic numbers such that $\deg(\beta) < \deg(\alpha)$ and $\deg(\gamma) < \deg(\alpha)$.

Let K be the Galois closure of $\mathbb{Q}(\alpha)$. To approach this problem, we will also show that if α has such property, then there exist β and γ that satisfy $\alpha = \beta\gamma$, $\deg(\beta) < \deg(\alpha)$, $\deg(\gamma) < \deg(\alpha)$ and $\beta, \gamma \in K$. Then, we will use the factorizations of ideals into prime ideals and some facts about units.

Theorem 3.1. *Let α, β, γ be algebraic numbers such that $\alpha = \beta\gamma$, $\deg(\beta) < \deg(\alpha)$ and $\deg(\gamma) < \deg(\alpha)$. Then, there exist β' and γ' such that $\alpha = \beta'\gamma'$, $\deg(\beta') < \deg(\alpha)$, $\deg(\gamma') < \deg(\alpha)$ and β', $\gamma' \in K$ where K is the Galois closure of $\mathbb{Q}(\alpha)$*

Proof. Let α, β, γ and K be as in the theorem. Let $K_\beta = K \cap \mathbb{Q}(\beta)$ and $K_\gamma = K \cap \mathbb{Q}(\gamma)$.
Now we will assume that α is different than 0, because if it were the result would be trivial. Let $L = K\mathbb{Q}(\beta) = K(\beta) = K(\gamma)$. Let $P(x) = x^t + a_{t-1}x^{t-1} + ... + a_0$ be the minimal polynomial of β over K, from Lemma 2.2 P is also the minimal polynomial of β over K_β.
Let Q be the polynomial

$$Q(x) = \frac{x^t}{a_0}P(\alpha/x) = x^t + \alpha\frac{a_1}{a_0}x^{t-1} + ... + \alpha^{t-1}\frac{a_{t-1}}{a_0}x + \frac{\alpha^t}{a_0}.$$

Clearly, Q is in $K[x]$, because all of its coefficients are in K. It can also be seen that Q is monic.
Then, $Q(\gamma) = \gamma^t P(\beta)/a_0 = 0$. Then Q divides the minimal polynomial of γ in K. Since $K(\beta) = K(\gamma)$, the minimal polynomials of β and γ over K should have the same degree, thus Q has degree t. Hence, Q has to be the minimal polynomial of γ over K. From the proposition Q is also the minimal polynomial of γ over $K_\gamma = K \cap \mathbb{Q}(\gamma)$.
Let $\beta' = a_0/a_1$ and $\gamma' = \alpha a_1/a_0$, clearly $\beta'\gamma' = \alpha$. Now, as a_0 and a_1 are coefficients of $P \in K_\beta[x]$, then $a_0 \in K_\beta$ and $a_1 \in K_\beta$, hence $\beta' = a_0/a_1 \in K_\beta$. Also, $\gamma' = \alpha a_1/a_0$ is a coefficient of $Q \in K_\gamma[x]$, then $\gamma' \in K_\gamma$. Now we have the β' and γ' required. ☐

Theorem 3.2. *Let K_1 and K_2 be two number fields inside another number field L so that L is Galois over $\mathbb{Q}$ and let $K = K_1 \cap K_2$. Let I_1 and I_2 be two fractional ideals of K_1 and K_2 such that $I_1\mathcal{O}_L = I_2\mathcal{O}_L$ and satisfy the following. Let $J = I_1\mathcal{O}_L = I_2\mathcal{O}_L$. For each prime number p that divides the discriminant of L over $\mathbb{Q}$, $v_\mathfrak{p}(J) = 0$ for each prime ideal $\mathfrak{p} \subset \mathcal{O}_L$ that divides p. Then, there exist a fractional ideal $I \subset K$ such that $I_1 = I\mathcal{O}_{K_1}$ and $I_2 = I\mathcal{O}_{K_2}$*

Proof. Let p be a prime number. Let $\mathfrak{p}$ be a prime ideal in K that divides p. Let $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^e\mathfrak{P}_2^e...\mathfrak{P}_m^e$, $\mathfrak{p}\mathcal{O}_{K_1} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_s^{e_s}$ and $\mathfrak{p}\mathcal{O}_{K_2} = \mathfrak{q}_1^{f_1}\mathfrak{q}_2^{f_2}...\mathfrak{q}_t^{f_t}$ be the factorization of $\mathfrak{p}$ in prime ideals in L, K_1 and K_2 respectively. All the exponents of the prime ideals $\mathfrak{P}$ are the same because L/K is Galois. It can also be seen that each of $\mathfrak{p}_i$ is a product of some $\mathfrak{P}_j^{e/e_i}$ and each $\mathfrak{q}_i$ is a product of some $\mathfrak{P}_j^{e/f_i}$ because ramification is multiplicative on towers of extensions. Let S_i be the set of the prime ideals $\mathfrak{P}_k$ that divide $\mathfrak{p}_i$ and T_j be the set of the prime ideals $\mathfrak{P}_k$ that divide $\mathfrak{q}_j$. Let S be the set of all the $\mathfrak{P}_i$. Each $\mathfrak{P}_i$ lies over exactly one $\mathfrak{p}_j$ and over exactly one $\mathfrak{q}_k$, therefore, $S = \cup S_i = \cup T_i$. Also, the S_i are pairwise disjoint, and the same holds for the T_j. Let

G be the Galois group of L over K and let H_1 and H_2 be the subgroups of G that belong to K_1 and K_2 respectively.

The following lemmas will use the same notation as above

Lemma 3.3. $G =< H_1, H_2 >$

Proof. Let $H =< H_1, H_2 >$ and let K_H be the fixed field of H. H_1 and H_2 are subgroups of G, then $H < G$. $H_1 < H$ and $H_2 < H$, then $K_H \subset K_1$ and $K_H \subset K_2$, then $K_H \subset K_1 \cap K_2 = K$. Then, $H > G$. Thus, $G = H =< H_1, H_2 >$. □

Lemma 3.4. *Let $\sigma \in H_1$. Then, for each $\mathfrak{P}_i$, $\sigma(\mathfrak{P}_i)$ and $\mathfrak{P}_i$ are in the same S_j. The same for $\sigma \in H_2$ and T_j*

Proof. Let $\mathfrak{P}_i \in S$. Let j such that $\mathfrak{P}_i \in S_j$, then $\mathfrak{P}_i$ divides $\mathfrak{p}_j$. Since $\sigma \in H_1$ and $\mathfrak{p}_j \subset K_1$, $\sigma(\mathfrak{p}_j) = \mathfrak{p}_j$. Then, $\prod_{\mathfrak{P}_k \in S_j} \sigma(\mathfrak{P}_k)^{e/e_j} = \prod_{\mathfrak{P}_k \in S_j} \mathfrak{P}_k^{e/e_j}$. We know that an automorphism takes prime ideals to prime ideals. Then, $\sigma(\mathfrak{P}_i) = \mathfrak{P}_k$ for some $\mathfrak{P}_k \in S_j$. Thus, $\sigma(\mathfrak{P}_i)$ and $\mathfrak{P}_i$ are in the same S_j. Analogously, for $\sigma \in H_2$ and T_j □

Lemma 3.5. *Assume that p does not divide the discriminant of L over $\mathbb{Q}$. If $\mathfrak{P}_i, \mathfrak{P}_j \in S_k$ or $\mathfrak{P}_i, \mathfrak{P}_j \in T_k$ for some k, then $v_{\mathfrak{P}_i}(J) = v_{\mathfrak{P}_j}(J)$*

Proof. If $\mathfrak{P}_i, \mathfrak{P}_j \in S_k$, then $\mathfrak{p}_k \mathcal{O}_L = \mathfrak{P}_i \mathfrak{P}_j ...$ in its decomposition. Let $v_{\mathfrak{p}_k}(I_1) = e$, then $J = I_1 \mathcal{O}_L = \mathfrak{p}_k^e ....$ Replacing $\mathfrak{p}_k$ for its product of prime ideals in L, $J = (\mathfrak{P}_i^e \mathfrak{P}_j^e ...) ....$ Then $v_{\mathfrak{P}_i}(J) = v_{\mathfrak{P}_j}(J)$. Analogously the same will occur if $\mathfrak{P}_i, \mathfrak{P}_j \in T_k$. □

Let us assume that p does not divide the discriminant of L over $\mathbb{Q}$

Let $\mathfrak{P} = \mathfrak{P}_1$. All the $\sigma \in Gal(L/K)$ act transitively on all the $\mathfrak{P}_i$. Then, for each $\mathfrak{P}_i$, there exist $\sigma \in Gal(L/K)$ such that $\mathfrak{P}_i = \sigma(\mathfrak{P})$ Let $\mathfrak{Q} = \mathfrak{P}_i$ for some i and let $\sigma \in Gal(L/K)$ such that $\mathfrak{Q} = \sigma(\mathfrak{P})$. Let H_1 and H_2 be the subgroups of G that belong to K_1 and K_2 respectively. From Lemma 3.3, $\sigma = \sigma_1 \sigma_2 ... \sigma_\ell$ where $\sigma_i \in H_1$ or $\sigma_i \in H_2$. For each σ_i and any prime ideal $\mathfrak{P}_j$, from the Lemma 3.4 $\sigma_i(\mathfrak{P}_j)$ and $\mathfrak{P}_j$ are prime ideals in the same S_k or T_k. From the Lemma 3.5, $v_{\sigma_i}(\mathfrak{P}_j)(J) = v_{\mathfrak{P}_j}(J)$. Thus, $v_{\mathfrak{P}}(J) = v_{\sigma_\ell(\mathfrak{P})}(J) = v_{\sigma_{\ell-1}\sigma_\ell(\mathfrak{P})}(J) = ... = v_{\sigma_1\sigma_2...\sigma_\ell(\mathfrak{P})}(J) = v_{\sigma(\mathfrak{P})}(J) = v_{\mathfrak{Q}}(J)$.

This was done for any $\mathfrak{Q}$ of the form $\mathfrak{P}_i$, then $v_{\mathfrak{P}_i}(J) = e$ for all i, thus $v_{\mathfrak{p}}(J) = e$ too. Now, we have that the ideal of J that has in its factorization prime ideals that divide $\mathfrak{p}$ comes from $\mathfrak{p}^e$ which is an ideal in K. Therefore, doing this for all prime ideals $\mathfrak{p} \in K$, we have that $J = \prod_{\mathfrak{p} \in Spec(K)} \mathfrak{p}^{e_i}$ comes from an ideal in K.

□

Now we will describe the algorithm to determine whether or not α can be written as $\beta\gamma$ for some algebraic numbers β and γ such that $\deg(\beta) < \deg(\alpha)$ and $\deg(\gamma) < \deg(\alpha)$. Let L be the Galois closure of $\mathbb{Q}(\alpha)$. From Theorem 1.4, it will suffice to search for $\beta, \gamma \in L$.

Now, for each pair of subfields of L that have dimension less than $\deg(\alpha)$, let one such pair be K_1 and K_2, we will check if there exist $\beta \in K_1$ and $\gamma \in K_2$ that satisfy $\alpha = \beta\gamma$.

Here we will use some facts about prime ideals. Let I_α be the principal fractional ideal generated by α in L. Now we want some principal fractional ideals I_β and

I_γ in K_1 and K_2 respectively such that $I_\alpha = I_\beta I_\gamma$, which is the same as $v_{\mathfrak{p}}(I_\alpha) = v_{\mathfrak{p}}(I_\beta) + v_{\mathfrak{p}}(I_\gamma)$ for all prime ideals $\mathfrak{p}$ in L.
We will show that the ideals I_β and I_γ can be taken to have a very constrained form and that it will suffice to take such ideals of that form. Let S be the set of the following

- The prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ such that the prime number in $\mathbb{Q}$ below $\mathfrak{p}$ does not divide the discriminant of L over K.
- The prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ such that there exist a prime ideal $\mathfrak{P} \subset \mathcal{O}_L$ over $\mathfrak{p}$ that appears in the factorization of I_α in prime ideals.
- Prime ideals that are representatives of each ideal class in K.

Let S_1, S_2 and T be the sets of prime ideals in K_1, K_2 and L that lie over some prime ideal K that belongs to S.

For the next two propositions we will assume that there exist such principal fractional ideals I_β and I_γ such that $I_\alpha = I_\beta I_\gamma$.

Proposition 3.6. *There exist I'_β and I'_γ so that the prime ideals in K that lie below any prime that appears in the factorization of I'_β or I'_γ are all in S and $I'_\beta I'_\gamma = I_\alpha$.*

Proof. Let $I_\beta = \prod \mathfrak{p}^{e_{\mathfrak{p}}} \in I(K_1)$, let $I_1 = \prod_{\mathfrak{p}\in S_1} \mathfrak{p}^{e_{\mathfrak{p}}} \in K_1$ and let $I''_\beta = I_\beta I_1^{-1}$, then $I''_\beta = \prod_{\mathfrak{p}\notin S_1} \mathfrak{p}^{e_{\mathfrak{p}}} \in I(K_1)$. Similarly, let $I_\gamma = \prod \mathfrak{q}^{e_{\mathfrak{q}}} \in I(K_2)$, let $I_2 = \prod_{\mathfrak{q}\in S_1} \mathfrak{q}^{e_{\mathfrak{q}}} \in I(K_2)$, and let $I''_\gamma = I_\gamma I_2^{-1}$, then $I'_\gamma = \prod_{\mathfrak{q}\notin S_2} \mathfrak{q}^{e_{\mathfrak{q}}} \in I(K_2)$. Let $J = I''_\beta I''_\gamma = I_\beta I_1^{-1} I_\gamma I_2^{-1} = I_\gamma I_1^{-1} I_2^{-1} \in I(L)$.

$J = I''_\beta I''_\gamma = \prod_{\mathfrak{p}\notin S_1} \mathfrak{p}^{e_{\mathfrak{p}}} \prod_{\mathfrak{q}\notin S_2} \mathfrak{q}^{e_{\mathfrak{q}}}$, then $J = \prod_{\mathfrak{P}\notin T} \mathfrak{P}^{e_{\mathfrak{P}}}$.

$J = I_\alpha I_1^{-1} I_2^{-1}$, then $J = \prod_{\mathfrak{P}\in T} \mathfrak{P}^{e_{\mathfrak{P}}}$ since I_α, I_1, I_2 have in their factorization only prime ideals in T.

Then, J has to be $\mathcal{O}_L$. Then we have that $I''_\beta I''_\gamma = \mathcal{O}_L$, then $I''_\beta \mathcal{O}_L = I''^{-1}_\gamma \mathcal{O}_L$. Now we know that the fractional ideal $I''_\beta = \prod_{\mathfrak{p}\notin S_1} \mathfrak{p}^{e_{\mathfrak{p}}} \mathcal{O}_L$ only has in its factorization prime ideals that are not in T. As a consequence, the prime number that lies below $\mathfrak{P}$ does not divide the discriminant of L. The same happens for I''^{-1}_γ.

Now we have that I'_β and I'^{-1}_γ satisfy the condition of Theorem 3.2. Then there exists a fractional ideal $J \in I(K)$ such that $I''_\beta = J\mathcal{O}_{K_1}$ and $I''^{-1}_\gamma = J\mathcal{O}_{K_2}$. Let $\mathfrak{p} \in S$ be the representative of the ideal class of J. Let $I'_\beta = I_1\mathfrak{p}$ and $I'_\gamma = I_2\mathfrak{p}^{-1}$ Now all the prime ideals in K that lie below any prime ideal that appears in the factorization of I'_β are the ones in S and the same for I'_γ. $I'_\beta = I_1\mathfrak{p}^{-1} = I_\beta I''^{-1}_\beta \mathfrak{p} = I_\beta J^{-1}\mathfrak{p}$ is in the same ideal class as I_β, then I'_β is principal. Analogously, I'_γ is principal. Recall that $J = I_\alpha I_1^{-1} I_2^{-1}$ and $J = \mathcal{O}_L$. Then, $I_\alpha = I_1 I_2$, therefore, $I_\alpha = I'_\beta I'_\gamma$. □

Now, we will assume that I_β and I_γ are the I'_β and I'_γ found.

Proposition 3.7. *There exists a set of prime ideals S such that I_β and I_γ contain only prime ideals that lie over some prime ideal in S. Then there exist I'_β and I'_γ such that the exponents of the prime ideals in the factorization of I'_β in K_1 and the factorization of I_γ in K_2 are bounded by some computable number N.*

Proof. Let c_1 and c_2 be the number of elements in the ideal class groups of K_1 and K_2, let c be the lcm of c_1 and c_2.
For each prime ideal $\mathfrak{p} \in S$, let $m_{\mathfrak{p}} = \sum |v_{\mathfrak{P}_i}(I_\alpha)|$ where $\mathfrak{P}_i$ are all the prime ideals in L over $\mathfrak{p}$. Let $M = \max(m_{\mathfrak{p}})$ for all the prime ideals $\mathfrak{p} \in S$. Let $n = [L : K]$.
Let $N = cn^2 + M$.

Let $\mathfrak{p} \in S$ be a prime ideal in K. Let the decompositions of $\mathfrak{p}$ be $\mathfrak{p}\mathcal{O}_{K_1} = \prod \mathfrak{p}_i^{e_i}$, $\mathfrak{p}\mathcal{O}_{K_2} = \prod \mathfrak{q}_i^{f_i}$ and $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i^{e}$. Let $\mathfrak{p}_i = \prod \mathfrak{P}^{e/e_i}$ for some $\mathfrak{P}$, let S_i be that set of the $\mathfrak{P}$ that divide $\mathfrak{p}_i$. Let $\mathfrak{q}_i = \prod \mathfrak{P}^{e/f_i}$ for some $\mathfrak{P}$, let T_i be the set of those $\mathfrak{P}$ that divide $\mathfrak{q}_i$.

Lemma 3.8. *For each $\mathfrak{p}_i$ and $\mathfrak{q}_j$, all the numbers $v_{\mathfrak{p}_i}(\beta)$ and $v_{\mathfrak{q}_i}(\gamma)$ can be taken to be bounded by N*

Proof. Let $x_i = v_{\mathfrak{p}_i}(I_\beta)$ for all i and $y_j = v_{\mathfrak{q}_j}(I_\gamma)$ for all j. Now we will check that $v_{\mathfrak{P}_i}(I_\alpha) = v_{\mathfrak{P}_i}(I_\beta) + v_{\mathfrak{P}_i}(I_\gamma)$ for each $\mathfrak{P}_i$. Let $\mathfrak{P}$ be one of the $\mathfrak{P}_i$, let i_1 and i_2 such that $\mathfrak{P}$ lies over $\mathfrak{p}_{i_1}$ in K_1 and lies over $\mathfrak{q}_{i_2}$ in K_2. Then, checking the valuations over $\mathfrak{P}$ we have that $x_{i_1}(e/e_{i_1}) + y_{i_2}(e/f_{i_2}) = v_{\mathfrak{P}}(I_\alpha)$.

Let us assume that one exponent of the x_i or y_j is not bounded by $cn^2 + M$. Without loss of generality $x_1 > cn^2 + M$. Let $t = \lfloor x_1/cn \rfloor$. Let $x_1' = x_1 - tcn < cn$, let $x_i' = x_i - tcn(e_i/e_1)$ and $y_j' = y_j + tcn(f_j/e_1)$ for all i and j. Such numbers x_i' and y_j' are integers because all e_i and f_j divide e and e divides n . Now, each of the equations of the form $x_{i_1}'(e/e_{i_1}) + y_{i_2}'(e/f_{i_2}) = v_{\mathfrak{P}}(I_\alpha)$ is going to be satisfied. Then the valuation equation will be satisfied for each prime ideal in L that lies over $\mathfrak{p}$. Let $\mathfrak{P}_{i_1}$ be a prime ideal that divides $\mathfrak{p}_1$ Let $y = y_j$ for some j. We will now show that there is an equation of the following form

$$x_1'(e/e_1) + y_j'(e/f_j) = t$$

for some constant $t \leq M$. This will allow us to bound y_j

Let $\mathfrak{P}$ be a prime ideal in T_j for some j. From Lemmas 3.3 and 3.4 there is an element of $Gal(L/K)$ that takes $\mathfrak{P}_{i_1}$ to $\mathfrak{P}$ and that is generated by H_1 and H_2. Let that element be $\sigma = \sigma_\ell \sigma_{\ell-1} ... \sigma_1$ with minimal ℓ. This minimal ℓ can make sure that all $\sigma_k \sigma_{k-1} ... \sigma_1(\mathfrak{P}_{i_1})$ are different prime ideals. We can assume that there are not σ_i and σ_{i+1} such that they are both in H_1 or both in H_2. If $\sigma_0 \in H_1$, from Lemma 3.5 $\sigma_0(\mathfrak{P}_{i_0}) \in S_1$, then $\sigma_0(\mathfrak{P}_{i_0})$ is a prime ideal that divides $\mathfrak{p}_1$. Thus, we can take $\sigma_0(\mathfrak{P}_{i_0})$ instead of $\mathfrak{P}_{i_0}$ and assume that $\sigma_0 \in H_2$. Analogously, we can assume that $\sigma_\ell \in H_1$ because $\mathfrak{P}$ was chosen as a prime ideal in T_j. Therefore, $\sigma_i \in H_1$ for i even and $\sigma_i \in H_2$ for i odd. Also, l is even Let $\mathfrak{P}_{i_k} = \sigma_{k-1} ... \sigma_1(\mathfrak{P}_{i_1})$. For all k we will have the following using Lemma 3.5. $\sigma_{2k} \in H_1$, then $\mathfrak{P}_{i_{2k}}$ and $\mathfrak{P}_{i_{2k+1}}$ are in the same S_a for some a. Analogously, $\mathfrak{P}_{i_{2k-1}}$ and $\mathfrak{P}_{i_{2k}}$ are in the same T_b for some b. Let $\mathfrak{P}_{i_k} \in S_{a_k}$ and $\mathfrak{P}_{i_k} \in T_{b_k}$ for all k. Then, $a_{2k} = a_{2k+1}$ and $b_{2k-1} = b_{2k}$. Recall that $\mathfrak{P}_{i_1} \in S_1$ and that $\mathfrak{P}_{i_{\ell+1}} = \mathfrak{P} \in S_j$. Then, $a_1 = 1$ and $b_{\ell+1} = j$. Taking the valuation of $\mathfrak{P}_{i_k}$,

$$x_{a_k}'(e/e_{a_k}) + y_{b_k}'(e/f_{b_k}) = v_{\mathfrak{P}_{i_k}}(I_\alpha)$$

for each k. Let that equation be E_k. The equation $\sum_1^{\ell+1}(-1)^k E_k$ will become

$$x_{a_1}'(e/e_{a_1}) + y_{b_{\ell+1}}'(e/f_{b_{\ell+1}}) = \sum_1^{\ell+1}(-1)^k v_{\mathfrak{P}_{i_k}}(I_\alpha)$$

We know that $a_1 = 1$ and $b_{\ell+1} = j$. Also all the $\mathfrak{P}_{i_k}$ are different. Then,

$$|x'_1(e/e_1) + y'_j(e/f_j)| = |\sum_1^{\ell+1}(-1)^k v_{\mathfrak{P}_{i_k}}(I_\alpha)| \leq \sum |v_{\mathfrak{P}_i}(I_\alpha)|$$

Analogously we can get

$$|x'_1(e/e_1) - x'_i(e/e_i)| \leq \sum |v_{\mathfrak{P}_i}(I_\alpha)|$$

Then, $|y'_j| \leq M(f_j/e) + |x'_1(f_j/e_1)| < M + cn^2$ for any j and $|x'_i| \leq M(e_i/e) + |x'_1(e_i/e_1)| < M + cn^2$. Thus, all x'_i and y'_j are bounded by $N = M + cn^2$.

□

Let $x_{\mathfrak{p},i} = v_{\mathfrak{p}_i}(I_\beta)$ for all $\mathfrak{p}_i$ that divide $\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ in K. Analogously let $y_{\mathfrak{q},j} = v_{\mathfrak{q}_j}(I_\beta)$. and let $x'_{\mathfrak{p},i}$ and $y'_{\mathfrak{q},j}$ be the exponents after bounding them using Lemma 3.8. Let

$$I'_\beta = \prod_{\mathfrak{p}\in S}(\prod_{\mathfrak{p}_i \text{ over } \mathfrak{p}} \mathfrak{p}_i^{x'_{\mathfrak{p},i}})$$

and

$$I'_\gamma = \prod_{\mathfrak{p}\in S}(\prod_{\mathfrak{q}_j \text{ over } \mathfrak{p}} \mathfrak{q}_i^{y'_{\mathfrak{q},j}})$$

Now,

$$I'_\beta I_\beta^{-1} = \prod_{\mathfrak{p}\in S}(\prod_{\mathfrak{p}_i \text{ over } \mathfrak{p}} \mathfrak{p}_i^{-tcn(e_i/e_1)})$$

This ideal has all of its exponents multiples of c which is a multiple of the class group of K_1. Then there exists a principal fractional ideal J_1 in K_1 such that $I'_\beta I_\beta^{-1} = J_1$. Then, I'_β is principal, analogously I'_γ is also principal.

□

Now it suffices to search for principal fractional ideals I_β and I_γ that satisfy the following

- Their factorizations only contain prime ideals that lie over a prime ideal in S
- The exponents of such prime ideals are bounded

Let $\mathfrak{p} \in S$ be a prime ideal in K. Let the decompositions of $\mathfrak{p}$ be $\mathfrak{p}\mathcal{O}_{K_1} = \prod \mathfrak{p}_i^{e_i}$, $\mathfrak{p}\mathcal{O}_{K_2} = \prod \mathfrak{q}_i^{f_i}$ and $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i^{e}$. Let $x_i = v_{\mathfrak{p}_i}(I_\beta)$ for all i and $y_j = v_{\mathfrak{q}_j}(I_\gamma)$. What we want now is to find such x_i and y_j or determine if they exist. Let $x = x_1$. As seen in the proof of Lemma 3.8, for every z of the form x_i or y_j there is an equation that involves $ax + bz = c$. Then, we have that every variable of the system of equations is uniquely determined by x. So, for all x with $|x| < cn^2 + M$ we compute the other variables and check if they satisfy all the equations. This way, we will get a finite number of possibilities. We do the same for every prime ideal over S and end up with finitely many possibilities. For each of those possibilities we compute the class of the ideals in K_1 and K_2. We only keep the possibilities that give us principal fractional ideals both in K_1 and K_2, let the set of these solutions be A. A solution for I_β and I_γ gives us one of these possibilities after doing all the changes. If A were empty then there is no solution for $I_\beta I_\gamma = I_\alpha$. Otherwise, there is a set of finite solutions for the ideals. For each solution I_β and I_γ, let β be a generator of I_β and γ a generator for I_γ. Then, the principal fractional ideal generated by $\beta\gamma$ in L is the same as the one generated by α, then there exist a unit $u \in L$ such that $\alpha = \beta\gamma u$. As we do this for each solution of ideals, we get a finite set of units, let that be S_u.

Proposition 3.9. *There are principal fractional ideals $I_\alpha \in I(L)$, $I_\beta \in I(K_1)$, $I_\gamma \in I(K_2)$ such that $I_\alpha = I_\beta I_\gamma$. Then, there exist $\beta \in K_1$ and $\gamma \in K_2$ such that $\beta\gamma = \alpha$ if and only if some unit of L in S_u can be written as the product of two units in K_1 and K_2.*

Proof. Let us assume that there is some unit $u \in S_u$ that can be written as u_1u_2 where u_1 is a unit in K_1 and u_2 is a unit in K_2. Then, there are $\beta \in K_1$ and $\gamma \in K_2$ such that $\alpha = \beta\gamma u$ because $u \in S_u$ and that is how S_u was defined. Then, $\alpha = (\beta u_1)(\gamma u_2)$ where $\beta u_1 \in K_1$ and $\gamma u_2 \in K_2$.
Now let us assume that there are $\beta \in K_1$ and $\gamma \in K_2$ such that $\alpha = \beta\gamma$. Then, the principal fractional ideals generated by β and γ had to be a solution for $I_\beta I_\gamma = I_\alpha$. Then, there had to be $\beta' \in K_1$ and $\gamma' \in K_2$ that are generators of the principal fractional ideals generated by β and γ respectively such that $\alpha = \beta'\gamma' u$. From that such unit u was also included in S_u. Now, generators in a principal fractional ideal differ up to a unit. Then, there exist units $u_1 \in K_1$ and $u_2 \in K_2$ such that $\beta = \beta u_1$ and $\gamma = \gamma' u_2$. Then, $\beta'\gamma' u = \alpha = \beta\gamma = \beta' u_1 \gamma' u_2$. Thus, $u = u_1u_2$ □

Now we only need to check for each unit $u \in S$ if there exist units $u_\beta \in K_1$ and $u_\gamma \in K_2$ such that $u_\beta u_\gamma = u$.
It is known that the unit group of a field has the form $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}^n$. From [2] the generators of unit group of a field can be computable. Then, using group theory and linear algebra it determined whether or not there exist such units u_β and u_γ.

4. Sums of polynomials of algebraic numbers

Let $P_1, P_2 \in \mathbb{Q}[x]$. Given an algebraic number α, describe an algorithm to decide whether or not α can be expressed as $P_1(\beta) + P_2(\gamma)$ where β and γ are algebraic numbers such that $\deg(\beta) < \deg(\alpha)$ and $\deg(\gamma) < \deg(\alpha)$.

Theorem 4.1. *There exist algebraic numbers α, β, γ and two polynomials $P_1, P_2 \in \mathbb{Q}[x]$ such that $\alpha = P_1(\beta) + P_2(\gamma)$, $\deg(\beta) < \deg(\alpha)$ and $\deg(\gamma) < \deg(\alpha)$ and there does not exist β' and γ' such that $\alpha = P_1(\beta') + P_2(\gamma')$, $\deg(\beta') < \deg(\alpha)$, $\deg(\gamma') < \deg(\alpha)$ and β', $\gamma' \in K$ where K is the Galois closure of $\mathbb{Q}(\alpha)$.*

Proof. Let x_1 be a negative root of the polynomial $x^3 - 3x + 1$ and x_2 be a negative root of the polynomial $x^3 + x^2 - 2x - 1$. Let $\alpha = x_1 + x_2$, $\beta = \sqrt{x_1}$, $\gamma = \sqrt{x_2}$, $P_1(x) = P_2(x) = x^2$.

It can be proved that $\deg(\alpha) = 9$. Clearly, $\deg(\beta) = \deg(\gamma) = 6$. Thus, α, β and γ satisfy the condition.

$\mathbb{Q}(x_1)$ and $\mathbb{Q}(x_2)$ are Galois because both have discriminants that are squares in $\mathbb{Q}$. Then, $\mathbb{Q}(\alpha) = \mathbb{Q}(x_1)\mathbb{Q}(x_2)$ is also Galois, then the Galois closure of $\mathbb{Q}(\alpha)$ is $\mathbb{Q}(\alpha)$. Since $x_1, x_2 \in \mathbb{R}$, $\mathbb{Q}(\alpha) \subset \mathbb{R}$. If there existed β' and γ' such that $\alpha = P_1(\beta') + P_2(\gamma')$, then $\alpha = \beta'^2 + \gamma'^2$. Since $\alpha < 0$, either β' or γ' does not belong to $\mathbb{R}$. Thus, one of them cannot be inside $\mathbb{Q}(\alpha)$, which is the Galois closure of $\mathbb{Q}(\alpha)$. □

.

References

[1] Daniel Marcus. *Number Fields.*
[2] Henri Cohen. *A Course in Computational Algebraic Number Theory.*

E-mail address: bdiehs@mit.edu