Algebraic number theory
Revision exercises

Nicolas Mascot (n.a.v.mascot@warwick.ac.uk)
Aurel Page (a.r.page@warwick.ac.uk)
TA: Pedro Lemos (lemos.pj@gmail.com)

Version: March 2, 2017

Exercise 1. What is the ring of integers of $\mathbb{Q}(\sqrt{98})$?

Exercise 2. What kinds of number fields have a unit group of rank 1 ?

Exercise 3. Compute the class group of $\mathbb{Q}(\sqrt{-47})$.

Exercise 4. The aim of this exercise is to determine the class group of $K = \mathbb{Q}(\sqrt{82})$, seen as a subfield of $\mathbb{R}$.

1. Prove that the class group of K is either trivial or isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$.
2. What is the rank of the unit group of K ? Compute a fundamental unit $u > 1$ of K.
3. Suppose that there exist an element $\beta = x + y\sqrt{82} \in \mathbb{Z}_K$ of norm 2. Why may we assume that $\frac{1}{\sqrt{u}} < \beta < \sqrt{u}$? Prove that $x - y\sqrt{82} = \frac{2}{\beta}$, use this to derive bounds on x, and deduce that no such β exists.
4. Prove similarly that no element of $\mathbb{Z}_K$ has norm -2.
5. What is the class group of K ?
6. Was is absolutely necessary that the unit u be fundamental for the above reasoning to be valid ?

Exercise 5. *Let $f(x) = x^3 - 4x^2 + 2x - 2$, which is an irreducible polynomial over $\mathbb{Q}$ (why ?), and let $K = \mathbb{Q}(\alpha)$, where α is a root of f.*

1. *Given that* $\operatorname{disc} f = -300$*, what can you say about the ring of integers of K and the primes that ramify in K ? What if, on the top of that, you notice that $f(x+3) = x^3 + 5x^2 + 5x - 5$?*

We have $\operatorname{disc} f = -300 = -2^2 \cdot 3 \cdot 5^2$, so the order $\mathbb{Z}[\alpha]$ is p-maximal at every prime $p \neq 2, 5$. Besides, f is Eisenstein at 2, so $\mathbb{Z}[\alpha]$ is actually also maximal at $p = 2$, and 2 is totally ramified in K; incidentally this also proves that f is irreducible as claimed. We thus have only two possibilities: either $\mathbb{Z}[\alpha]$ is also maximal at $p = 5$, in which case $\mathbb{Z}_K = \mathbb{Z}[\alpha]$, so that $\operatorname{disc} K = -2^2 \cdot 3 \cdot 5^2$ and so K ramifies precisely at 2, 3 and 5, or $\mathbb{Z}[\alpha]$ is not maximal at $p = 5$, in which case $\mathbb{Z}[\alpha]$ has index exactly 5 (and not a larger power of 5 since $5^4 \nmid \operatorname{disc} f$), and so $\operatorname{disc} K = -2^2 \cdot 3$ so K is ramified precisely at 2 and 3, but not at 5.

However, the fact that $\alpha - 3$ is a root of $f(x+3)$ which is Eisenstein at 5 proves that the order $\mathbb{Z}[\alpha - 3]$ is maximal at 5 and that 5 is totally ramified in K. But clearly $\mathbb{Z}[\alpha - 3] = \mathbb{Z}[\alpha]$, so $\mathbb{Z}[\alpha]$ is in fact maximal at 5 and so $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ and K is ramified precisely at 2, 3 and 5. On the top of that, we have shown that 2 and 5 are actually *totally* ramified. We do not know yet whether 3 is totally ramified.

2. *Prove that $\mathbb{Z}_K$ is a PID.*

   Hint: For $n \in \mathbb{Q}$, what relation is there between $f(n)$ and the norm of $n - \alpha$? Use this to find elements of small norm, and thus relations in the class group.

   Let (r_1, r_2) be the signature of K. As $\operatorname{disc} K = -300 < 0$, we know that r_2 is odd, and so the relation $r_1 + 2r_2 = [K : \mathbb{Q}] = 3$ forces $r_1 = r_2 = 1$. As a result, the Minkowski bound for K is $M = \frac{3!}{3^3}\frac{4}{\pi}\sqrt{300} \approx 4.9$, so the class group of K is generated by the primes above 2 and 3.

   We already know that 2 is totally ramified, say $2\mathbb{Z}_K = \mathfrak{p}_2^3$, whence the relation $[\mathfrak{p}_2]^3 = 1$ in the class group. To compute the decomposition of 3, we factor f mod 3 (this is legitimate because the order $\mathbb{Z}[\alpha]$ attached to f, being maximal at every p, is in particular maximal at 3). We thus compute that

   $$f \equiv x^3 - x^2 - x + 1 \bmod 3 \equiv (x-1)(x^2-1) \equiv (x-1)^2(x+1) \bmod 3,$$

   whence the decomposition $3\mathbb{Z}_K = \mathfrak{p}_3^2\mathfrak{p}_3'$, where $\mathfrak{p}_3 = (3, \alpha - 1)$ and $\mathfrak{p}_3' = (3, \alpha + 1)$. We also get the relation $[\mathfrak{p}_3]^2[\mathfrak{p}_3'] = 1$ in the class group.

   Now that we have generators, we need to find relations between these generators. For this, we look for elements of small norm : if the norm of an element only involves powers of 2 and 3, then the principal ideal generated by this element will have the same norm (up to sign), and so its factorisation will only involve $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_3'$, whence a relation between $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$ and $[\mathfrak{p}_3']$. We have

   $$N(n - \alpha) = \prod_{\sigma\colon K \hookrightarrow \mathbb{C}} \sigma(n - \alpha) = \prod_{\sigma\colon K \hookrightarrow \mathbb{C}} \big(n - \sigma(\alpha)\big) = f(n)$$

   for all $n \in \mathbb{Q}$ where the products range over the embeddings of K into $\mathbb{C}$, so we can use this formula to compute the norm of elements of the form $n - \alpha$.

   For example, we have $N(\alpha) = f(0) = -2$, whence $(\alpha) = \mathfrak{q}_2$ where $\mathfrak{q}_2$ is some prime of inertial degree 1 above 2, which can only be $\mathfrak{p}_2$. Thus $[\mathfrak{p}_2] = 1$.

Similarly, we have $N(1-\alpha) = f(1) = -3$, so $(1-\alpha) = \mathfrak{q}_3$ for some prime $\mathfrak{q}_3$ of degree 1 above 3. Thanks to the criterion

$$\mathfrak{p} \mid (\beta) \Longleftrightarrow (\beta) \subseteq \mathfrak{p} \Longleftrightarrow \beta \in \mathfrak{p}$$

valid for all prime $\mathfrak{p}$ and element $\beta \in \mathbb{Z}_K$, we see that $(1-\alpha) = \mathfrak{p}_3$.

Therefore $[\mathfrak{p}_3] = 1$ and so $[\mathfrak{p}_3'] = 1$, so the class group is trivial and $\mathbb{Z}_K$ is a PID.

3. *Find a generator for each of the primes above 2, 3 and 5.*

   We have already proved that $\mathfrak{p}_2 = (\alpha)$ and that $\mathfrak{p}_3 = (\alpha - 1)$. Besides, we know that $(5) = \mathfrak{p}_5^3$ is totally ramified, and since $\alpha - 3$ is a root of $f(x+3) = x^3 + 5x^2 + 5x - 5$, we have $N(\alpha - 3) = 5$ whence $\mathfrak{p}_5 = (\alpha - 3)$.

   It remains to find a generator for $\mathfrak{p}_3'$. For this, we can use the relation $(3) = \mathfrak{p}_3^2\mathfrak{p}_3' = (\alpha-1)^2\mathfrak{p}_3'$ to deduce that $\mathfrak{p}_3' = (\beta)$ where $\beta = \frac{3}{(\alpha-1)^2}$. Note that we get for free that β is an algebraic integer, and that its norm is ± 3.

   There is (at least) one other easy way to find a generator for $\mathfrak{p}_3'$: we have $N(2-\alpha) = f(2) = -6$, so the ideal $(2-\alpha)$ factors as $\mathfrak{q}_2\mathfrak{q}_3$, a,d as in the previous question we see that $\mathfrak{q}_2 = \mathfrak{p}_2$ and that $\mathfrak{q}_3 = \mathfrak{p}_3'$. Thus $\mathfrak{p}_3' = (2-\alpha)/(\alpha) = (\beta')$, where $\beta' = \frac{2-\alpha}{\alpha} = \frac{2}{\alpha} - 1 = \alpha^2 - 4\alpha + 1$ in view of the relation $f(\alpha)/\alpha = 0$.

4. *Use the results of the previous question to discover that $u = 2\alpha^2 - \alpha + 1$ is a unit.*

   The key to discovering units is finding more than one generator for the same principal ideal.

   For instance, we have just seen that $\mathfrak{p}_3' = (\beta) = (\beta')$, so β'/β is a unit. Unfortunately, it turns out that

   $$\frac{\beta'}{\beta} = (\alpha^2 - 4\alpha + 1)\frac{(\alpha-1)^2}{3} = -1,$$

   so this unit is not a very interesting one...

   Let's try again : we have $(2) = \mathfrak{p}_2^3 = (\alpha)^3 = (\alpha^3)$, so $u = \alpha^3/2 = 2\alpha^2 - \alpha + 1$ is a unit.

   We could also have used the fact that $(5) = (\alpha - 3)^3$ to discover the unit $v = \frac{(\alpha-3)^3}{5} = -\alpha^2 + 5\alpha - 5$.

5. We use the unique embedding of K into $\mathbb{R}$ to view K as a subfield of $\mathbb{R}$ from now on. Prove that there exists a unit $\varepsilon \in \mathbb{Z}_K^\times$ such that $\mathbb{Z}_K^\times = \{\pm\varepsilon^n, n \in \mathbb{Z}\}$ and $\varepsilon > 1$.

   According to Dirichlet's theorem, the rank of $\mathbb{Z}_K^\times$ is $r_1 + r_2 - 1 = 1$. Besides, as K can be embedded into $\mathbb{R}$, the only roots of unity it contains are ± 1, so $\mathbb{Z}_K^\times = \{\pm\varepsilon^n, n \in \mathbb{Z}\}$ for some fundamental unit ε. Possibly after replacing ε with $\pm\varepsilon^{\pm 1}$ which is also a fundamental unit, we may assume that $\varepsilon > 1$.

   Note that since $\mathbb{Z}_k^\times$ has rank 1, there must be a relation between our units u and v; indeed it turns out that $v = 1/u$.

6. *By the technique of exercise 2 from exercise sheet number 5, it can be proved that* $\varepsilon \geqslant 4.1$. *Given that* $u \approx 23.3$, *prove that* u *is a fundamental unit.*

   Hint : Reduce u *modulo the primes above 3 to prove that* u *is not a square in* $\mathbb{Z}_K$.

   What is the regulator of K *?*

   We have $u = \pm\varepsilon^n$ for some $n \in \mathbb{Z}$. As $u > 1$, we must in fact have $u = \varepsilon^n$ for some $n > 0$. Besides, since $\varepsilon > 4.1$, we have $n \leqslant 2$. As a result, we either have $u = \varepsilon$ or $u = \varepsilon^2$; in the first case, u is a fundamental unit, in the second case it isn't.

   In order to prove that u is fundamental, we are going to prove that u is not a square in K. As u is a unit, its norm is ± 1, so we could conclude immediately if its norm were -1; unfortunately $N(u) = +1$, so we must find something else.

   The key is to compute the reduction of u modulo some primes $\mathfrak{p}$: if we get a non-square in the finite field $\mathbb{Z}_K/\mathfrak{p}$, this will prove that u is not a square. Now, every element of $\mathbb{F}_2$ is a square, so let us not consider $\mathfrak{p} = \mathfrak{p}_2$. Let us try $\mathfrak{p} = \mathfrak{p}_3$ instead : we have $\alpha - 1 \in \mathfrak{p}_3$, so $\alpha \equiv 1 \bmod \mathfrak{p}_3$ and so $u = 2\alpha^2 - \alpha + 1 \equiv 2 \bmod \mathfrak{p}_3$, which is not a square in $\mathbb{Z}_K/\mathfrak{p}_3$, bingo ! You may check that, on the other hand, $\mathfrak{p} = \mathfrak{p}_3'$ and $\mathfrak{p}_5$ were inconclusive.

   As a consequence, the regulator of K is $\log \varepsilon = \log u$. (This turns out to be pretty close to π, but this is purely coincidental.)

Exercise 6. *Let* $f(x) = x^4 + 3x^3 - 18x^2 - 24x + 129$, *which is an irreducible polynomial over* $\mathbb{Q}$ *(why ?), and let* $K = \mathbb{Q}(\alpha)$, *where* α *is a root of* f.

1. *If I told you that* $\operatorname{disc} f = 930069$, *why would not that be very useful to you ? Which information can you get from that nonetheless ?*

   The primary use of the discriminant is the determination of the ring of integers and of the ramification of the primes. However, this is done in terms of the factorisation of the discriminant, and since we'd rather not factor 930069 by hand there is not much we can do. There is still something though : since we are dealing with a field of degree 4, the possible signatures are $(r_1, r_2) = (4, 0)$, $(2, 1)$ and $(0, 2)$, and the fact that $\operatorname{disc} f > 0$ and that $\operatorname{disc} K$ differs from it by a square means that $\operatorname{disc} K > 0$, so r_2 is even. As a result, our field K is either totally real or totally imaginary.

2. *I now tell you that the roots of* f *are approximately* $-4.1 \pm 0.1i$ *and* $2.6 \pm 1.0i$. *What is the signature of* K *? Can you compute the trace of* α *from these approximate values ? Why is the result obvious ?*

   The non-realness of the roots means that K is totally imaginary, so its signature is in fact $(0, 2)$. The roots of f are the images of α under the embeddings of K into $\mathbb{C}$, so $\operatorname{Tr}(\alpha)$ is the sum of these roots, which is approximately -3. But α is an algebraic integer, so its trace is an integer and so $\operatorname{Tr}(\alpha) = -3$ exactly. However, we already knew that : the trace of an algebraic number is minus the

coefficient of x^{n-1} in its characteristic polynomial (same rule as for matrices). As f is irreducible, it is the characteristic polynomial of α, and so $\mathrm{Tr}(\alpha) = -3$.

3. *If I now tell you that* $\operatorname{disc} f$ *factors as* $3^3 \cdot 7^2 \cdot 19 \cdot 37$*, what can you say about the ring of integers of* K *and the primes that ramify in* K *?*

   We immediately see that $\mathbb{Z}[\alpha]$ is maximal at every prime except possibly at 3 and 7, and that its index is at most $3 \cdot 7$. Even if 3 did divide the index, $\operatorname{disc} K$ would still be divisible by 3 because 3 shows up to an odd power in $\operatorname{disc} f$, so 3 is definitely ramified in K, and so are 19 and 37. The factor 7^2 in $\operatorname{disc} f$ could either come from $\operatorname{disc} K$, in which case 7 ramifies and $\mathbb{Z}[\alpha]$ is maximal at 7, or from the index of $\mathbb{Z}[\alpha]$, in which case 7 does not ramify and $\mathbb{Z}[\alpha]$ is not maximal at 7. The other primes are unramified in K.

   One last thing : if you pay attention enough (and you should !), you'll notice that f is Eisenstein at 3 (and hence irreducible as claimed). As a result, $\mathbb{Z}[\alpha]$ is maximal at 3, and 3 is totally ramified in K. Thus either $\mathbb{Z}[\alpha]$ has index 7 and 7 does not ramify, or $\mathbb{Z}[\alpha] = \mathbb{Z}_K$ and 7 does ramify. In the former case, there would exists elements of $\mathbb{Z}_K$ which, when written as polynomials in α, would have a non-trivial denominator, which would be powers of 7 only.

4. *In principle (don't actually do it), how could you test whether* $\beta = \frac{\alpha^3 - 2\alpha^2 - \alpha + 2}{7}$ *is an algebraic integer ?*

   I'd compute its characteristic polynomial : β is an algebraic integer if and only if this polynomial lies in $\mathbb{Z}[x]$. To do so, I could for example use the formula

$$\chi(\beta) = \prod_{\sigma\colon K \hookrightarrow \mathbb{C}} \big(x - \sigma(\beta)\big) = \prod_{\substack{z \in \mathbb{C} \\ f(z)=0}} \left(x - \frac{z^3 - 2z^2 - z + 2}{7}\right)$$

$$= \mathrm{Res}_y \left(f(y), x - \frac{y^3 - 2y^2 - y + 2}{7}\right).$$

5. *If I now tell you that the characteristic polynomial of* β *is* $\chi(\beta) = x^4 + 28x^3 + 207x^2 + 154x + 247$*, whose discriminant is* $\operatorname{disc} \chi(\beta) = 25364993616$*, which conclusions can you draw from that ?*

   Lots of conclusions. First, since $\chi(\beta)$ lies in $\mathbb{Z}[x]$, we see that β is an algebraic integer, so that $\mathbb{Z}_K$ is strictly larger than $\mathbb{Z}[\alpha]$. In view of question 3, this means that $\mathbb{Z}[\alpha]$ has index 7, that 7 does not ramify in K, and that $\operatorname{disc} K = 3^3 \cdot 19 \cdot 37$.

   Besides, $\mathbb{Z}[\alpha, \beta]$ is an order which is strictly larger than $\mathbb{Z}[\alpha]$, its index is strictly smaller (by a factor which is a power of 7 to be precise, since the denominator of β w.r.t. $\mathbb{Z}[\alpha]$ is 7), and since the index of $\mathbb{Z}[\alpha]$ is 7 which is prime, we must have $\mathbb{Z}_K = \mathbb{Z}[\alpha, \beta]$.

   Finally, since $\operatorname{disc} \chi(\beta) \neq 0$, $\chi(\beta)$ is squarefree. It is thus the minimal polynomial of β (remember proposition 1.2.18), so β has degree 4 and is thus another primitive element for K. Since it is also an algebraic integer, $\mathbb{Z}[\beta]$ is an order in K.

6. *Given that* $\operatorname{disc}\chi(\beta)$ *factors as* $2^4 \cdot 3^3 \cdot 17^4 \cdot 19 \cdot 37$*, what is the index of the order* $\mathbb{Z}[\beta]$ *? What consequence does this have on the expression of a* $\mathbb{Z}$*-basis of* $\mathbb{Z}_K$ *in terms of* β *?*

   The formula

$$\operatorname{disc}\mathcal{O} = [\mathbb{Z}_K : \mathcal{O}]^2 \operatorname{disc} K$$

   shows that the index of $\mathbb{Z}[\beta]$ is $2^2 \cdot 17^2$. A consequence of this is that if we were to elements of $\mathbb{Z}_K$ as polynomials in β, we would get non-trivial denominators, which would be made up of powers of 2 and 17.

7. *Let* $\gamma = \frac{\beta^2-3\beta-3}{34}$*, and let* $\delta = \frac{\beta^3-12\beta-9}{34}$*, whose respective characteristic polynomials are* $\chi(\gamma) = x^4-13x^3+42x^2+8x+1$ *and* $\chi(\delta) = x^4+139x^3+5163x^2+973$*. Prove that* $\{1, \beta, \gamma, \delta\}$ *is a* $\mathbb{Z}$*-basis of* $\mathbb{Z}_K$*.*

   As β is a primitive element for K, the elements 1, β, β^2 and β^3 form a $\mathbb{Q}$-basis of K. Since the elements 1, β, γ, δ are in echelon form with respect to this basis, they also form a $\mathbb{Q}$-basis of K. Let Λ be the lattice they span.

   The fact that $\chi(\gamma)$ and $\chi(\delta)$ lie in $\mathbb{Z}[x]$ shows that γ and δ are algebraic integers, so $\Lambda \subseteq \mathbb{Z}_K$. Besides, it is clear that $\Lambda \supsetneq \mathbb{Z}[\beta]$.

   The change of basis matrix between the two aforementioned bases of K is

$$\begin{pmatrix} 1 & 0 & \frac{-3}{34} & \frac{-9}{34} \\ 0 & 1 & \frac{-3}{34} & \frac{-12}{34} \\ 0 & 0 & \frac{1}{34} & 0 \\ 0 & 0 & 0 & \frac{1}{34} \end{pmatrix}$$

   whose determinant is clearly $1/34^2$. As these bases are $\mathbb{Z}$-bases of $\mathbb{Z}[\beta]$ and of Λ, this means that $[\Lambda : \mathbb{Z}[\beta]] = 34^2 = 2^2 \cdot 17^2 = [\mathbb{Z}_K : \mathbb{Z}[\beta]]$. The containment $\Lambda \subseteq \mathbb{Z}_K$ and the equality of indices then forces $\Lambda = \mathbb{Z}_K$.

   Note that we get for free the fact that Λ is stable under multiplication, which was by no means obvious.

8. *Compute explicitly the decomposition of 2, 3, and 7 in* K*.*

   Since $\mathbb{Z}[\alpha]$ is maximal at 2, we may compute the decomposition of 2 by factoring f mod 2. Clearly, neither 0 nor 1 is a root of f mod 2, so f is either irreducible or the product of 2 irreducible factors of degree 2. The only polynomials of degree 2 over $\mathbb{F}_2$ are x^2, x^2+1, x^2+x and x^2+x+1, and clearly only the last one is irreducible. Therefore, if f mod 2 were reducible, it would be $(x^2+x+1)^2$, but this is impossible. There are two ways to see why : we can use the fact that we are in characteristic 2 to compute that $(x^2+x+1)^2 = x^{2^2}+x^2+1^2 \not\equiv f \bmod 2$, or we can say that if f were not squarefree mod 2, then its discriminant would be 0 mod 2, which we know is not the case. Either way, we deduce that f remains irreducible mod 2, so that 2 is inert in K. In symbols, $2\mathbb{Z}_K = \mathfrak{p}_2$ is a prime of norm 2^4.

We have already seen that 3 is totally ramified in K. To be more precise, as $\mathbb{Z}[\alpha]$ is maximal at 3 it is legitimate to factor f mod 3; we find $f \equiv x^4 \bmod 3$, whence $3\mathbb{Z}_K = \mathfrak{p}_3^4$, where $\mathfrak{p}_3 = (3, \alpha)$ is a prime of norm 3^1.

Finally, we may **not** determine the decomposition of 7 by factoring f mod 7, because the order $\mathbb{Z}[\alpha]$ is not maximal at 7. However, since $7^2 \nmid \operatorname{disc} \chi(\beta)$, the order $\mathbb{Z}[\beta]$ is maximal at 7, so we are saved. We have $\chi(\beta) \equiv x^4 - 3x^2 + 2 \equiv (x^2-1)(x^2-2) \equiv (x-1)(x+1)(x-3)(x+3) \bmod 7$, so

$$7\mathbb{Z}_K = (7, \beta-1)(7, \beta+1)(7, \beta-3)(7, \beta+3)$$

is totally split.

9. *What is the rank of the unit group of K ? Can you spot a nontrivial (i.e. not ± 1) unit of K ?*

   Since the signature of K is $(0, 2)$, the rank of $\mathbb{Z}_K^\times$ is $0 + 2 - 1 = 1$.

   The fact that the constant term of $\chi(\gamma)$ is 1 indicates that $N(\gamma) = (-1)^4 \cdot 1$, so γ is a unit of norm $+1$.

10. *What can you say about the roots of unity contained in K ? How could you use this to test whether the unit you spotted in the previous question if a root of unity ?*

    If we had a p-th root of 1 in K where p is an odd prime, then K would contain the p-th cyclotomic field, whose degree is $p-1$ and which is ramified at p; therefore the degree of K would be a multiple of $(p-1)$ and p would ramify in K. This excludes all the possibilities, except $p = 3$.

    If we did have a 3rd root of 1, say ζ, in K, then we would also have $-\zeta \in K$, which is a 6th root of 1. According to proposition 5.2.9, we would then have $N(\mathfrak{p}) \equiv 1 \bmod 6$ for every prime $\mathfrak{p}$ not above 2 or 3, but this is not contradictory with the decomposition of 7 in K.

    So, all we can say is that the roots of unity in K are either the 6th roots of unity, or just ± 1. In any case, a root of unity $u \in K$ would satisfy $u^6 = 1$, so we could determine whether γ is a root of unity by checking if $\gamma^6 = 1$. (In fact, we could save ourselves some effort by checking if $\gamma^2 \pm \gamma + 1 = 0$ — thank you, cyclotomic polynomials !).

    In fact, it turns out that K does contain the 6th roots of unity, that γ is not a root of unity, and that γ is in fact a fundamental unit of K, as luck would have it. However, I really do not think this can be proved without massive help from a computer.