PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 124, Number 6, June 1996

NORMSETS AND DETERMINATION OF UNIQUE FACTORIZATION IN RINGS OF ALGEBRAIC INTEGERS

JIM COYKENDALL

(Communicated by William W. Adams)

ABSTRACT. The image of the norm map from R to T (two rings of algebraic integers) is a multiplicative monoid S. We present conditions under which R is a UFD if and only if S has unique factorization into irreducible elements. From this we derive a bound for checking if R is a UFD.

1. INTRODUCTION

In this paper $F \supseteq K$ will denote finite extensions of $\mathbf{Q}$, the rational numbers, with rings of integers R and T respectively. We will also make the assumption that T is a *unique factorization domain* (UFD). It is well-known that the norm function, N_K^F, from F to K maps R into a multiplicative submonoid S of T. Such monoids may or may not have unique factorization. If F is Galois over K we prove:

Theorem. *R is a UFD if and only if the monoid S has unique factorization.*

In fact more is true; if the "small" elements (where "small" is determined by the Minkowski bound of the extension) of S have unique factorization, then R is a UFD (see Lemmas 3.2 and 3.3 and Theorem 3.4) in an even more general setting than the Galois case.

From this we derive a bound for determining if R is a UFD, and we give an explicit computation for the quadratic case.

2. DETERMINATION OF UNIQUE FACTORIZATION

We begin this section with a couple of definitions:

Definition 2.1. Let $S \subseteq T$ be a multiplicatively closed subset containing 1, and let $a \in S$. Then we say that a is *irreducible* if whenever $a = bc$ with $b, c \in S$, then either b or c is a unit.

Received by the editors March 21, 1994 and, in revised form, December 29, 1994.
1991 *Mathematics Subject Classification.* Primary 11R04, 11R29; Secondary 11Y40.
Key words and phrases. Normsets, Galois (extension), norm factorization field (extension), Minkowski bound.

Definition 2.2. We call S a *unique factorization monoid* (UFM) if every non-zero element of S can be written uniquely as a finite product of irreducible elements.

Remark 2.3. If we let S be the set of all values of the norm function $N_K^F|_R{:}R \to T$, then the multiplicativity of the norm function and the fact that R and T are Noetherian (hence atomic) show that any element of S has finite factorization into irreducibles. We will call such an S a normset (with respect to T) of R.

Definition 2.4. Consider a prime element p of T which factors as $\mathcal{P}_1^{e_1}...\mathcal{P}_k^{e_k}$ in R with corresponding degrees $\{f_1, ..., f_k\}$. We say that p is a *principal gcd prime* if both of the following conditions hold:

1. $\mathcal{P}_i$ is non-principal for some i.
2. f=gcd$\{f_1, ..., f_k\}$ is an element of $\{f_1, ..., f_k\}$ and at least one of the primes of degree f is principal.

Definition 2.5. We say that F is a *norm factorization field extension of* K (NFF) if either R is a UFD or there is a prime p of T satisfying 1. but not 2. of Definition 2.4.

Remark 2.6. Some examples of these fields are:

1. All finite Galois fields over K.
2. Any field F over K that is itself a UFD.
3. All non-UFD, non-Galois fields F over K that have a non-zero density for the set of primes in K that have a unique degree 1 factor that is in a specified ideal class of F.

Theorem 2.7. *Let R be the ring of algebraic integers of F, a norm factorization field extension of K. Let S be the normset of R with respect to T (a UFD). Then S is a UFM$\Longrightarrow R$ is a UFD and if F is Galois over K, then S is a UFM$\Longleftrightarrow R$ is a UFD.*

To prove this theorem we will use the following lemma.

Lemma 2.8. *In the Galois case if R is a UFD, then $\pi \in R$ is a (non-zero) prime$\Longleftrightarrow$*
$N_K^F(\pi)$ is irreducible.

Proof of Lemma 2.8. ($\Leftarrow$) π not prime means $\pi = ab$ with a, b non-units; therefore $N_K^F(\pi) = N_K^F(a)N_K^F(b)$.

($\Rightarrow$) Assume that $N_K^F(\pi) = N_K^F(a)N_K^F(b)$ with neither norm on the right equal to a unit. Choose $N_K^F(a)$ to be irreducible. Then by the other implication, a is prime. Therefore as $N_K^F(a) = \sigma_1(a)\dots\sigma_n(a)$, where σ_i are the elements of $G = \mathrm{Gal}(F/K)$, this implies that $a|\sigma_i(\pi)$ for some i. Therefore a conjugate of a divides π. So as π and a are both primes, they must be conjugates (up to a unit). Therefore $N_K^F(b)$ is a unit, and we are done by contradiction.

Proof of Theorem 2.7. ($\Longleftarrow$) Let R be a UFD. Given any $a \in R$ we clearly have an irreducible factorization in S given by $N_K^F(a) = \prod_{i=1}^k N_K^F(\pi_i)$, where $a = \prod_{i=1}^k \pi_i$ is the prime factorization of a. It remains to show that this factorization in the normset is unique.

Let $N_K^F(a) = \prod_{i=1}^r N_K^F(\xi_i)$ be another such factorization. First of all note that for this new factorization to be irreducible, ξ_i must be prime for all i. Also note that $N_K^F(a)$ has $k|G|$ prime factors in R, so therefore $k = r$.

As R is a UFD, this implies that for all $1 \leq i \leq k$ there are $1 \leq j, l \leq k$ such that $\pi_i = \sigma_l(\xi_j)$ (up to a unit). In particular this means that $N_K^F(\pi_i) = N_K^F(\xi_j)$ (up to a unit in S). If we divide out this pair of norms and continue inductively, we can see that the factorizations are the same up to a unit as $k=r$. So this direction is established.

($\Longrightarrow$) Assume that R is not a UFD. As F is an NFF, there is a prime element of T (say p) that factors as $\mathcal{P}_1^{e_1} ... \mathcal{P}_k^{e_k}$ with respective degrees $\{f_1, ..., f_k\}$. For the first case we will assume that $f = \gcd(\{f_1, ..., f_k\})$ is not in the set of degrees. If for every distinct α in the monoid J generated by $\{f_1, ..., f_k\}$ there is a principal ideal of norm p^α, then pick f_i to be a minimal element of the set of degrees and pick f_j such that f_i does not divide f_j. Now we consider the following two factorizations in the normset:

$$(p^{f_i})^{f_j} = (p^{f_j})^{f_i}.$$

The minimality of f_i and the fact that f_i does not divide f_j show that S is not a UFM.

On the other hand, assume that there is an $\alpha \in J$ such that there is no principal ideal of norm p^α (we assume this α to be the minimal element of J with this property). As $\alpha \in J$, then there is an ideal I of norm p^α and therefore there are elements of S of the form $p^\alpha r$ such that $(r, p) = 1$. Obtaining such elements can be done by multiplying I by an ideal in the class of I^{-1} that is relatively prime to (p) (see [2]). So among all elements of norm $p^\alpha r$ we pick the one with minimal r (here "minimal" means with respect to the lengths of prime factorizations of r in T). Consider the following equation in S:

$$(p^\alpha r)^n = (p^n)^\alpha r^n; \quad n = [F : K].$$

To see that this leads to non-unique factorization, it suffices to show that $p^\alpha r$ is irreducible. Assume that $p^\alpha r = p^{\alpha_1} r_1 p^{\alpha_2} r_2$. By the minimality of r, both α_1, α_2 are positive. But then the minimality of α implies that there are principal ideals of norm p^{α_1} and p^{α_2}, therefore there is a principal ideal of norm p^α, a contradiction. This establishes the first case.

For the second case, assume that f is in the set of degrees. This implies that all primes of degree f are non-principal. Let $\mathcal{P}$ be such a prime and consider the ideal $\mathcal{Q}$ in the inverse class of $\mathcal{P}$ such that $\mathcal{Q}$ is relatively prime to (p) as in the previous proof. Let r be the order of $\mathcal{P}$ in the class group and consider the ideal equation

$$(\mathcal{P}\mathcal{Q})^r = (\mathcal{P}^r)(\mathcal{Q}^r).$$

Taking norms one obtains the equation:

$$(p^f n)^r = (p^{fr})(n^r).$$

But by assumption, there is no way to reconcile these factorizations as f is minimal, and there are no principal ideals of norm p^f. This concludes the proof of the theorem as S is not a UFM.

Remark 2.9. In the non-Galois case one would not expect that UFD implies UFM in general. For example one might have an extension of degree 5 and an (unramified) prime p that splits into two (principal) primes of degrees 2 and 3. In this case we have the two distinct irreducible factorizations in the normset

$$(p^2)^3 = (p^3)^2.$$

So the normset fails to have unique factorization. However, we can extend this example to obtain a partial converse to Theorem 2.7.

Theorem 2.10. *Let F be an NFF of degree 2,3,4, or 6 over K with ring of integers R and normset S. Then S is a UFM$\Longleftrightarrow R$ is a UFD.*

Proof. It suffices to show that in the above cases, R is a UFD$\Longrightarrow S$ is a UFM. As R is a UFD, the normset S is generated by the norms of all the prime ideals of R. As T is a UFD, it suffices to show that all powers of primes factor uniquely in S. Here we recall that if the degree of the extension is n, then $n = e_1f_1 + \cdots + e_kf_k$, where the e's are the ramification indices and the f's are the degrees in the decomposition of a prime.

Consider the following partitions of the above numbers:

$4 = 2 + 2$,

$6 = 2 + 2 + 2 = 3 + 3 = 2 + 4$.

These are the only "non-trivial" partitions (i.e. do not involve a "1" or a single term) possible for the above numbers. Note that if we have a trivial partition, then either we have a unique prime over p (in which case the powers of p factor uniquely in the normset) or we have a prime of degree one over p (in which case there is an element of norm p and we have unique factorization of powers of p). Checking the above partitions on a case-by-case basis, we can see that in all cases we have a single generator of the powers of p in the normset and therefore unique factorization of the powers of p. This establishes the theorem.

Remark 2.11. We note here that what makes Theorem 2.10 work is the fact that 1,2,3,4,6 are the unique positive integers that have the property that any partition contains a minimal element dividing the rest. For any other positive integer, we can construct a theoretical counterexample to the analog of Theorem 2.10 as per Remark 2.9.

Example 2.12. Consider $\mathbf{Z}[\sqrt{-14}]$. In this ring of integers the normset is generated by the binary quadratic form $x^2 + 14y^2$. Notice that this form represents 14 but does not represent either 2 or 7. Therefore as $(4)(49)=(14)^2$ are two distinct irreducible factorizations in the normset, the normset is not a UFM and this ring cannot be a UFD.

We would like to conclude this section with a question. In Definitions 2.4 and 2.5 we imposed the loosest condition that we could to obtain a class of fields such that UFM$\Longrightarrow$UFD. It appears that this class of fields is much larger than the Galois fields, but by how much? It seems plausable to expect that all non-Galois fields are indeed NFFs, but we have yet to prove it.

3. A Minkowski bound for determination of unique factorization

In Example 2.12 we showed that the ring of integers $\mathbf{Z}[\sqrt{-14}]$ was not a UFD. This was relatively easy because it is easy to see that the normset of this ring does not have unique factorization. Generally speaking, we have a well-defined method for determining when a ring of integers is not a UFD, but we would also like to know when we have done "enough checking". In other words, we would like to find a finitely-terminating process to determine if we have a UFM (and hence a UFD). We start this section with a famous theorem due to Minkowski. (Note: in this section all normsets will be with respect to $\mathbf{Z}$ and all extensions will be Galois so that we have the equivalence of UFD and UFM.)

Theorem 3.1 (Minkowski Bound). *Let R be a ring of algebraic integers; then in every ideal class of R there is an (integral) ideal of norm less than or equal to $M=\frac{n!}{n^n}(\frac{4}{\pi})^r\sqrt{|d_K|}$ with n being the degree of the extension, r one-half the number of complex embeddings, and d_K the discriminant of the field. This M is called the Minkowski bound for R.*

Minkowski's theorem tells us that R is a UFD if and only if all ideals of norm less than or equal to M are principal, and it is easy to see that R is a UFD if and only if all prime ideals of norm less than or equal to M are principal. This gives us enough information to be able to construct a finite algorithm testing the normset (and hence the ring) for unique factorization given a complete knowledge of a "small piece" of the normset.

Let R be the ring of integers of a finite, Galois extension of $\mathbf{Q}$, and $\mathcal{P}$ a prime of R lying over p with degree f_p. We also denote the normset of R as S. We define:

$$P_1 = \{p \in \mathbf{Z}, p : prime | p^{f_p} \leq M\}.$$

Here we give an easy lemma:

Lemma 3.2. *R is a UFD $\Longleftrightarrow \forall\ p{\in}P_1\ \pm p^{f_p} \in S$.*

Proof. ($\Longrightarrow$) is trivial.

($\Longleftarrow$) Let $\mathcal{P}$ be an ideal of norm $p^{f_p} \leq M$. As $p \in P_1$, we have $\pm p^{f_p} \in S$. In other words, there is an element in R of norm $\pm p^{f_p}$. Therefore this element must generate a conjugate of $\mathcal{P}$. So $\mathcal{P}$ is principal, and we are done.

To use Lemma 3.2 we need an algorithm that determines the relative degree f_p for every prime (in fact, we need only concern ourselves with primes that are less than or equal to the Minkowski bound). The following lemma gives us an algorithm that accomplishes this end.

Lemma 3.3. *Let $N(\overline{X})$ be the norm form for R (with respect to some $\mathbf{Z}$ basis) and $\overline{N}(\overline{X})$ its reduction* $\bmod p$. *Then $f_p = \inf\{f_\lambda | \overline{N}(\overline{X}) = p^{f_\lambda} u$ has a solution* $\bmod p^n$ *with u a unit$\}$.*

Proof. First note that as $N(\overline{X})$ is an n degree form in n variables (where n is the degree of the field extension) with coefficients in $\mathbf{Z}$, then reduction of the norm form makes sense modulo any p. Also we note that as the n-tuple $(p, p, \ldots, p)$ is a solution to $\overline{N}(\overline{X}) = 0 \mod p^n$, the set in Lemma 3.3 is non-empty. Let $\mathcal{P} \supseteq (p)$ and let the norm of $\mathcal{P}$ be p^{f_p}. We denote the infimum of the set in Lemma 3.3 by h.

Assume that we have a $\overline{\gamma}$ such that $\overline{N}(\overline{\gamma}) = 0 \mod p^h$. Then $\overline{\gamma}$ has a pullback $\gamma \in R$ such that the norm of γ is $p^h k$. So $\gamma \in \sigma(\mathcal{P})$ for some σ in $\mathrm{Gal}(F/\mathbf{Q})$. Therefore $N(\mathcal{P})|N(\gamma)$, so $f_p \leq h$. Now as h is the infimum of the above set, we merely have to show that f_p is contained in the set to obtain the desired equality. But note that as $N(\mathcal{P}) = p^{f_p}$, then there is an element of R with norm $p^{f_p}k$ with $(p, k) = 1$ (obtained by finding a relatively prime ideal in the inverse class of $\mathcal{P}$ as in the proof of Theorem 2.7). So we have a solution to $\overline{N}(\overline{X}) \mod p^{f_p}$, and hence the lemma is established.

Combining the previous two lemmas gives our desired algorithm. To determine if R is a UFD, first we consider the primes in $\mathbf{Z}$ that are less than or equal to

the Minkowski bound. For each of these primes we find the relative degree as per Lemma 3.3 (and eliminate each prime such that $p^{f_p} > M$). With this remaining set of primes we merely check to see if $\pm p^{f_p} \in S$. If all are represented in the normset, then R is a UFD and if any are missing, then R is not a UFD. As a result of this we can easily strengthen Theorem 2.7 to say:

Theorem 3.4. *R (as above) is a UFD $\iff$ S is a UFM and if R is not a UFD, then there is an integer $n \leq M$, the Minkowski bound, such that n is involved in a non-unique factorization in the normset.*

Remark 3.5. In fact if R is the ring of integers of an NFF that is not a UFD, then its normset, S, is not a UFM (Theorem 2.7). It is easy to see by the above methods that again there is an $n \leq M$ that is involved in a non-unique factorization in S.

Example 3.6. Let $F = \mathbf{Q}[\sqrt{d}]$ be a quadratic field (here we make the standard assumption that d is a square-free integer) with R the ring of integers of F. In this example we will write down what has to be done to discover if a given quadratic field has unique factorization. It is well known that the ring of integers of this field is $\mathbf{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \mod(4)$ and $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \mod(4)$. In the first case the discriminant is $4d$ and in the second it is d. In this case the condition of Lemma 3.3 translates to $f_p = 1$ if and only if either p divides the discriminant or if $(\frac{d}{p})=1$, where ( ) is the Legendre symbol. So here the algorithm for finding f_p is easily stated (and implemented). In this case one checks all primes less than or equal to the Minkowski bound, and every prime fitting the criteria above (f_p=1) must appear (up to a sign) in the normset.

Acknowledgments

I would like to express my gratitude to Dr. Robert Perlis, Dr. Steve Chase, and Dr. Moss Sweedler for answering several questions that helped me shorten and improve my results and for helping me to "polish my style". Thanks also to Dr. Shankar Sen for always being there to listen and help. Also I would like to thank Dr. David Dobbs for his unending support.

References

1. J. W. S. Cassels and A. Frohlich, *Algebraic Number Theory*, Academic Press, London, 1967.
2. H. Cohn, *Advanced Number Theory*, Dover Publications, New York, 1980. MR **82b:**12001
3. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer-Verlag/Polish Scientific Publishers, Warszawa, 1990. MR **91h:**11107

Department of Mathematics, Cornell University, Ithaca, New York 14853
E-mail address: jimbob@math.cornell.edu
Current address: Department of Mathematics, Lehigh University, Bethlehem, Pennsylvania 18015
E-mail address: jbc4@lehigh.edu