PROPERTIES OF THE NORMSET RELATING TO THE CLASS GROUP

Jim Coykendall

Abstract: In [4] the normset and its multiplicative structure was studied. In that paper it was shown that under certain conditions (including Galois) that a normset has unique factorization if and only if its corresponding ring of integers has unique factorization. In this paper we shall examine some of the properties of a normset and describe what it says about the class group of the corresponding ring of integers.

1. INTRODUCTION AND NOTATION

Following the notation of [4] K$\subseteq$F will denote algebraic number fields with rings of integers T$\subseteq$R. We also assume that T is a PID and that F is Galois over K. The normset of R (with respect to T) will be denoted by S and the norm function by N. With these assumptions, it is known that R is a UFD if and only if one has unique factorization in S in the obvious way (this property is denoted by "S is a UFM"). In the case that S is not a UFM then R is not a UFD and has some nontrivial class group. Classically the order of the class group is said to be a "measure of by how much R misses being a UFD." One would therefore like to know how much information about the class group can be distilled from the normset e.g. what invariants do the class group and the normset have in common. In this paper, we examine a property of the normset that we call saturation and show that this property implies a specific structure for the class group. In the quadratic case we will see that the saturation property i s equivalent to the class group being $\mathbf{Z}_2$-elementary abelian. Examples are constructed to show that in the general case this nice equivalence does not exist; and in the last section we show how these properties relate to the so called "property N" from the work of Bumby and Dade [1] and [2]. Briefly, an irreducible integer α has property N if the existence of another integer β with N(α)=N(β) implies that β is also irreducible.

2. SATURATION IN THE NORMSET

We begin this section with two alternative definitions of saturation and we note that the Galois assumption is not needed here:

DEFINITION 2.1: We say that S is *strongly saturated* if the existence of $\alpha, \beta \in$R with $\frac{\mathrm{N}(\alpha)}{\mathrm{N}(\beta)} \in$ T implies the

existence of $\gamma \in$R such that N(γ)=N(β) and $\gamma|\alpha$.

For the next definition, we first define an equivalence notation on the normset by saying that N(α) is equivalent to N(β) if N(α)=uN(β) with u some unit of R. By abuse of notation we will also refer to this as S. When distinctions are needed, they will be made clear.

DEFINITION 2.2: We say that S is *saturated* if the existence of $r, s \in$S with $\frac{r}{s} \in$T implies that $\frac{r}{s} \in$S.

Saturation, the property that we will devote most of our attention to, is an abstract property of a normset. Strong saturation, however, is intrinsically dependent upon the ring. It is clear that strong saturation implies saturation, and we shall see later that in the imaginary quadratic case that these two notions are equivalent. In the more general case, however, these two notions are distinct and we shall see an example (2.4) of this that also demonstrates why we must declare all norms equivalent up to a unit.

EXAMPLE 2.3: Consider the field $\mathbf{Q}(\sqrt{-53})$. In this case the ring of integers of this field is $\mathbf{Z}[\sqrt{-53}]$, and the normset is generated by the binary quadratic form F(x,y)=x^2+53y^2. Note that F(1,1)=54 and F(3,0)=9 and so both 54 and 9 are in the normset. It is easy to see that the quotient 6 is not in the normset. So this is an example of a non-saturated normset. Saturated examples are easier since any UFD must have a saturated normset (this is a simple exercise for quadratic fields, we shall see it proven shortly).

EXAMPLE 2.4: Consider the ring of integers $\mathbf{Z}[\sqrt{34}]$. The normset of this ring is generated by the binary quadratic form G(x,y)=x^2-34y^2. This ring also has fundamental unit with a positive norm and class number 2 ([3] for example). we note here that G(5,1)=-9 and G(3,0)=9. Therefore this ring is not strongly saturated as there is no element of norm -1, but it turns out that when we declare all norms equivalent up to a unit this normset is saturated. We will see the proof of this later.

REMARK 2.5: As we shall see, the saturation measures the difference between the class group and the group of ideal classes containing an ideal with a principal norm (we use this terminology to mean that there is an ideal in the given class that has the same norm as some principal ideal), which we shall see is completely dependent on the Galois action on the class group. In the quadratic case, the more unsaturated the normset is, the further the class group is from being $\mathbf{Z}_2 \oplus ... \oplus \mathbf{Z}_2$. In the imaginary quadratic case, saturation measures how much the class group and the group of genera differ.

3. THE NORM GROUP

In this section we develop the concept of the norm group as a tool to get a better look at the properties of saturation. We use the terminology norm group because the group can be defined by an equivalence relation on the normset. Here we choose a different (but equivalent) method of definition.

DEFINITION 3.1: We define the extended normset to be:

$$S^{ext}=\{a \in T | (a) = N(I); I : \text{integral ideal of } R\} \text{ (modulo unit equivalence)}$$

We note here that $S \subseteq S^{ext}$ and that equality holds if and only if R is a UFD.

DEFINITION 3.2: We define the normgroup to be $G_1=N_1(R)=N_1(F)=Q(S^{ext})/Q(S)$, where Q( ) denotes the quotient group of the monoid.

REMARK 3.3: N_1 is a functor from the category of finite extensions of $\mathbf{Q}$ (resp. their rings of integers) to the category of finite abelian groups. Note that the Galois assumption is unnecessary. To see how N_1 acts on morphisms, consider $f:R_1 \longrightarrow R_2$. As R_1 and R_2 are rings of integers, then f is nontrivial if and only if it is injective. So we can consider R_1 to be isomorphic to a subring of R_2 and F_1 to be isomorphic to a subfield of F_2 where F_1 is the quotient field of R_1 and F_2 is the quotient field of R_2. So the induced map on the norm groups is $a \longmapsto (f(a))^n$ with $n=[F_2:F_1]$, and f the map of rings (or fields). That this is a functorial correspondence follows from the basic properties of the norm map. The fact that G_1 is finite will follow from the next theorem.

THEOREM 3.4: There is an exact sequence:

$$1 \longrightarrow H \xrightarrow{\iota} CL(R) \xrightarrow{\phi} G_1 \longrightarrow 1$$

where $H=\{[I] \in CL(R) | [I] \text{ contains an ideal with a principal norm}\}$.

Proof: Define $\phi: CL(R) \longrightarrow G_1$ by $\phi([I])=[N(I)]$. This map is well-defined because if $[I]=[J]$ then there is an $a \in F$ such that $aI=J$, therefore $N(a)N(I)=N(J)$ so in G_1, $[N(I)]=[N(J)]$. Clearly this is a homomorphism due to the multiplicativity of the norm. To see that ϕ is surjective, note that $[a] \in G_1$ means that $a=N(I)$ for some invertible ideal of R so [I] is our desired preimage.

It remains to show that $H=\ker(\phi)$. Let $[J] \in H$, which implies that there is an $I \in [J]$ such that $N(I)=N(b)$ for some $b \in R$. So $\phi([J])=\phi([I])=[N(I)]=[N(b)]=1$. The other containment is similar.

THEOREM 3.5: S is saturated if and only if H=1.

Proof: ($\Longrightarrow$) Assume $H \neq 1$. then there is a nontrivial ideal class [I] containing an ideal with a principal norm. Say that $I \in [I]$ has norm $n \in S$. Pick a split prime $\mathcal{P}$ in $[I^{-1}]$ with norm p (see [3] or [8]). Note that $\mathcal{P}I$

is a principal ideal so there is an element of norm pn. But there is no element of norm p by the choice of $\mathcal{P}$. So S is not saturated and we have established the first direction.

($\Longleftarrow$) If S is not saturated, then there are elements ξ and η of norms n and m respectively such that n=km with k$\in$T. So clearly there is a principal ideal of norm k, we merely need to show the existence of a nonprincipal ideal of norm k. Let the ideal factorizations of ξ and η be given by $\xi = \mathcal{P}_1...\mathcal{P}_r$ and $\eta = \mathcal{Q}_1...\mathcal{Q}_s$. As N($\eta$)|N($\xi$), $s < r$ and each $\mathcal{Q}_i$ is a conjugate of $\mathcal{P}_i$ (without loss of generality). So if we consider the ideal $\mathcal{P}_{s+1}...\mathcal{P}_r$, this is an integral ideal of norm k, but it cannot be principal, for then there would be an element in R of norm k which is a contradiction. So H$\neq$1. This establishes Theorem 3.5.

Now that we have completed these preliminary theorems, we turn our attention to what this saturation property says about the structure of the class group.

THEOREM 3.6: Let F over K be Galois with [F:K]=n=$p_1^{a_1}...p_k^{a_k}$ and assume that the normset of R is saturated, then CL(R) is the product of its Sylow subgroups CL(R)$\cong$S(p_1)$\times...\times$S(p_k) with each S(p_i)$\cong\mathbf{Z}_{p_i^{b_1}} \times \mathbf{Z}_{p_i^{b_2}} \times ... \times \mathbf{Z}_{p_i^{b_t}}$ with $b_j \leq a_i$ for all $1 \leq j \leq t$.

Proof: Assume that CL(R) is not of the above form. In the first case, assume that there is an ideal class [J] of order r such that r has a nontrivial factor that is prime to n. By taking the appropriate power of this element we obtain an ideal class [I] of order s such that (s,n)=1. In this case [I^n] contains a principal norm (since an extension of degree n has a normset containing all perfect n^{th} powers). But as (s,n)=1, [I^n] is certainly not principal. So H$\neq$1 and hence the normset S is not saturated.

In the second case, assume that there is an element of CL(R) of order r with p_i^a||r with $a > a_i$. By the same argument as above, we can then find an element [I] of order p_i^a. Since $a > a_i$, [I^n] contains a principal norm but is certainly not principal. So again H$\neq$1 and so S is not saturated.

In general the converse to Theorem 3.6 is not true. In certain cases, however, one can obtain some partial converses. We start out with a theorem for quadratic extensions. This theorem shows that in the quadratic case the full converse to Theorem 3.6 is true and that saturation means that the class group is 2-elementary abelian (or trivial).

THEOREM 3.7: In a quadratic extension, the following conditions are equivalent.

1. S is saturated.
2. H=1.
3. CL(R)$\cong G_1$.
4. CL(R)$\cong\mathbf{Z}_2 \oplus ...\oplus\mathbf{Z}_2$ (or 1).

Proof: We have already seen that 1.$\Longleftrightarrow$2.$\Longleftrightarrow$3.$\Longrightarrow$4. So it suffices to show that 4.$\Longrightarrow$1. Assume that CL(R)$\cong(\mathbf{Z}_2)^n$ with $n \geq 0$. Let ξ,$\eta\in$R such that N(η)|N(ξ). Let the prime ideal factorization of ξ and η be $\xi=\mathcal{P}_1...\mathcal{P}_k$, $\eta=\mathcal{Q}_1...\mathcal{Q}_r$. We note that as each ideal class is its own inverse and conjugation determines inverse classes in quadratic fields, we have that the Galois group acts trivially on the group of ideal classes. As N(η)|N(ξ), this means that $k \geq r$, and (without loss of generality) $\mathcal{Q}_i$ is a conjugate of $\mathcal{P}_i$ for all $i \leq r$. So we conclude that $\widetilde{\eta}=\mathcal{P}_1...\mathcal{P}_r$ is still principal. Therefore $\widetilde{\eta}|\xi$ and the quotient has the appropriate norm. So S is saturated. This completes the proof.

What makes the above proof work is the fact that in quadratic extensions, conjugation determines the inverse class, and if the class group is $\mathbf{Z}_2 \oplus ... \oplus \mathbf{Z}_2$ then every class is its own inverse. We will now obtain a partial converse to a special case of Theorem 3.6 and then we shall present an example showing that a full converse is unobtainable. But we will begin with a theorem that illustrates what is going on.

THEOREM 3.8: The normset S is saturated if and only if the Galois group acts trivially on the class group.

Proof: ($\Longleftarrow$) Same as the proof for Theorem 3.7.

($\Longrightarrow$) Assume that G does not act trivially on the Galois group. Let $\mathcal{P}$ be a split prime lying over the prime p of T in an ideal class that is not fixed by $\sigma \in$G, and let [F:K]=n. Clearly there is an element in the normset of norm p^n. It suffices to show (by Theorem 3.5) that there is a nonprincipal ideal of norm p^n. First we note that the saturation of S implies (by Theorem 3.6) that $\mathcal{P}^n$ is principal. Consider the ideal $\mathcal{P}^{n-1}\sigma(\mathcal{P})$. The norm of this is clearly p^n, but it is nonprincipal because $[\sigma(\mathcal{P})]$ is not equal to $[\mathcal{P}]$. This establishes the theorem.

THEOREM 3.9: [F:K]=p: prime and CL(R)$\cong\mathbf{Z}_p$ then S is saturated.

Proof: First we note that by Theorem 3.6, saturation implies p-elementary abelian so the cyclic group of order p is a good place to start looking for a converse. We note that Gal(F/K)$\cong\mathbf{Z}_p$. Since any element of the Galois group induces an automorphism of the class group, the Galois group can be thought of as contained in Aut(CL(R))$\cong$Aut($\mathbf{Z}_p$)$\cong\mathbf{Z}_{p-1}$. But as p and p-1 are relatively prime, we see that any action of the Galois group has to be trivial. Therefore by Lemma 3.8 we conclude that S is saturated.

REMARK 3.10: The above theorem utilizes the fact that $\mathbf{Z}_p$ has order that is relatively prime to its automorphism group. However it is an easy exercise (e.g.[7]) to see that the order of the automorphism group of $(\mathbf{Z}_p)^r$ is $(p^r-1)(p^r-p)...(p^r-p^{r-1})$, so in particular is divisible by p. This distressing fact is an obstruction to improving the converse of Theorem 3.6. We will soon see an example of why this is so.

REMARK 3.11: We note here that in the imaginary quadratic case, or in the real quadratic case with negative fundamental unit, or in any case where the equation N(a)=uN(b) with a,b in R and u a unit of R implies the existence of an element of R with N(x)=u (for example $\mathbf{Z}[\sqrt{15}]$ has positive fundamental unit, but satisfies this property), saturation implies strong saturation. To see this note that the proof that trivial Galois action implies saturation actually constructs an element of the appropriate norm up to a unit, and if the above condition is satisfied, then we have strong saturation.

EXAMPLE 3.12: Let F be a cubic, Galois extension of $\mathbf{Q}$ with class group $\mathbf{Z}_3 \oplus \mathbf{Z}_3$. Denote the Galois group by $\{e, \sigma, \sigma^2\}$. We denote the various ideal classes by ordered pairs from $\mathbf{Z}_3$, and we assume that the Galois group acts on the classes as per the following table:

Class [I]	σ ([I])	σ^2([I])	σ^3([I])
(0,0)	(0,0)	(0,0)	(0,0)
(1,0)	(0,1)	(2,2)	(1,0)
(2,0)	(0,2)	(1,1)	(2,0)
(0,1)	(2,2)	(1,0)	(0,1)
(0,2)	(1,1)	(2,0)	(0,2)
(1,1)	(2,0)	(0,2)	(1,1)
(2,2)	(1,0)	(0,1)	(2,2)
(1,2)	(1,2)	(1,2)	(1,2)
(2,1)	(2,1)	(2,1)	(2,1)

Note that the Galois group is indeed cyclic of order 3, and that any ideal class times all of its conjugates is principal. Now using our knowledge of the Galois action on this group, we pick three split primes $\mathcal{P}$ in the class (1,0), $\mathcal{Q}$ in the class (0,2), and $\mathcal{R}$ in the class (2,1). Note that $\mathcal{PQR}$ is principal. Now we consider the ideal $\sigma^2(\mathcal{P})\sigma(\mathcal{Q})$ which is also principal. It is easy to see that the $N(\sigma^2(\mathcal{P})\sigma(\mathcal{Q}))|N(\mathcal{PQR})$ and this quotient is $N(\mathcal{R})$, but as $\mathcal{R}$ is a split prime, there is no element of norm $N(\mathcal{R})$. So we see that the normset is not saturated. A concrete example of this field can be found in [6]. The cyclic, cubic field of conductor 1267=7.181 and class number 9 has the property that the group of "ambiguous classes", that is the classes fixed by the Galois action has order 3. This example is also discussed in some detail in [5].

4. ON THE WORK OF BUMBY AND DADE

In [1] and [2] Bumby and Dade extensively studied the problem of when irreducible integers are com-

pletely determined by their norms. They say that an irreducible integer α has property N if the existence of another integer β such that N(α)=N(β) implies that β is also irreducible. I will list a couple of the results.

THEOREM 4.1: Let K be a quadratic number field with class group H. Then K satifies property N if and only if
(a) H has exponent 2
or (b) H is odd
or (c) K is real with positive fundamental unit and the 2-Sylow subgroup of the narrow class group is cyclic.

Proof: See [1].

THEOREM 4.2: If the Galois group acts trivally on the class group, then property N holds.

Proof: See [2].

One can see that there is a definite connection between property N and the saturation properties of the normset in the quadratic case. In general, this paper and the work of Bumby and Dade point to a divergence of these properties for non-quadratic extensions. We will conclude with a theorem that illuminates the connections.

THEOREM 4.3: Saturation (and therefore strong saturation) implies property N.

Proof: Saturation is equivalent to trivial Galois action. Apply Theorem 4.2.

ACKNOWLEDGEMENTS

The author would like to express his gratitude to the referee for helpful suggestions on the improvement of this paper.

REFERENCES

[1]. R.T. Bumby, *Irreducible integers in Galois extensions*, Pacific J. Math.**22** no. 2 (1967), 221-229.
[2]. R.T Bumby and E.C. Dade, *Remark on a problem of Niven and Zuckerman*, Pacific J. Math.**22** no. 1 (1967), 15-18.
[3]. H. Cohn, *Advanced Number Theory*, Dover Publications, New York, 1980.

[4]. J. Coykendall, *Normsets and determination of unique factorization in rings of algebraic integers*, Proc. American Math. Soc., to appear.

[5]. G. Gras, *Sur les l-classes d'ideaux dans les extensions cycliques relatives de degre premier l*, Annales de l'Institut Fourier **23**, 3 (1973), 1-48 and **23**, 4 (1973), 1-43.

[6] M. Gras, *Methodes et algorithmes pour le calcul numerique du nombre de classes et des unites des extensions cubiques cycliques de* **Q**, J. Reine Angew. Math. **277** (1975), 89-116.

[7]. M. Hall, *The theory of groups*, Chelsea Publishing Co., New York, 1976.

[8]. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer-Verlag/Polish Scientific Publishers, Warszawa, 1990.