Norms and elasticities in rings of algebraic integers

Jim Coykendall & Jared Kettinger
Clemson University

July 2024

Elasticity of the Normset

Classically, the Dedekind-Hasse norm has been used to explore properties of rings of algebraic integers. We recall that if $K \subseteq F$ is an extension of algebraic number fields and $\alpha \in F$ then

$$N_K^F(\alpha) = \prod_\sigma \sigma(\alpha) \in K$$

with the product taken over distinct embeddings into $\mathbb{C}$.

Elasticity of the Normset

Classically, the Dedekind-Hasse norm has been used to explore properties of rings of algebraic integers. We recall that if $K \subseteq F$ is an extension of algebraic number fields and $\alpha \in F$ then

$$N_K^F(\alpha) = \prod_\sigma \sigma(\alpha) \in K$$

with the product taken over distinct embeddings into $\mathbb{C}$.
If this norm function is restricted to the ring of integers of F (T) then the image forms a subset of the ring of integers of K (R). What is more, the norm is a monoid homomorphism with the properties that $N_K^F(\alpha) = 0$ if and only if $\alpha = 0$ and if $\alpha \in T$ then α is a unit in T if and only if $N_K^F(\alpha)$ is a unit in R.

Here are some older theorems on the interplay between a ring of integers and its set of norms.

Here are some older theorems on the interplay between a ring of integers and its set of norms.

Theorem (AB, PAMS 1996)

If F/K is Galois and R, the ring of integers of F is a UFD, then the ring of integers of F is a UFD if and only if its set of integral norms is a UFM.

Here are some older theorems on the interplay between a ring of integers and its set of norms.

Theorem (AB, PAMS 1996)

If F/K is Galois and R, the ring of integers of F is a UFD, then the ring of integers of F is a UFD if and only if its set of integral norms is a UFM.

Over the next few years various aspects of these ideas were studied. For example, it was shown that the set of integral norms is saturated (that is, contains quotient of norms up to a unit if they are integral) if and only if the Galois group acts trivially on the class group. Special attention was focused on the quadratic case.

Here are some older theorems on the interplay between a ring of integers and its set of norms.

Theorem (AB, PAMS 1996)

If F/K is Galois and R, the ring of integers of F is a UFD, then the ring of integers of F is a UFD if and only if its set of integral norms is a UFM.

Over the next few years various aspects of these ideas were studied. For example, it was shown that the set of integral norms is saturated (that is, contains quotient of norms up to a unit if they are integral) if and only if the Galois group acts trivially on the class group. Special attention was focused on the quadratic case. The previous theorem was generalized in

Here are some older theorems on the interplay between a ring of integers and its set of norms.

Theorem (AB, PAMS 1996)

If F/K is Galois and R, the ring of integers of F is a UFD, then the ring of integers of F is a UFD if and only if its set of integral norms is a UFM.

Over the next few years various aspects of these ideas were studied. For example, it was shown that the set of integral norms is saturated (that is, contains quotient of norms up to a unit if they are integral) if and only if the Galois group acts trivially on the class group. Special attention was focused on the quadratic case. The previous theorem was generalized in

Theorem (AB, J. Number Theory 1998)

If F/K is Galois and R, the ring of integers of F is a UFD, then the ring of integers of F is an HFD if and only if the elasticity in the set of norms is 1.

In 1999, we have the following.

In 1999, we have the following.

Theorem (AB, Comm. Alg.)

Let $F/\mathbb{Q}$ be an algebraic number field with ring of integers $\overline{R}$. If $R \subseteq \overline{R}$ is an order with the HFD property, then $\overline{R}$ is an HFD. If, in addition, F is Galois over $\mathbb{Q}$ of odd degree, then $\overline{R}$ is a UFD.

In 1999, we have the following.

Theorem (AB, Comm. Alg.)

Let $F/\mathbb{Q}$ be an algebraic number field with ring of integers $\overline{R}$. If $R \subseteq \overline{R}$ is an order with the HFD property, then $\overline{R}$ is an HFD. If, in addition, F is Galois over $\mathbb{Q}$ of odd degree, then $\overline{R}$ is a UFD.

Here is some more recent work. Much of the next couple of slides can also be found (in very different language) in a couple of recent papers:

In 1999, we have the following.

Theorem (AB, Comm. Alg.)

Let $F/\mathbb{Q}$ be an algebraic number field with ring of integers $\overline{R}$. If $R \subseteq \overline{R}$ is an order with the HFD property, then $\overline{R}$ is an HFD. If, in addition, F is Galois over $\mathbb{Q}$ of odd degree, then $\overline{R}$ is a UFD.

Here is some more recent work. Much of the next couple of slides can also be found (in very different language) in a couple of recent papers:

- *On monoids of weighted zero-sum sequences and applications to norm monoids in Galois number fields and binary quadratic forms* by A. Geroldinger, F. Halter-Koch, and Q. Zhong
- *Monoids of sequences over finite abelian groups defined via zero-sums with respect to a given set of weights and applications to factorizations of norms of algebraic integers* S. Boukheche, K. Merito, O. Ordaz, and W. Schmid

We will highlight some of the interesting results in our context and show where this leads.

We will highlight some of the interesting results in our context and show where this leads.

It is well-known (Valenza-Narkiewicz) that if R is a ring of algebraic integers then its elasticity is given by $\rho(R) = \frac{D(\mathrm{Cl}(R))}{2}$ if the class number is greater than 1 (here $D(\mathrm{Cl}(R))$ denotes the Davenport constant of the class group). It was also shown in one of the earlier papers referenced before that if S is the set of integral norms of R then in the Galois case $\rho(R) \geq \rho(S)$ ("Galois" is important here as UFD rings of integers can have very high elasticities in their set of norms if Galois is not enforced and the degree of the extension exceeds 6). Additionally, it was shown in some cases (e.g. trivial Galois action on the class group) that we can have $\rho(R) = \rho(S)$ (this observation, coupled with Carlitz' theorem highlights why the HFD property is preserved in the set of norms).

We will highlight some of the interesting results in our context and show where this leads.

It is well-known (Valenza-Narkiewicz) that if R is a ring of algebraic integers then its elasticity is given by $\rho(R) = \frac{D(\mathrm{Cl}(R))}{2}$ if the class number is greater than 1 (here $D(\mathrm{Cl}(R))$ denotes the Davenport constant of the class group). It was also shown in one of the earlier papers referenced before that if S is the set of integral norms of R then in the Galois case $\rho(R) \geq \rho(S)$ ("Galois" is important here as UFD rings of integers can have very high elasticities in their set of norms if Galois is not enforced and the degree of the extension exceeds 6). Additionally, it was shown in some cases (e.g. trivial Galois action on the class group) that we can have $\rho(R) = \rho(S)$ (this observation, coupled with Carlitz' theorem highlights why the HFD property is preserved in the set of norms).

This raises the obvious question that asks what is the relationship between the elasticity of the set of norms and the elasticity of the parent ring of integers.

Definition

Let A be an abelian group and G a subgroup of $Aut(A)$. We define $D_G(A) := n$ to be the length of the longest 0 sequence such that if $\{\phi_i\}$ is a collection of automorphisms from G, with

$$\sum_{i=1}^{n} \phi_i(a_i) = 0$$

then the sequence has no proper subsequence.

Definition

Let A be an abelian group and G a subgroup of $Aut(A)$. We define $D_G(A) := n$ to be the length of the longest 0 sequence such that if $\{\phi_i\}$ is a collection of automorphisms from G, with

$$\sum_{i=1}^{n} \phi_i(a_i) = 0$$

then the sequence has no proper subsequence.

This generalized Davenport constant is clearly bounded above by the "ordinary" Davenport constant and in a couple of cases (e.g. if the automorphism group consists of the identity and the automorphism that inverts each element and A is the direct product of a group of odd order and a $2-$elementary abelian group).

Theorem

Let R be a Galois ring of integers with class group A. If S is the set of norms of R and $|A| > 1$ then $\rho(S) = \dfrac{D_G(A)}{2}$.

Theorem

Let R be a Galois ring of integers with class group A. If S is the set of norms of R and $|A| > 1$ then $\rho(S) = \dfrac{D_G(A)}{2}$.

The next result is a corollary to this theorem and is also a nice way to see some of the results alluded to earlier in this talk.

Theorem

Let R be a Galois ring of integers with class group A. If S is the set of norms of R and $|A| > 1$ then $\rho(S) = \frac{D_G(A)}{2}$.

The next result is a corollary to this theorem and is also a nice way to see some of the results alluded to earlier in this talk.

Corollary

If R is a quadratic ring of integers and A is the direct product of a group of odd order and a $2-$elementary abelian group, then $\rho(R) = \rho(S)$.

Focusing on the Galois case, we note that Galois groups place some restrictions on class groups that are possible. For example, we noted earlier that if $F/\mathbb{Q}$ is of odd degree then R is an HFD if and only R is a UFD (since class number 2 is problematic for odd Galois group). This can be extended further.

Focusing on the Galois case, we note that Galois groups place some restrictions on class groups that are possible. For example, we noted earlier that if $F/\mathbb{Q}$ is of odd degree then R is an HFD if and only R is a UFD (since class number 2 is problematic for odd Galois group). This can be extended further.

Theorem

Let $p < 23$ be a prime and $a \in \mathbb{Z}$ be not divisible by the p^{th} power of any prime. If R is the ring of integers of the splitting field of $x^p - a$, then R is an HFD if and only if R is a UFD.

Focusing on the Galois case, we note that Galois groups place some restrictions on class groups that are possible. For example, we noted earlier that if $F/\mathbb{Q}$ is of odd degree then R is an HFD if and only R is a UFD (since class number 2 is problematic for odd Galois group). This can be extended further.

Theorem

Let $p < 23$ be a prime and $a \in \mathbb{Z}$ be not divisible by the p^{th} power of any prime. If R is the ring of integers of the splitting field of $x^p - a$, then R is an HFD if and only if R is a UFD.

The proof of this hinges on the fact that $\mathbb{Z}[\zeta_p]$ (where ζ_p is a primitive p^{th} root of unity) is a UFD if (and only if) $p < 23$.

To see how the Galois group forces conditions on the class group, we consider a stronger Galois action.

To see how the Galois group forces conditions on the class group, we consider a stronger Galois action.

Definition

Let G be a finite group and A an abelian group with A' some specified subgroup of A. We say that G is a Galois action on A if

1. $e_G \cdot a = a$ *for all* $a \in A$.

To see how the Galois group forces conditions on the class group, we consider a stronger Galois action.

Definition

Let G be a finite group and A an abelian group with A' some specified subgroup of A. We say that G is a Galois action on A if

1. $e_G \cdot a = a$ *for all* $a \in A$.
2. $g_1 \cdot (g_2 \cdot a) = g_1 g_2 \cdot a$ *for all* $g_1, g_2 \in G$, $a \in A$.

To see how the Galois group forces conditions on the class group, we consider a stronger Galois action.

Definition

Let G be a finite group and A an abelian group with A' some specified subgroup of A. We say that G is a Galois action on A if

1. $e_G \cdot a = a$ *for all* $a \in A$.
2. $g_1 \cdot (g_2 \cdot a) = g_1 g_2 \cdot a$ *for all* $g_1, g_2 \in G$, $a \in A$.
3. $g(a_1 a_2) = g(a_1)g(a_2)$ *for all* $g \in G, a_1, a_2 \in A$.

To see how the Galois group forces conditions on the class group, we consider a stronger Galois action.

Definition

Let G be a finite group and A an abelian group with A' some specified subgroup of A. We say that G is a Galois action on A if

1. $e_G \cdot a = a$ *for all* $a \in A$.
2. $g_1 \cdot (g_2 \cdot a) = g_1 g_2 \cdot a$ *for all* $g_1, g_2 \in G$, $a \in A$.
3. $g(a_1 a_2) = g(a_1) g(a_2)$ *for all* $g \in G, a_1, a_2 \in A$.
4. $\prod_{g \in G} g(a) \in A'$ *for all* $a \in A$.

In practice, A' is often e_A and the fourth "norm" condition is a translation of the fact that in extensions of $\mathbb{Z}$ (or a PID in general) then the norm of an ideal is principal.

In practice, A' is often e_A and the fourth "norm" condition is a translation of the fact that in extensions of $\mathbb{Z}$ (or a PID in general) then the norm of an ideal is principal.
It is also worth noting a couple of other useful facts.

In practice, A' is often e_A and the fourth "norm" condition is a translation of the fact that in extensions of $\mathbb{Z}$ (or a PID in general) then the norm of an ideal is principal.
It is also worth noting a couple of other useful facts.
The first is that the first three properties guarantee that $\prod_{g \in G} g(a)$ is fixed by every $x \in G$, so at the very most A' can be construed as the elements of A stabilized by all of G.

In practice, A' is often e_A and the fourth "norm" condition is a translation of the fact that in extensions of $\mathbb{Z}$ (or a PID in general) then the norm of an ideal is principal.
It is also worth noting a couple of other useful facts.
The first is that the first three properties guarantee that $\prod_{g \in G} g(a)$ is fixed by every $x \in G$, so at the very most A' can be construed as the elements of A stabilized by all of G.
The second is that for torsion class groups, it suffices to consider Galois actions on $p-$groups Sylow $p-$subgroups are always characteristic.

Here are a couple of conditions that arise using the interplay of Galois groups and class groups.

Here are a couple of conditions that arise using the interplay of Galois groups and class groups.

Theorem

Let F be a Galois extension of degree p^r with ring of integers R. If A is the class group of R and $S(q)$ is a nontrivial Sylow $q-$subgroup of A, then q is either equal to p or $q \equiv 1 mod(p)$.

Here are a couple of conditions that arise using the interplay of Galois groups and class groups.

Theorem

Let F be a Galois extension of degree p^r with ring of integers R. If A is the class group of R and $S(q)$ is a nontrivial Sylow $q-$subgroup of A, then q is either equal to p or $q \equiv 1 mod(p)$.

Note that this theorem illustrates why the quadratic case is so (nicely) deceptive. All quadratic extensions (in characteristic 0) are Galois and the previous highlights that "anything can happen."

Here is another theorem along these lines.

Here is another theorem along these lines.

Theorem

Let F be a cyclic extension of odd prime order p with ring of integers R. If A is the class group of R, then A cannot be cyclic of order p^n for any $n \geq 2$.

Here is another theorem along these lines.

Theorem

Let F be a cyclic extension of odd prime order p with ring of integers R. If A is the class group of R, then A cannot be cyclic of order p^n for any $n \geq 2$.

Example

For a cyclic extensions of order 3, there are examples with 3−elementary abelian class group, but of course no cyclic of order 9. There is, however, an example with class group $\mathbb{Z}_3 \times \mathbb{Z}_9$. If we write the elements of $\mathbb{Z}_3 \times \mathbb{Z}_9$ in the usual way, we have the following orbits under the Galois action of the automorphism that takes $(1,0)$ to $(1,3)$ and $(0,1)$ to $(2,4)$: $\{(0,0)\},\{(0,3)\},\{(0,6)\}$ and

$\{(1,0),(1,3),(1,6)\},\{(2,0),(2,6),(2,3)\},\{(0,1),(2,4),(1,4)\},$
$\{(1,1),(0,7),(2,1)\},\{(0,2),(1,8),(2,8)\},\{(1,2),(2,2),(0,5)\},$
$\{(0,4),(2,7),(1,7)\},\{(1,5),(2,5),(0,8)\}$

We can also take a given extension with Galois group G and use "small" localizations to create smaller class groups.

We can also take a given extension with Galois group G and use "small" localizations to create smaller class groups.

Theorem

Let R be a Dedekind domain with torsion class group A and group of automorphisms G. Suppose that $x \in R$ is a nonzero nonunit and

$$(x) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_k^{e_k}.$$

Then $Cl(R[\frac{1}{x}]) \cong A/G\langle [\mathfrak{P}_1], [\mathfrak{P}_2], \cdots, [\mathfrak{P}_k] \rangle$ (where $G < X >$ is the group generated by all automorphic images of the elements in X).

The previous theorem allows us to excise a minimal amount of A to produce (in many cases) a "large" homomorphic image of A. In the case of rings of algebraic integers, this localization is spiritually almost a ring of integers itself (in fact, it is the exact analog of rings of integers if the base ring of $\mathbb{Z}$ were to be replaced by $\mathbb{Z}[\frac{1}{x}]$ for some nonzero x).

The previous theorem allows us to excise a minimal amount of A to produce (in many cases) a "large" homomorphic image of A. In the case of rings of algebraic integers, this localization is spiritually almost a ring of integers itself (in fact, it is the exact analog of rings of integers if the base ring of $\mathbb{Z}$ were to be replaced by $\mathbb{Z}[\frac{1}{x}]$ for some nonzero x).

This theorem also (again) underscores how galactically misleading the quadratic case is; in this case, any homomorphic image can be obtained in a finite localization (in the quadratic case, any subgroup of the class group is stable with respect to the two automorphisms).

As a final remark, we note that it would be nice to determine if all Galois actions on class groups can be achieved. This might be quite hard if we are too restrictive (e.g. the status of the inverse Galois problem is still unknown), but more general constructions might save the day. We are currently considering this and other aspects.

Thank you all!!

Thank you all!!

Thanks, Scott and Marco!