QUADRATIC FORMS, THE GROTHENDIECK-WITT RING, TRANSFERS, NORMS, AND RESTRICTIONS

KYLE ORMSBY

Throughout these notes, let F denote a field of characteristic different from 2.

1. QUADRATIC FORMS

1.1. **The basics.** A *quadratic form* over F is a homogeneous degree 2 polynomial with coefficients in F. In general, these look like

$$f(x_1, \dots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j \in F[x_1, \dots, x_n].$$

Of course, $x_i x_j = x_j x_i$, and the coefficient of this term in the above expression is $a_{ij} + a_{ji}$. In order to render the coefficients symmetric, we may define $a'_{ij} = (a_{ij} + a_{ji})/2$ so that

$$f = \sum_{i,j=1}^{n} a'_{ij} x_i x_j$$

as well. In this fashion, f determines and is determined by a unique symmetric matrix $M_f = (a'_{ij})$.

Example 1.1. Suppose $f(x, y) = ax^2 + bxy + cy^2$. The associated matrix is

$$M_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

In the above example, it is easy to see that $f(x, y) = (x\ y) M_f \begin{pmatrix} x \\ y \end{pmatrix}$, and this behavior is generic. Writing x for the column vector associated with $(x_1, x_2, \dots, x_n)$, we have

$$f(x) = x^T M_f x$$

where $(\ )^T$ indicates transpose.

We define an *equivalence* of n-ary quadratic forms f and g to be a linear change of variables that turns g into f. In other words, f is equivalent to g when there exists an invertible matrix $A \in \mathrm{GL}_n(F)$ such that $f(x) = g(Ax)$. Since

$$g(Ax) = (Ax)^T M_g (Ax) = x^T (A^T M_g A) x,$$

we see that f and g are equivalent if and only if

$$M_f = A^T M_g A$$

for some $A \in \mathrm{GL}_n(F)$. As such, equivalence of forms is equivalent to *congruence* of the associated symmetric matrices.

Example 1.2. Let $f(x,y) = xy$ and let $h(x,y) = x^2 - y^2$. Substituting $x \mapsto x+y$, $y \mapsto x-y$, we see that

$$f(x+y, x-y) = (x+y)(x-y) = x^2 - y^2 = h(x,y),$$

so f and h are equivalent. We also have $M_f = \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}$, $M_h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and $M_h = A^T M_f A$ for $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Exercise 1.3. Prove that equivalence of forms is an equivalence relation.

We have already seen that the study of quadratic forms up to equivalence is the same as the study of symmetric matrices up to congruence. It will be beneficial to investigate two more equivalent structures that are slightly more abstract. The first of these is a *quadratic space* (V,q), which is an n-dimensional vector space V equipped with degree 2 homogeneous function $q : V \to F$. Here "degree 2 homogeneous" means that $q(ax) = a^2 q(x)$ for all $a \in F$ and $x \in V$. Such a function is called a *quadratic map* on V.

Exercise 1.4. Prove the following facts about quadratic spaces and quadratic forms:

(a) An n-ary quadratic form f determines a quadratic space (F^n, f) where (abusing notation) we think of f as a function $F^n \to F$ given by evaluating the polynomial f.
(b) A quadratic space (V,q) along with a choice of basis $e_1, \dots, e_n$ of V determines a symmetric matrix M_q with entries $(M_q)_{ii} = q(e_i)$ and $(M_q)_{ij} = \frac{1}{2}(q(e_i+e_j) - q(e_i) - q(e_j))$.
(c) Under this correspondence, an equivalence of quadratic forms corresponds to a linear isomorphism $A : V' \to V$ such that $q(Ax) = q'(x)$ for all $x \in V'$ (where (V,q) and (V',q') are quadratic spaces).

The final equivalent structure is that of a *symmetric bilinear form* $B : V \times V \to F$. Here V is an n-dimensional F-vector space and B is a bilinear map such that $B(v,w) = B(w,v)$ for all $v, w \in V$.

Exercise 1.5. Prove the following facts about quadratic spaces and symmetric bilinear forms:

(a) A bilinear form B on V determines a quadratic space (V,q) where $q(x) := B(x,x)$.
(b) A quadratic space (V,q) determines a bilinear form B on V via *polarization*:

$$B(v,w) = \frac{1}{2}(q(v+w) - q(v) - q(w)).$$

(c) The assignments in (a) and (b) are inverse to each other.
(d) Equivalence of quadratic forms corresponds to *isometry* of symmetric bilinear forms: if B, B' are symmetric bilinear forms on V, V', respectively, an isometry $(V,B) \to (V',B')$ is a linear isomorphism $A : V \to V'$ such that $B'(Av, Aw) = B(v,w)$ for all $v, w \in V$.

In summary, we have the following dictionary of concepts:

$$\left\{ \begin{array}{c} \text{quadratic forms} \\ \text{up to equivalence} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{symmetric matrices} \\ \text{up to congruence} \end{array} \right\}$$
$$\leftrightarrow \left\{ \begin{array}{c} \text{quadratic spaces} \\ \text{up to equivalence} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{symmetric bilinear forms} \\ \text{up to isometry} \end{array} \right\}.$$

The first two structures are nice because they are classical and concrete and lend themselves to manual computation. The final two structures are nice because they are coordinate-free and often permit more elegant proofs. We shall freely translate results between all four structures.

Proposition 1.6. Let B be a symmetric bilinear form on V with matrix M associated with an ordered basis $e_1, \ldots, e_n$ of V. Then the following statements are equivalent:

(a) M is an invertible matrix;
(b) the function $x \mapsto B(\ , x) : V \to V^*$ is an isomorphism;
(c) for $x \in V$, $B(x, y) = 0$ for all $y \in V$ if and only if $x = 0$.

We leave the proof as a moral exercise for the reader. If these conditions hold, we call (V, B) a *regular* symmetric bilinear form and call its associated quadratic form *nonsingular*.

For a subspace $W \subseteq V$ of a bilinear space (V, B), let

$$W^\perp := \{x \in V \mid B(x, W) = 0\}$$

denote the *orthogonal complement* of W. We call $V^\perp$ the *radical* of V. Note that B is regular if and only if $V^\perp = 0$, but proper subspaces of regular spaces need not be regular.

Another moral exercise (*hint*: use (b) of the previous proposition and the rank-nullity theorem):

Proposition 1.7. Let (V, B) be a regular bilinear space and $W \subseteq V$ a subspace of V. Then

(a) $\dim W + \dim W^\perp = \dim V$, and
(b) $(W^\perp)^\perp = W$.

1.2. **Diagonalization.** A quadratic form f is *diagonal* if it is of the form $\sum a_i x_i^2$, in which case its associated symmetic matrix is diagonal with entries $a_1, \ldots, a_n$. Our present goal is to show that every quadratic form is equivalent to a diagonal form. We warn the reader diagonal forms need not have the same a_i in order to be equivalent.

Let $F^\times := F \smallsetminus \{0\}$ denote the multiplicative group of units in F.

Definition 1.8. A quadratic form f over F *represents* $d \in F^\times$ if there exists $\lambda \in F^n$ such that $f(\lambda) = d$. Write $D_F(f) = D(f)$ for the set of values in $F^\times$ represented by f.

Exercise 1.9. Check that $D(f)$ only depends on the equivalence class of f.

If $a, d \in F^\times$, then $d \in D(f)$ if and only if $a^2 d \in D(f)$. As such, $D(f)$ is a union of cosets of $F^\times$ modulo squares in $F^\times$. We shall write $F^{\boxtimes} := \{x^2 \mid x \in F^\times\}$ for the group of squares in $F^\times$, and call $F^\times/F^{\boxtimes}$ the *group of square classes* of F. Note that $\mathbb{C}^\times/\mathbb{C}^{\boxtimes} = \{\mathbb{C}^{\boxtimes}\}$ since $\mathbb{C}^{\boxtimes} = \mathbb{C}^\times$. Also note that $\mathbb{R}^\times/\mathbb{R}^{\boxtimes} = \{\pm\mathbb{R}^{\boxtimes}\}$, where $\mathbb{R}^{\boxtimes} = \mathbb{R}_{>0}$. Finally, note that every finite field has group of square classes of order 2 since the squaring map is 2-to-1.

We now define a new operation on quadratic forms / symmetic matrices / bilinear spaces / quadratic spaces.

Definition 1.10. Let $f(x_1, \ldots, x_m), g(x_1, \ldots, x_n)$ denote quadratic forms over F with associated matrices M, N. Let $(V, q), (V', q')$ denote quadratic spaces with polarizations B, B', respectively. The following operations correspond to each other in our dictionary and are all called *orthogonal sum*:

(a) $f \oplus g$ is the $(m+n)$-ary quadratic form $f(x) + g(y) \in F[x, y]$;
(b) $M \oplus N$ is the block diagonal matrix $\begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix}$;
(c) $(V, q) \oplus (V', q')$ is the quadratic space $(V \oplus V', q \oplus q')$ where $V \oplus V'$ is the usual direct sum of vector spaces and $q \oplus q' : V \oplus V' \to F$ is the map $(v, v') \mapsto q(v) + q'(v')$;
(d) $(V, B) \oplus (V', B')$ is the bilinear space $(V \oplus V', B \oplus B')$ where $(B \oplus B')((x, y), (x', y')) = B(x, y) + B'(x', y')$.

Given $a \in F$, let $\langle a \rangle$ denote the quadratic form ax^2. Then $\langle a_1 \rangle \oplus \cdots \oplus \langle a_n \rangle$ is the diagonal quadratic form $a_1x_1^2 + \cdots + a_nx_n^2$. We make the notational convention

$$\langle a_1, \ldots, a_n \rangle := \langle a_1 \rangle \oplus \cdots \oplus \langle a_n \rangle,$$

which provides a compact notation for diagonal quadratic forms.

Lemma 1.11 (Representation Criterion)**.** For a bilinear space (V, B) and $d \in F^\times$, $d \in D(V, B)$ if and only if there is another bilinear space (V', B') and an isometry $V \cong \langle d \rangle \oplus V'$.

The representation criterion is essential for what follows, so we will go through its proof in detail.

Proof. If $V \cong \langle d \rangle \oplus V'$, then $d \in D(\langle d \rangle \oplus V')$ by evaluation at the vector $(1, 0'_V)$.

For the converse, we first reduce to the case where V is regular. Take a suspace W such that $V \cong V^\perp \oplus W$. Clearly $D(V) = D(W)$, and W is regular. Thus without loss of generality, we may assume V is regular.

By hypothesis, there is some $v \in V$ with $q(v) = d$ (where $q(v) = B(v, v)$ is the depolarization of B). The quadratic subspace $F\{v\}$ is equivalent to $\langle d \rangle$, and $F\{v\} \cap (F\{v\})^\perp = 0$. Since $\dim F\{v\} + \dim F\{v\}^\perp = \dim V$ by Proposition 1.7, we conclude that $V \cong \langle d \rangle \oplus F\{v\}^\perp$. □

Theorem 1.12. *If (V, B) is any bilinear space over F, then there exist $a_1, \ldots, a_n \in F$ such that $V \cong \langle a_1, \ldots, a_n \rangle$.*

Proof. If $D(V, B) = \varnothing$, then B is identically 0 and $V = \langle 0, \ldots, 0 \rangle$. If there exists $d \in D(V, B)$, then $V \cong \langle d \rangle \oplus V'$ for some (V', B'), and the proof proceeds by induction on $\dim V$. □

Exercise 1.13. Read the example on p.35 of Lam (ignoring the part about signatures and anisotropicity for the moment). Make sure you understand how to diagonalize a quadratic form via completion of squares. Review this sage documentation and make sure you can use sage to diagonalize a quadratic form via the command `rational_diagonal_form()`.

Proposition 1.14. If (V, B) is a (not necessarily regular) bilinear space and W is a regular subspace, then $V = W \oplus W^\perp$. Furthermore, if U is a subspace of V such that $V = W \oplus U$, then $U = W^\perp$.

Proof idea. Use the Gram-Schmidt process to prove the first statement. The second statement is relatively easy using the first. □

We conclude this subsection by briefly discussing the *determinant* of a nonsingular quadratic form f. This is defined to be $d(f) := \det(M_f) \cdot F^{\boxtimes} \in F^\times / F^{\boxtimes}$. Note that if f is equivalent to g, then $M_f = A^T M_g A$ for some invertible A, and hence

$$d(f) = \det(M_g) \det(A)^2 \cdot F^{\boxtimes} = d(g),$$

so $d(f)$ is an invariant of the equivalence class of f. Interestingly, d turns orthogonal sum into product: $d(f \oplus g) = d(f)d(g)$. Furthermore, $d(\langle a_1, \ldots, a_n \rangle) = a_1 \cdots a_n \cdot F^{\boxtimes}$.

1.3. **Witt decomposition and cancellation.** So far, these notes have followed Lam's presentation quite closely, but at this point I am going to skip the section on hyperbolic spaces. (Someone will lecture on this content next week.) The important definition is that $\mathbb{H} := \langle 1, -1 \rangle$ is called the *hyperbolic plane*, and a space equivalent to an orthogonal sum of hyperbolic planes is called a *hyperbolic space*. A vector $v \in (V, B)$ is called *isotropic* if $B(v, v) = 0$. A bilinear space is called *isotropic* if it contains a nonzero isotropic vecotr; it is called *totally*

FIGURE 1. Ernst Witt, 1911–1991. Emmy Noether's Ph.D. student and one of the most prominent algebraists of his generation. His devotion to the Nazi party casts a dark shadow over his legacy.

isotropic if all nonzero vectors are isotropic (in which case B is identically 0). A space which is not isotropic is called *anisotropic*. It's not hard to prove that a 2-dimensional quadratic space is regular and isotropic if and only if it is equivalent to $\mathbb{H}$.

This brings us to Witt's decomposition theorem:

Theorem 1.15 (Witt decomposition)**.** *Any quadratic space (V, q) splits into an orthogonal sum $(V_t, q_t) \oplus (V_h, q_h) \oplus (V_a, q_a)$ where V_t is totally isotropic, V_h is hyperbolic (or zero), and V_a is anisotropic. The isometry types of V_t, V_h, V_a are all uniquely determined.*

Proof idea. For existence, first take V_0 such that $V = V^\perp \oplus V_0$. Then $V_t = V^\perp$ is totally isotropic and V_0 is regular. It turns out that you can split hyperbolic planes off of isotropic spaces, and we do this inductively until V_0 is anisotropic. Uniqueness will follow from the forthcoming Witt cancellation theorem. □

Theorem 1.16 (Witt cancellation)**.** *If q, q', q'' are arbitrary quadratic forms, then $q \oplus q' \cong q \oplus q''$ if and only if $q' \cong q''$. (Thus it is permissible to "cancel" the summand q from the first isometry.)*

Exercise 1.17. Read the proof on pp.12-15 of Lam.

1.4. **Tensor products of quadratic spaces.** We have already seen how to take sums of quadratic spaces via the orthogonal sum operation. We now turn to products, which will be accomplished with tensor products. We first define the tensor product of two F-vector spaces.

Let V, W denote F-vector spaces. Let $F(V \times W)$ denote the F-vector space with basis $V \times W$ (so elements of $F(V \times W)$ are finite F-linear combinations of ordered pairs $(v, w) \in V \times W$). Define an equivalence relation $\sim$ on $F(V \times W)$ such that for all $v, v' \in V$, $w, w' \in W$, and $a \in F$,

(i) $(v, w) \sim (v, w)$,
(ii) $(v, w) + (v', w) \sim (v + v', w)$ and $(v, w) + (v, w') \sim (v, w + w')$, and
(iii) $a(v, w) \sim (av, w) \sim (v, aw)$.

Definition 1.18. The *tensor product* of V and W is

$$V \otimes W := F(V \times W)/\sim .$$

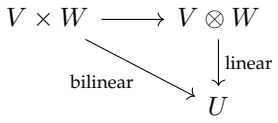
The equivalence class of (v, w) in $V \otimes W$ is denoted $v \otimes w$.

The classes $v \otimes w$ are called *simple tensors*; generic elements of $V \otimes W$ are linear combinations of simple tensors.

Exercise 1.19. Suppose V has basis $v_1, \ldots, v_m$ and W has basis $w_1, \ldots, w_n$. Prove that $V \otimes W$ has basis $\{v_i \otimes w_j \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$. In particular, $\dim V \otimes W = \dim V \cdot \dim W$.

The job of tensor products is to turn bilinear algebra into linear algebra, as exhibited by the following proposition.

Proposition 1.20. For F-vectors spaces V, W, let $V \times W \to V \otimes W$ be the map $(v, w) \mapsto v \otimes w$. For each F-vector space U, there is a bijective correspondence between bilinear maps $V \times W \to U$ and linear transformations $V \otimes W \to U$ making the diagram



commute.

Proof idea. The relations encoded by $\sim$ clearly make a composite $V \times W \to V \otimes W \xrightarrow{\text{linear}} U$ bilinear. Given a bilinear map $B : V \times W \to U$, we would like to define $V \times W \to U$ by $v \otimes w \mapsto B(v, w)$. Well-definition follows from bilinearity of B. Now check that these assignments are inverse to each other. □

Exercise 1.21. Show that there are natural isomorphisms $U \otimes (V \otimes W) \cong (U \otimes V) \otimes W$ and $\tau : V \otimes W \cong W \otimes V$. (We call the second isomorphism the *twist*.) Check that $\tau \circ \tau = \mathrm{id}$.

By Proposition 1.20, our bilinear forms $B : V \times V \to F$ are the same thing as linear maps $B : V \otimes V \to F$, and we will freely use either perspective. For instance, given bilinear spaces $(V, B), (W, B')$, we can define $B \otimes B' : (V \otimes W) \otimes (V \otimes W) \to F$ by re-associating the domain as $(V \otimes V) \otimes (W \otimes W)$, performing B and B' on each factor, respectively, and then multiplying the result. On simple tensors, this looks like

$$(B \otimes B')((v_1 \otimes w_1) \otimes (v_2 \otimes w_2)) = B(v_1 \otimes v_2) \cdot B(w_1 \otimes w_2).$$

This is the tensor (or *Kronecker*) product of B and B'. If B and B' have de-polarization q and q', respectively, we have $(q \otimes q')(v \otimes w) = q(v) \cdot q(w)$.

Exercise 1.22. Prove that the tensor product satisfies commutative, associative, and distributive laws:

(a) $q \otimes q' \cong q' \otimes q$,
(b) $q \otimes (q' \otimes q'') \cong (q \otimes q') \otimes q''$, and
(c) $q \otimes (q' \oplus q'') \cong (q \otimes q') \oplus (q \otimes q'')$.

Note that the distributive law along with the easy computation $\langle a\rangle \otimes \langle b\rangle \cong \langle ab\rangle$ imply that on diagonal forms,

$$\langle a_1, \dots, a_m\rangle \otimes \langle b_1, \dots, b_n\rangle \cong \langle a_1b_1, a_1b_2, \dots, a_1b_n, \dots, a_ib_j, \dots, a_mb_n\rangle.$$

From now on, when r is a nonnegative integer and f is a quadratic form, we will write $r \cdot f$ for the r-fold orthogonal sum of f with itself.

Proposition 1.23. If q is any regular quadratic form, then $q \otimes \mathbb{H} \cong (\dim q) \cdot \mathbb{H}$.

Proof. By Theorem 1.12, we may write $q \cong \langle a_1, \dots, a_n\rangle$ for some $a_i \in F$, and in fact all $a_i \in F^\times$ since q is regular (and thus has no totally isotropic summand). Then

$$q \otimes \mathbb{H} \cong \langle a_1\rangle \otimes \mathbb{H} \oplus \cdots \oplus \langle a_n\rangle \otimes \mathbb{H},$$

so it suffices to show that $\langle a\rangle \otimes \mathbb{H} \cong \mathbb{H}$ for any $a \in F^\times$. We have $\langle a\rangle \otimes \mathbb{H} \cong \langle a, -a\rangle$. You will finish the proof in the following exercise. □

Exercise 1.24. Prove that for all $a \in F^\times$, $\langle a, -a\rangle \cong \langle 1, -1\rangle = \mathbb{H}$.

2. The Witt and Grothendieck-Witt rings

From now on, if not mentioned, we will assume that all quadratic forms/spaces are nonsingular/regular.

2.1. **Definitions and basic properties.** Let $M(F)$ denote the set of isometry classes of (nonsingular) quadratic forms over F. The binary operations $\oplus$ and $\otimes$ define the structure of a commutative semiring on $M(F)$. (A semiring is like a ring, but without mandating additive inverses. You are already very familiar with the semiring $\mathbb{N}$ of natural numbers.) By the Witt cancellation theorem, $M(F)$ satisfies additive cancellation, but it does not have additive inverses (dimension is additive and takes values in $\mathbb{N}$).

To remedy this situation, we appeal to the *Grothendieck construction*. Let M be a commutative cancellation monoid under addition. Define $\sim$ on $M \times M$ by

$$(x, y) \sim (x', y') \text{ if and only if } x + y' = x' + y \in M.$$

The cancellation law implies that $\sim$ is an equivalence relation on $M \times M$. The *Grothendieck group* of M is $\mathrm{Groth}(M) := (M \times M)/\sim$ with addition induced by

$$(x, y) + (x', y') = (x + x', y + y').$$

This addition is well defined, and the classes of (x, y) and (y, x) are additive inverses of each other. Thus $\mathrm{Groth}(M)$ is a group. Furthermore, $i : M \to \mathrm{Groth}(M)$ defined by $i(x) = (x, 0)$ is an injection making M a sub-monoid of $\mathrm{Groth}(M)$. Note that $-i(y) = (0, y)$, so we may think of the pair (x, y) as the "formal difference" of x and y.

Proposition 2.1. There is a bijective correspondence between monoid homomorphisms from M to an Abelian group A and group homomorphisms $\mathrm{Groth}(M) \to A$ making the diagram

$$\begin{array}{ccc} M & \longrightarrow & \mathrm{Groth}(M) \\ & \searrow & \downarrow \\ & & A \end{array}$$

commute.

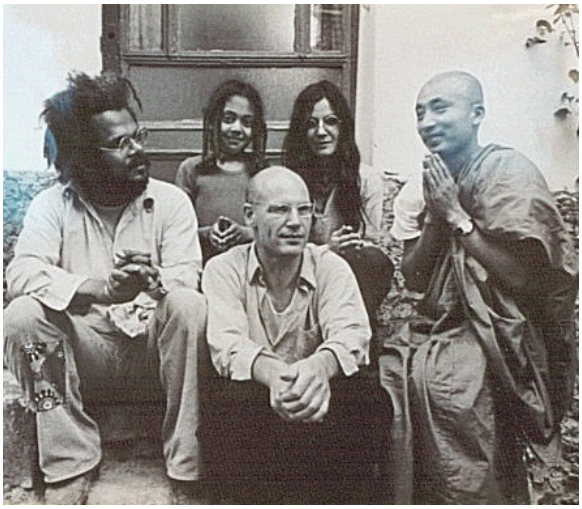


FIGURE 2. Alexander Grothendieck (center), 1928–2014. Creator of modern algebraic geometry. Also a radical pacifist and famous recluse. Not a Nazi.

The proof is a moral exercise. Finally, if M has a (commutative) multiplication making it a semiring, then the multiplication

$$(x, y)(x', y') = (xx' + yy', yx' + xy')$$

induces a (commutative) multiplication on $\mathrm{Groth}(M)$ that makes it into a (commutative) ring.

Definition 2.2. The *Grothendieck-Witt ring* of F is $\mathrm{GW}(F) := \mathrm{Groth}(M(F))$.

Note that every element of $\mathrm{GW}(F)$ has a representative of the form $q - q'$ where q, q' are (isometry classes of) nonsingular quadratic forms. Since $M(F) \subseteq \mathrm{GW}(F)$, the statements $q = q' \in \mathrm{GW}(F)$ and $q \cong q'$ are synonymous.

The dimension map $\dim : M(F) \to \mathbb{Z}$ is a semiring homomorphism and thus extends uniquely (by Proposition 2.1) to a ring homomorphism $\dim : \mathrm{GW}(F) \to \mathbb{Z}$ given by $\dim(q - q') = \dim(q) - \dim(q')$. Let $\mathrm{GI}(F)$ denote the kernel of $\dim$; we call $\mathrm{GI}(F)$ the *fundamental ideal* of $\mathrm{GW}(F)$. Since $\dim$ is surjective, $\mathrm{GW}(F)/\mathrm{GI}(F) \cong \mathbb{Z}$.

Another important subset of $\mathrm{GW}(F)$ is $\mathbb{Z} \cdot \mathbb{H}$, the integer multiples of the hyperbolic plane. By Proposition 1.23, $\mathbb{Z} \cdot \mathbb{H} = (\mathbb{H})$ is an ideal in $\mathrm{GW}(F)$.

Definition 2.3. The quotient ring $\mathrm{W}(F) := \mathrm{GW}(F)/\mathbb{Z} \cdot \mathbb{H}$ is called the *Witt ring* of F.

The Witt and Grothendieck-Witt rings are both "functorial in field extensions." By this, we mean that if $F \subseteq E$ is an extension of fields (*i.e.* F is a subfield of E), then there is a natural map $\mathrm{res}^E_F : \mathrm{GW}(F) \to \mathrm{GW}(E)$ such that

(i) $\mathrm{res}^F_F = \mathrm{id}$, and
(ii) for field extensions $F \subseteq E \subseteq L$, $\mathrm{res}^L_E \circ \mathrm{res}^E_F = \mathrm{res}^L_F$.

The map res_E^F is called *restriction*[1] and is given by extension of scalars: an F-quadratic form $f \in F[x_1, \ldots, x_n]$ is simply viewed as an element of $E[x_1, \ldots, x_n]$.

Exercise 2.4. Describe res_F^E on symmetric matrices, quadratic spaces, and bilinear spaces. In the latter two cases, you should use the concept of extension of scalars on a vector space: $V \mapsto E \otimes V$.

Witt defined $\mathrm{W}(F)$ in 1937 and observed that it had the following properties (see Lam p.29 for a proof).

Proposition 2.5. (a) The elements of $\mathrm{W}(F)$ are in bijective correspondence with the isometry classes of *anisotropic* quadratic forms.
(b) Two forms represent the same element of $\mathrm{W}(F)$ if and only if their anisotropic parts are isometric: $q = q' \in \mathrm{W}(F)$ if and only if $q_a \cong q'_a$.
(c) If $\dim q = \dim q'$, then $q = q' \in \mathrm{W}(F)$ if and only if $q \cong q'$.

Contemplation of the following diagram will result in (1) a definition of the fundamental ideal $\mathrm{I}(F) \subseteq \mathrm{W}(F)$, (2) a definition of the mod 2 rank homomorphism $\dim_0$, (3) a proof that $\mathrm{GI}(F) \cong \mathrm{I}(F)$, and (4) a proof that $\mathrm{W}(F)/\mathrm{I}(F) \cong \mathbb{Z}/2\mathbb{Z}$:

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & 0 & \longrightarrow & \mathbb{Z}\cdot\mathbb{H} & \longrightarrow & 2\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{GI}(F) & \longrightarrow & \mathrm{GW}(F) & \xrightarrow{\dim} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{I}(F) & \longrightarrow & \mathrm{W}(F) & \xrightarrow{\dim_0} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & & .
\end{array}$$

2.2. **More on square classes.** We have seen that the determinant induces a monoid homomorphism $d : M(F) \to F^\times/F^{\boxtimes}$ (where the monoid structures are $\oplus$ and $\cdot$, respectively). As such, we get a homomorphism of Abelian groups $d : \mathrm{GW}(F) \to F^\times/F^{\boxtimes}$ by setting $d(q - q') = d(q)/d(q') = d(q)d(q')$ (since $aF^{\boxtimes} = a^{-1}F^{\boxtimes}$). Since $d(\mathbb{H}) = -F^{\boxtimes}$, the homomorphism d does not factor through $\mathrm{W}(F)$. Let's fix that.

Define the *signed determinant* of a nonsingular n-dimensional form q by

$$d_\pm(q) = (-1)^{n(n-1)/2} d(q) \in F^\times/F^{\boxtimes}.$$

Then $d_\pm(\mathbb{H}) = F^{\boxtimes}$ (as we would like), but $d_\pm$ is no longer a monoid homomorphism! To remedy this, define

$$Q(F) := \mathbb{Z}/2\mathbb{Z} \times F^\times/F^{\boxtimes}$$

as a set and introduce the novel binary operation

$$(e, d) \cdot (e', d') = (e + e', (-1)^{ee'} dd').$$

[1] *Extension* would be a more natural name for this map, but we are headed towards Mackey and Tambara functors for which (for group-theoretic reasons) this type of map is called restriction.

This operation is commutative and associative with identity $(0, F^{\boxtimes})$. The inverse of (e, d) is $(e, (-1)^e d)$. Furthermore, the inclusion $d \mapsto (0, d)$ identifies $F^\times/F^{\boxtimes}$ as an index 2 subgroup of $Q(F)$. In general, $Q(F)$ is a *nonsplit extension* of $F^\times/F^{\boxtimes}$ by $\mathbb{Z}/2\mathbb{Z}$.

Proposition 2.6. The function $(\dim_0, d_\pm) : M(F) \to Q(F)$ is a monoid homomorphism extending to a group homomorphism $\mathrm{GW}(F) \to Q(F)$ which induces a group isomorphism $\mathrm{W}(F)/\mathrm{I}^2(F) \cong Q(F)$.

Proof sketch. The first statement is a rote calculation. Also, $(\dim_0, d_\pm)$ is surjective since $\langle a\rangle$ is sent to $(1, aF^{\boxtimes})$ and $\langle 1, -a\rangle$ is sent to $(0, aF^{\boxtimes})$. Since $\mathbb{H}$ is sent to $(0, (-1)d(\mathbb{H})) = (0, F^{\boxtimes})$, we get an iduced map $\mathrm{W}(F) \to Q(F)$. It turns out that $\mathrm{I}(F)$ is additively generated by binary forms $\langle 1, a\rangle$, so $\mathrm{I}^2(F)$ is additively generated by four-dimensional forms $\langle 1, a\rangle \otimes \langle 1, b\rangle = \langle 1, a, b, ab\rangle$. Now compute

$$(\dim_0, d_\pm)(\langle 1, a, b, ab\rangle) = (0, (-1)^0 a \cdot b \cdot abF^{\boxtimes}) = (0, F^{\boxtimes}).$$

Thus $(\dim_0, d_\pm)$ induces a surjection $\mathrm{W}(F)/\mathrm{I}^2(F) \to Q(F)$. Finally, construct an inverse $Q(F) \to \mathrm{W}(F)/\mathrm{I}^2(F)$ by sending $(0, aF^{\boxtimes})$ to $\langle 1, -a\rangle + \mathrm{I}^2(F)$ and $(1, aF^{\boxtimes})$ to $\langle a\rangle + \mathrm{I}^2(F)$. Now check that g is a homomomorphism and two-sided inverse to f. □

Corollary 2.7. The ideal $\mathrm{I}^2(F)$ consists of classes of even-dimensional forms q for which $d(q) = (-1)^{n(n-1)/2}$ (where $n = \dim q$).

Corollary 2.8. Restriction of the above isomorphism results in an isomorphism $\mathrm{I}(F)/\mathrm{I}^2(F) \cong F^\times/F^{\boxtimes}$.

The above corollary is the first nontrivial instance of the famed *Milnor conjecture*, which says that $K_n^M(F)/(2) \cong \mathrm{I}^n(F)/\mathrm{I}^{n+1}(F)$ for all $n \geq 0$. Here $K_n^M(F)$ is "Milnor K-theory," which we will not describe in general at the moment. But we can say that $K_1^M(F) \cong F^\times$ and $2K_1^M(F) \cong F^{\boxtimes}$, and that recovers the formulation in the corollary.

2.3. **First computations.** Our present task is to compute our first (Grothendieck-)Witt rings. A field F is called *quadratically closed* when $F^\times = F^{\boxtimes}$, *i.e.*, when every element of F is a square. Algebraically closed fields like $\mathbb{C}$ and $\overline{Q}$ are quadratically closed, but so are other fields like the constructible numbers and $\bigcup_{n\geq 0} \mathbb{F}_{5^{2^n}}$.

Proposition 2.9. A field F is quadratically closed if and only if $\dim : \mathrm{GW}(F) \to \mathbb{Z}$ is an isomorphism. In this case, $\dim_0 : \mathrm{W}(F) \cong \mathbb{Z}/2\mathbb{Z}$.

Proof. If F is quadratically closed, then $\langle a\rangle \cong \langle 1\rangle$, and $q \cong (\dim q)\langle 1\rangle$ for every form q. Thus $\dim$ is an isomorphism. Conversely, if $\dim$ is an isomorphism, then $\langle a\rangle \cong \langle 1\rangle$ for all $a \in F^\times$, so every $a \in F$ is a square. □

With this easy case done, we turn to a new class of fields which includes $\mathbb{R}$:

Definition 2.10. A field F is *Euclidean* if it is formally real[2] and $F^\times/F^{\boxtimes} = \{\pm F^{\boxtimes}\}$. In a Euclidean field, call the elements of $F^{\boxtimes}$ *positive*, and call the elements of $-F^{\boxtimes}$ *negative*. The *sign* of a nonzero element of F is defined similarly.

Proposition 2.11. If F is Euclidean, then the following statements hold:

(a) There are exactly two anisotropic forms of each positive dimension n, namely $n\langle 1\rangle$ and $n\langle -1\rangle$.

[2]This means that F has an ordering or, equivalently, no sum of squares in F is equal to -1. We will discuss formally real fields in much greater depth later on.

(b) The Witt ring of F is $\mathrm{W}(F) \cong \mathbb{Z}$.
(c) (Sylvester's law of inertia) Two nonsingular forms over F are equivalent if and only if they have the same dimension and the same signature.
(d) As an Abelian group, $\mathrm{GW}(F) \cong \mathbb{Z} \oplus \mathbb{Z}$. As a ring, $\mathrm{GW}(F) \cong \mathbb{Z}[C_2]$, the integral group ring of the cyclic group of order 2.

Proof. For (a), note that a form is anisotropic if and only if, in its diagonalization, the coefficients do not have mixed signs. The elements of $\mathrm{W}(F)$ are in bijective correspondence with anisotropic forms, so (b) follows.

For (c), we first define *signature*. We claim that in a diagonalization of a form q, the number of positive coefficients (and hence the number of negative coefficients as well) is uniquely determined. To see this, suppose that $\dim q = n$ and $r\langle 1\rangle \oplus (n-r)\langle -1\rangle$ and $s\langle 1\rangle \oplus (n-s)\langle -1\rangle$ are two diagonalizations of q with $s \geq r$. Passing to the Witt ring $\mathrm{W}(F)$, we have

$$r\langle 1\rangle - (n-r)\langle 1\rangle = s\langle 1\rangle - (n-s)\langle 1\rangle \in \mathrm{W}(F),$$

so $2r\langle 1\rangle = 2s\langle 1\rangle \in \mathrm{W}(F)$. By (b), we get that $r = s$. Thus we may write $n_+ = r$ for the number of positive terms, and $n_- = n - r$ for the number of negative terms. The *signature* of q is defined to be

$$\mathrm{sgn}(q) := n_+ - n_- = 2n_+ - n.$$

Two forms are equivalent if and only if they the same n and the same n_+, if and only if they have the same n and same signature. This is (c).

To prove (d), it suffices to show that $\langle 1\rangle$ and $\langle -1\rangle$ form a free $\mathbb{Z}$-basis for $\mathrm{GW}(F)$, which is the content of the following exercise. □

Exercise 2.12. Finish the proof of (d).

Remark 2.13. The isomorphism $\mathrm{W}(F) \to \mathbb{Z}$ in (b) is precisely the signature homomorphism.

Exercise 2.14. Make headway on Exercises 6 and 7 on p.48 of Lam.

At this point, we can also specify the restriction map $\mathrm{res}_F^{F(\sqrt{-1})}$ when F is Euclidean. For concreteness, we will suppose that $F = \mathbb{R}$ so that we are considering $\mathrm{res}_{\mathbb{R}}^{\mathbb{C}} : \mathrm{GW}(\mathbb{R}) \to \mathrm{GW}(\mathbb{C})$. Since $\langle -1\rangle \cong \langle 1\rangle$ over $\mathbb{C}$, $\mathrm{res}_{\mathbb{R}}^{\mathbb{C}}(n_+\langle 1\rangle \oplus n_-\langle -1\rangle) = (n_+ + n_-)\langle 1\rangle$, and we can identify $\mathrm{res}_{\mathbb{R}}^{\mathbb{C}}$ with the dimension homomorphism.

Our next goal is to determine the Witt and Grothendieck-Witt rings of finite fields. Let $\mathbb{F}_q$ denote the finite field with q elements, where $q = p^n$ for $p \neq 2$ a prime. Recall that $|\mathbb{F}_q^\times / \mathbb{F}_q^{\boxtimes}| = 2$. Denote its two square classes 1 and s. Note that $-1 \in \mathbb{F}_q^{\boxtimes}$ if and only if $q \equiv 1 \pmod 4$, so s may be taken to be -1 if and only if $q \equiv 3 \pmod 4$.

Proposition 2.15. Let $F = \mathbb{F}_q$, and $F^\times / F^{\boxtimes} = \{1, s\}$. Then
(a) s is a sum of two squares, and
(b) every nonsingular binary form is universal.

Proof. We first show that (a) implies (b). Since $\langle 1\rangle = \langle a^2\rangle$ for all $a \in F^\times$ and there are only two square classes, there are at most three nonequivalent binary forms:

$$f_1 = \langle 1, 1\rangle, \qquad f_2 = \langle s, s\rangle, \qquad f_3 = \langle 1, s\rangle.$$

We have $D(f_3) = F^\times$ since $F^\times = F^{\boxtimes} \cup sF^{\boxtimes}$. Part (a) implies that $D(f_1) = D(f_2) = F^\times$.

To establish (a), we argue in two cases. First, suppose $-1 \in F^{\boxtimes}$. Then $\langle 1, 1\rangle \cong \langle 1, -1\rangle = \mathbb{H}$, which is universal. Now suppose $-1 \notin F^{\boxtimes}$. The sets $F^{\boxtimes}$ and $1 + F^{\boxtimes}$ are subsets of F of the same cardinality; they are not equal since $1 \in F^{\boxtimes}$ but is not in $1 + F^{\boxtimes}$. Thus there exists

some $1+z^2$ which is not in $F^{\boxtimes}$. Since $-1 \notin F^{\boxtimes}$, $1+z^2 \neq 0$, so we may take s to be $1+z^2$, proving (a). □

Theorem 2.16. *Assume that every binary form over the field F is universal. Then*

(a) two quadratic forms are isometric if and only if they have the same dimension and same determinant;
(b) $\mathrm{GI}^2(F) \cong \mathrm{I}^2(F) = 0$ and $\mathrm{GI}(F) \cong \mathrm{I}(F) \cong F^\times/F^{\boxtimes}$; and
(c) $\mathrm{W}(F) \cong Q(F)$ as rings, and $\mathrm{GW}(F) = \mathbb{Z} \oplus \mathrm{GI}(F)$ with trivial multiplication on $\mathrm{GI}(F)$.

Proof. By hypothesis, any binary form $\langle a_1, a_2\rangle$ represents 1. By the Representation Criterion (Lemma 1.11), we learn that $\langle a_1, a_2\rangle \cong \langle 1, e\rangle$ for some $e \in F^\times$. These forms must have the same determinant, so $e = a_1a_2$ and $\langle a_1, a_2\rangle \cong \langle 1, a_1a_2\rangle$. By induction, an arbitrary nonsingular form $q \cong \langle a_1, \dots, a_n\rangle \cong \langle 1, \dots, 1, d(q)\rangle$. This proves (a).

Since $\mathrm{GI}(F)$ is additively generated by classes of the form $\langle a\rangle - \langle 1\rangle$, we know that $\mathrm{GI}^2(F)$ is additively generated by $(\langle a\rangle - \langle 1\rangle)(\langle b\rangle - \langle 1\rangle) = \langle ab\rangle + \langle 1\rangle - \langle a\rangle - \langle b\rangle = 0$. Thus $\mathrm{GI}^2(F) = 0$, proving the first part of (b). It follows that

$$\mathrm{GI}(F) \cong \mathrm{I}(F) \cong \mathrm{I}(F)/\mathrm{I}^2(F) \cong F^\times/F^{\boxtimes}$$

by Corollary 2.8.

For (c), recall that $\mathrm{W}(F)/\mathrm{I}^2(F) \cong Q(F)$ by Proposition 2.6, and we have just seen that $\mathrm{I}^2(F) = 0$, so $\mathrm{W}(F) \cong Q(F)$. The description of $\mathrm{GW}(F)$ follows from the split exact sequence

$$0 \to \mathrm{GI}(F) \to \mathrm{GW}(F) \xrightarrow{\dim} \mathbb{Z} \to 0.$$

□

As a corollary, we get the desired computation for finite fields.

Corollary 2.17. Let $F = \mathbb{F}_q$ with q odd.

(a) If $q \equiv 1 \pmod 4$, then $\mathrm{W}(F) \cong \mathbb{F}_2[F^\times/F^{\boxtimes}]$ as rings.[3]
(b) If $q \equiv 3 \pmod 4$, then $\mathrm{W}(F) \cong \mathbb{Z}/4\mathbb{Z}$ as rings.
(c) In all cases, $\mathrm{GW}(F) \cong \mathbb{Z} \oplus F^\times/F^{\boxtimes}$ as rings (with trivial multiplication on $F^\times/F^{\boxtimes}$).

Exercise 2.18. Work out the proof in detail by using the definition of $Q(F)$. You should get a split extension when $q \equiv 1 \pmod 4$ and a non-split one when $q \equiv 3 \pmod 4$.

Let's now think about the relevant restriction maps. Recall that $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if and only if $m \mid n$. Assume $m \mid n$, set $q = p^m$ and $q' = p^n$ so that $F \subseteq E$ for $F = \mathbb{F}_q$, $E = \mathbb{F}_{q'}$. The isomorphism $\mathrm{GW}(F) \to \mathbb{Z} \oplus F^\times/F^{\boxtimes}$ is just $(\dim, d)$, and these functions are preserved by extension of scalars. In other words, we have the commutative diagram

$$\begin{array}{ccc} \mathrm{GW}(F) & \xrightarrow{(\dim,d)} & \mathbb{Z} \oplus F^\times/F^{\boxtimes} \\ {\scriptstyle \mathrm{res}^E_F}\downarrow & & \downarrow \\ \mathrm{GW}(E) & \xrightarrow[(\dim,d)]{} & \mathbb{Z} \oplus E^\times/E^{\boxtimes}. \end{array}$$

where the horizontals are isomorphisms, and the right vertical takes $(n, aF^{\boxtimes}) \mapsto (n, aE^{\boxtimes})$.

[3]The right-hand side is a *group ring*. For a commutative ring R and group G, $R[G]$ consists of R-linear combinations of elements of G (*i.e.*, the free R-module with basis G). The multiplication is given by distribution and the rule $(rg)(sh) = (rs)(gh)$ for $r, s \in R$, $g, h \in G$.

Exercise 2.19. In this setting, there are only two possible homomorphisms $F^\times/F^{\boxtimes} \to E^\times/E^{\boxtimes}$, namely the trivial map and the (unique) isomorphism. Determine conditions on $F \subseteq E$ (perhaps in terms of q, q') that specify the corresponding map $F^\times/F^{\boxtimes} \to E^\times/E^{\boxtimes}$.

Exercise 2.20. Use your answer to the previous question to further specify res_F^E (both on GW and on W).

Your answer to the above question is the first step towards explicating the Tambara functor structure on GW over a finite field!

2.4. **Presentation of Witt and Grothendieck-Witt rings.** The Grothendieck-Witt ring $\mathrm{GW}(F)$ is generated (as a ring) by the elements $\langle a\rangle$, $a \in F^\times$. These satisfy the relations

(i) $\langle 1\rangle = 1$,
(ii) $\langle a\rangle\langle b\rangle = \langle a\rangle b$ for $a, b \in F^\times$, and
(iii) $\langle a\rangle + \langle b\rangle = \langle a+b\rangle(1 + \langle ab\rangle)$ for $a, b, a+b \in F^\times$.

Indeed, (i) and (ii) are obvious, while (iii) follows from the fact that $\langle a, b\rangle$ represents $a + b$ and thus is equivalent to a form of the form $\langle a + b, e\rangle$. In order for determinants to match in $F^\times/F^{\boxtimes}$, we take $e = ab(a + b)$.

Theorem 2.21. *Let $\mathscr{F}$ be the free commutative ring generated by $\{[a] \mid a \in F^\times\}$. Let I be the ideal generated by the elements*

(i) $[1] - 1$,
(ii) $[ab] - [a] - [b]$ *for* $a, b \in F^\times$, *and*
(iii) $[a] + [b] - [a + b](1 + [ab])$ *for* $a, b, a + b \in F^\times$.

Then the map $\mathscr{F} \to \mathrm{GW}(F)$ given by $[a] \mapsto \langle a\rangle$ induces an isomorphism $\mathscr{F}/I$.

Proof idea. It is clear that $\mathscr{F} \to \mathrm{GW}(F)$ is surjective (since the forms $\langle a\rangle$ generate $\mathrm{GW}(F)$). The map extends to $\mathscr{F}/I$ because all the relations are satisfied in $\mathrm{GW}(F)$. We now want to define an inverse homomorphism $\mathrm{GW}(F) \to \mathscr{F}/I \to \mathrm{GW}(F)$ taking $q \cong \langle a_1, \ldots, a_n\rangle$ to $[a_1] + \cdots + [a_n]$. Well-definition requires some material we did not cover, namely Witt's Chain Equivalence Theorem (I.5.2 in Lam). □

Corollary 2.22. Let $\mathscr{F}'$ be the free abelian group generated by $\{\{a\} \mid a \in F^\times\}$. Let H be the subgroup of $\mathscr{F}'$ generated by the elements

(i) $\{ab^2\} - \{a\}$ for $a, b \in F^\times$ and
(ii) $\{a\} + \{b\} - \{a + b\} - \{ab(a + b)\}$ for $a, b, a + b \in F^\times$.

Then $\mathrm{GW}(F) \cong \mathscr{F}'/H$.

There are similar presentations of $\mathrm{W}(F) = \mathrm{GW}(F)/\mathbb{Z} \cdot \mathbb{H}$. We only need to add the relation $[1] + [-1] = 0$ or $\{1\} + \{-1\} = 0$.

3. Restriction and Transfer

Let's now jump to some material from Chapter VII of Lam.

3.1. **Scharlau's transfer.** Let $F \subseteq E$ be a field extension of finite degree. Let $s : E \to F$ be a nonzero F-linear functional on the F-vector space E. For any E-bilinear space (U, B), we may compose $B : U \times U \to E$ with the functional s to get an F-bilinear form

$$sB : U \times U \to F.$$

Proposition 3.1. If (U, B) is a regular E-bilinear space, then (U, sB) is a regular F-bilinear space.

FIGURE 3. Winfried Scharlau, b.1940. Ph.D. student of Friedrich Hirzebruch, Professor Emeritus in Münster, Grothendieck's biographer.

Proof. If not, there would exist $x_0 \in U$ such that $(sB)(x_0, U) = 0$. By regularity of (U, B), there exists $y_0 \in U$ such that $B(x_0, y_0) = d \neq 0$. For any $c \in E$, we have

$$B(x_0, (c/d)y_0) = (c/d) \cdot B(x_0, y_0) = c.$$

Applying s to this equation, we get

$$s(c) \in (sB)(x_0, U) = 0.$$

This contradicts s being nonzero. □

For $s : E \to F$ a nonzero F-linear functional, let $s_*(U)$ denote the bilinear space U over F with form sB. We call $s_*(U)$ the *transfer* of U (relative to s). The construction is due to Winfried Scharlau.

Exercise 3.2. The function $s_* : \mathrm{GW}(E) \to \mathrm{GW}(F)$ is *not* a ring homomorphism, but it is a group homomorphism.

Exercise 3.3. For extensions $F \subseteq E \subseteq K$ and nonzero functionals $t : K \to E$, $s : E \to F$, we have

$$(s \circ t)_* = s_* \circ t_*.$$

Exercise 3.4. Prove that

$$\dim_F s_*(U) = [E : F] \dim_E U.$$

A natural choice for $s : E \to F$ is the *field trace* $\mathrm{Tr}_{E/F} : E \to F$.

Definition 3.5. For a field extension $F \subseteq E$ and $\alpha \in E$, define $m_\alpha : E \to E$ to be the F-linear map $x \mapsto \alpha x$. The *trace* of α is

$$\mathrm{Tr}_{E/F}(\alpha) = \mathrm{Tr}(m_\alpha)$$

where the latter Tr is the linear algebra trace of a linear transformation (choose a basis, write m_α as a matrix, sum the diagonal entries).

It is a basic field theory fact that $\mathrm{Tr}_{E/F} \not\equiv 0$ if and only if $F \subseteq E$ is *separable*; this means that the F-minimal polynomial of every $\alpha \in E$ is separable (has no repeated roots). Thus we will restrict our attention to separable extensions $F \subseteq E$ and write tr_F^E for $(\mathrm{Tr}_{E/F})_*$. This will give the transfer maps on GW when considered as a Mackey or Tambara functor.

Our first theorem relating restriction and s_* is the Scharlau (or Frobenius) reciprocity theorem.

Theorem 3.6. *For a field extension $F \subseteq E$ and nonzero functional $s : E \to F$, let V be a quadratic space over F and U a quadratic space over E. Then*

$$s_*(\mathrm{res}_F^E V \otimes_E U) \cong V \otimes_F s_*(U).$$

In particular, with $U = \langle 1 \rangle_E$, we have

$$s_*(\mathrm{res}_F^E V) \cong V \otimes_F s_*(\langle 1 \rangle_E).$$

You can find the proof on pp.189–190 of Lam. Frobenius reciprocity theorems typically have something to do with a Mackey functor being a "Green functor" which are important things that we're not talking about this summer.

Exercise 3.7. Interpret Scharlau reciprocity as saying that s_* is a $\mathrm{GW}(F)$-module map, where we use $\mathrm{res}_F^E : \mathrm{GW}(F) \to \mathrm{GW}(E)$ to view $\mathrm{GW}(E)$ as a $\mathrm{GW}(F)$-module.

As a corollary to Scharlau reciprocity, we get that s_* takes hyperbolic spaces to hyperbolic spaces: s_* respects orthogonal sum, and

$$s_*(\mathbb{H}_E) = s_*(\mathrm{res}_F^E \mathbb{H}_F) \cong \mathbb{H}_F \otimes_F s_*(\langle 1 \rangle_E) \cong [E : F]\mathbb{H}_F,$$

where the last isometry holds because $\dim_F s_* \langle 1 \rangle_E = [E : F]$ and it is always the case that $\mathbb{H} \otimes q \cong (\dim q)\mathbb{H}$.

By the above paragraph, s_* also induces an Abelian group (and $\mathrm{W}(F)$-module) homomorphism $\mathrm{W}(E) \to \mathrm{W}(F)$.

We will have student lectures on Lam VII.2 and VII.3. These study the effect of res_F^E on W according to the parity of $[E : F]$. The main takeaways are that (1) res_F^E is a split injection of $\mathrm{W}(F)$-modules when $[E : F]$ is odd, and (2) $\ker(\mathrm{res}_F^{F(\sqrt{a})})$ is the ideal generated by $\langle 1, -a \rangle$ for $a \in F^\times \smallsetminus F^{\boxtimes}$. We will want to extend these results to GW. (The GW variants may or may not already be in the literature.)

3.2. **Galois Mackey functors.** At this point we have both restriction and transfer maps associated with field extensions, so the time is ripe to introduce the notion of a Galois Mackey functor. Fix a (profinite) Galois extension $F \subseteq E$ with Galois group G.[4] In Angélica's lectures, we have already seen the notion of a G-Mackey functor, at least when G is finite. For G profinite (which means it is a limit of finite groups), we make the same definitions, restricting our attention to finite G-sets. Finite G-orbits are isomorphic to G/U for U an open subgroup of G.[5] Thus it suffices to specify a G-Mackey functor on finite orbits G/U.

The (profinite) Galois correspondence provides a bijective correspondence between closed subgroups $H \leq G$ and subextensions $F \subseteq K \subseteq E$ by taking H to $E^H = \{e \in E \mid he = e \text{ for all } h \in H\}$. The inverse bijection takes K to $\mathrm{Gal}(K/F)$. Finite subextensions

[4] It's important to consider profinite Galois extensions because the algebraic and separable closures of F are, in general, profinite.

[5] Someone should talk about the basics of profinite groups. In particular, G gets a topology and subgroups are open if and only if they are closed and have finite index.

$F \subseteq K \subseteq E$ (meaning that $[K : F] < \infty$) are in bijective correspondence with open subgroups $U \subseteq G$.

Since finite transitive G-sets are all of the form G/U, $U \leq G$ open, we get a function $\mathscr{O}_G \to \mathrm{Sub}(F \subseteq E)$ taking $G/U \mapsto E^U$ where $\mathscr{O}_G$ is the set of finite G-orbits and $\mathrm{Sub}(F \subseteq E)$ is *ad hoc* notation for the set of finite subextensions of $F \subseteq E$ (*i.e.*, $F \subseteq K \subseteq E$ with $[K : F] < \infty$). This assignment lifts to the level of categories! We make $\mathscr{O}_G$ into a category by taking G-equivariant functions for our morphisms. For $\mathrm{Sub}(F \subseteq E)$ a morphism between subextensions $F \subseteq K, L \subseteq E$ is a field homomorphism $K \to L$which is the identity on F. To get a functor, we need to produce field homomorphisms from G-equivariant maps $G/U \to G/V$, $U, V \leq G$ open. First consider the case when $U \leq V \leq G$ and $G/U \to G/V$ is the restriction map. Note that since $U \leq V$, $E^V \subseteq E^U$, and it is this inclusion that we assign to the restriction map. Since source and target were swapped, we know that we are looking for a contravariant functor $\mathscr{O}_G^{\mathrm{op}} \to \mathrm{Sub}(F \subseteq E)$.

Exercise 3.8. Figure out what the conjugation maps in $\mathscr{O}_G$ naturally induce in $\mathrm{Sub}(F \subseteq E)$. Use the fact that the existence of a G-equivariant map $f : G/U \to G/V$ is the same as a subconjugacy $g^{-1}Vg \leq U$ to determine the value of the functor on f.

The fundamental theorem of profinite Galois theory says that the functor $\mathscr{O}_G^{\mathrm{op}} \to \mathrm{Sub}(F \subseteq E)$ is an equivalence of categories.

In our study of Mackey functors, it was useful to work with G-sets, not just G-orbits, and we will want a similar formulation when working with field extensions. By categorical yoga, the Cartesian product of G-sets corresponds to the tensor product of field extensions.[6]

Proposition 3.9. Suppose $F \subseteq E$ is a Galois extension of fields and $K, L \in \mathrm{Sub}(F \subseteq E)$. Then $K \otimes_F L$ is isomorphic to a Cartesian product of subextensions of $F \subseteq E$.

Proof. Choose a primitive element $\alpha \in E$ such that $K = F(\alpha)$. Then α has minimal polynomial f which is separable, and $K \cong F[t]/(f(t))$. Thus

$$K \otimes_F L \cong L[t]/f(t)L[t].$$

The polynomial $f(t)$ factors into a product of irreducible polynomials over L, say $f(t) = \prod f_i(t)$. Then

$$K \otimes_F L \cong \prod L[t]/f_i(t)L[t]$$

and each $L[t]/f_i(t)L[t]$ is a finite subextension of $F \subseteq E$. □

For $F \subseteq E$ a Galois field extension, an F-algebra R which is a subring of E and is isomorphic to a Cartesian product of finite subextensions of $F \subseteq E$ is called a *finite étale F-subalgebra* of E. We let $\mathrm{Fét}_{E/F}$ denote the category with objects the finite étale F-subalgebras of E and with morphisms $S \to R$ the set of F-algebra homomorphisms $R \to S$. (Note that we snuck an $(\ )^{\mathrm{op}}$ in here relative to the usual category of F-algebras! In the sequel, we will always work with F-algebra maps $R \to S$ and not their reversed avatars in $\mathrm{Fét}_{E/F}$.) If $G\,\mathrm{Fin}$ is the category of finite G-sets and G-equivariant maps, then the Galois correspondence provides inverse equivalences of categories

$$G\,\mathrm{Fin} \to \mathrm{Fét}_{E/F} \qquad \text{and} \qquad \mathrm{Fét}_{E/F} \to G\,\mathrm{Fin}\,.$$

This makes the following definition quite reasonable.

[6]This is because the Cartesian product of G-sets is a categorical product and hence turns into a categorical coproduct via a contravariant equivalence of categories. The coproduct of F-algebras (F-vector spaces which are commutative rings) R, S is $R \otimes_F S$ with multiplication $(r \otimes s)(r' \otimes s') = (rr') \otimes (ss')$.

Definition 3.10. Given a profinite Galois extension $F \subseteq E$, a *Galois Mackey functor* M for $F \subseteq E$ consists of

(a) an Abelian group $M(R)$ for each finite étale F-subalgebra of E and
(b) homomorphisms $\mathrm{res}_f : M(R) \to M(S)$ and $\mathrm{tr}_f : M(S) \to M(R)$ for each F-algebra homomorphism $f : R \to S$

satisfying the following conditions:

(i) $M(R \times S) \cong M(R) \times M(S)$ via the canonical map,
(ii) res_f and tr_f are functorial in f, and
(iii) given finite étale F-subalgebras R, S, T of E and a commutative square of F-algebra homomorphisms

$$\begin{array}{ccc} S \otimes_R T & \xleftarrow{f} & T \\ {\scriptstyle g}\uparrow & & \uparrow{\scriptstyle h} \\ S & \xleftarrow[k]{} & R, \end{array}$$

the square

$$\begin{array}{ccc} M(S \otimes_R T) & \xrightarrow{\mathrm{tr}_f} & M(T) \\ {\scriptstyle \mathrm{res}_g}\uparrow & & \uparrow{\scriptstyle \mathrm{res}_h} \\ M(S) & \xrightarrow[\mathrm{tr}_k]{} & M(R) \end{array}$$

commutes.

The Mackey axiom (iii) looks a little topsy turvy because the pullback of G-sets has been replaced by the pushout (= tensor product) of commutative rings. Things might look a little cleaner if we used the language of algebraic geometry (in which affine F-schemes form the opposite category of F-algebras), but we are avoiding the additional definitional burden.

Exercise 3.11. Formulate the "G-orbits and double coset formula" version of the above definition.

Theorem 3.12. *For a Galois extension $F \subseteq E$, the Grothendieck-Witt functor is a Galois Mackey functor.*

Before proving this theorem, we need to make sure we know what $\mathrm{GW}(R)$, res_f, and tr_f are for R a finite étale algebra and $f : R \to S$ an F-algebra homomorphism. An R-bilinear form is an R-module M and R-bilinear map $M \times M \to R$. We can play the same regularity, isometry, orthogonal sum, and tensor product games to form $\mathrm{GW}(R)$ as the Grothendieck construction on isometry classes of R-bilinear forms. Restriction along $f : R \to S$ is given by base change to S, so that (M, B) becomes $S \otimes_F M, \mathrm{id}_S \otimes_F B)$. This defines a ring map $\mathrm{res}_f : \mathrm{GW}(R) \to \mathrm{GW}(S)$.

Now suppose that $f : R \to S$ is a ring map (inducing an R-module structure on S) and $s : S \to R$ is an R-linear map. Then post-composition with s takes an S-bilinear form to an R-bilinear form. This defines an Abelian group homomorphism $s_* : \mathrm{GW}(S) \to \mathrm{GW}(R)$. When $f : R \to S$ is an F-algebra homomorhism between finite étale F-subalgebras of E, the usual construction produces an R-linear trace map $\mathrm{Tr}_f : S \to R$. We define $\mathrm{tr}_f := (\mathrm{Tr}_f)_*$.

It's good to have these elegant definitions in hand, but also note that by Proposition 3.9, nothing new is really going on. The algebras in questions are just products of fields, and

it is easy to show that $\mathrm{GW}(K \times L) \cong \mathrm{GW}(K) \times \mathrm{GW}(L)$. The maps res_f and tr_f may be computed "one field at a time."

For $R, S, T \in \mathrm{Fét}_{E/F}$, let $f : R \to S$ and $g : R \to T$ be two F-algebra maps, and let $s : S \to R$ be an R-linear map back into R. We get a T-linear map $t : T \otimes_R S \to T$ given by $b \otimes a \mapsto b \cdot g(s(a))$. There is also a ring homomorphism $h : S \to T \otimes_R S$ given by $a \mapsto 1 \otimes a$ such that

$$\begin{array}{ccc} R & \xrightarrow{g} & T \\ {\scriptstyle s}\uparrow & & \uparrow{\scriptstyle t} \\ S & \xrightarrow[h]{} & T \otimes_R S \end{array}$$

commutes. Given an S-bilinear form (M, B), we thus get two T-bilinear forms $\mathrm{res}_g(s_*(M, B))$ and $t_*(\mathrm{res}_h(M, B))$.

Lemma 3.13 (Dress, Appendix A Lemma 2.1)**.** There is a natural isometry $\mathrm{res}_g(s_*(M, B)) \cong t_*(\mathrm{res}_h(M, B))$

Proof. We first compute

$$\begin{aligned} \mathrm{res}_g(s_*(M, B)) &= \mathrm{res}_g(M|_R, sB) \\ &= (T \otimes_R M, \mathrm{id}_T \otimes_R sB). \end{aligned}$$

On the other hand,

$$\begin{aligned} t_*(\mathrm{res}_h(M, B)) &= t_*((T \otimes_R S) \otimes_S M, \mathrm{id}_{T \otimes_R S} \otimes_S B) \\ &\cong t_*(T \otimes_R M, \mathrm{id}_T \otimes_R B) \\ &= (T \otimes_R M, \mathrm{id}_T \otimes_R sB). \end{aligned}$$

Manifestly, the two expressions are equivalent. □

The following corollary is immediate.

Corollary 3.14. With the above notations, we have a commutative diagram

$$\begin{array}{ccc} \mathrm{GW}(R) & \xrightarrow{\mathrm{res}_g} & \mathrm{GW}(T) \\ {\scriptstyle s_*}\uparrow & & \uparrow{\scriptstyle t_*} \\ \mathrm{GW}(S) & \xrightarrow[\mathrm{res}_h]{} & \mathrm{GW}(T \otimes_R S). \end{array}$$

Finally, we can prove that GW is a Galois Mackey functor.

Proof of Theorem 3.12. We have already specified the data, and (i) holds because of the already-mentioned isomorphism $\mathrm{GW}(R \times S) \cong \mathrm{GW}(R) \times \mathrm{GW}(S)$ (where the map is the product of the the restrictions of the projection maps). Functoriality (ii) is a very easy check given our definitions of res_f and tr_f. The Mackey axiom (iii) remains, but this is just a specialization of Corollary 3.14 in which appropriate trace maps are taken for s and t. □

Corollary 3.15. The Witt functor is a Galois Mackey functor as well.

4. The Rost norm

In the next section, we will define a Galois Tambara functor, which will add "multiplicative transfers" / norms into the mix. The norm that will make GW into a Galois Tambara functor was defined by Markus Rost.

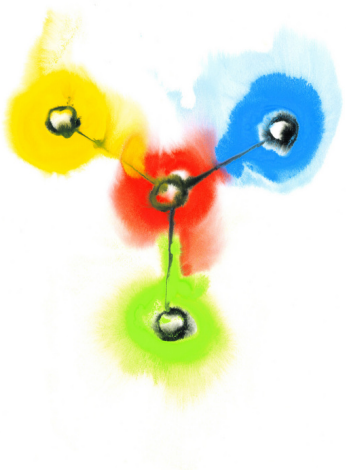


FIGURE 4. Markus Rost was born in 1958 and is a professor in Bielefeld. There aren't any pictures of him on the Internet, but his father, Herbert Rost, made this cover illustration of "triality" for *The Book of Involutions*, which Markus Rost coauthored. Rost's work on norm varieties was crucial for Voevodsky's proofs of the Milnor and Bloch-Kato conjectures.

Fix a field F, let R be a finite étale F-algebra, and let M be an R-module. For a natural number i, let $M^{\otimes i} := M \otimes_R \cdots \otimes_R M$ where there are i factors. The symmetric group Σ_i acts on $M^{\otimes i}$ in a natural way: for $\sigma \in \Sigma_i$,

$$\sigma(x_1 \otimes \cdots \otimes x_i) = x_{\sigma^{-1}1} \otimes \cdots \otimes x_{\sigma^{-1}i}.$$

(The inverses are there to ensure that we have a left action.) The *i-th symmetric power* of M is

$$\mathrm{Sym}^i_R(M) := (M^{\otimes i})^{\Sigma_i} = \{x \in M^{\otimes i} \mid \sigma x = x \text{ for all } \sigma \in \Sigma_i\}.$$

We may also form the *i-th exterior power* of M, $\bigwedge^i_R M$. This is done most naturally by taking a particular subspace of the *exterior algebra* of M, $\bigwedge M$. This is the quotient of the tensor algebra $T_R(M) = \bigoplus_{i \geq 0} M^{\otimes I}$ (with product given by concatenating simple tensors) by the ideal I generated by all simple tensors of the form $x \otimes x$, $x \in M$:

$$\bigwedge_R M := T_R(M)/I.$$

The image of $x_1 \otimes \cdots \otimes x_i$ in $\bigwedge_R M$ is denoted $x_1 \wedge \cdots \wedge x_i$. These symbols satisfy the familiar alternating relations $x \wedge x = 0$, $x \wedge y = -y \wedge x$, and $x_{\sigma 1} \wedge \cdots \wedge x_{\sigma i} = \mathrm{sgn}(\sigma) x_1 \wedge \cdots \wedge x_i$. The i-th exterior power of M, $\bigwedge^i_R M$, is the submodule spanned by i-fold wedge products of elements of M, $x_1 \wedge \cdots \wedge x_i$.

Exercise 4.1. If M is a free R-module of rank n, then the i-th exterior power of M has dimension $\binom{n}{i}$. In particular, $\bigwedge^n_R M \cong R$.

Now take $R, S \in \mathrm{Fét}_{E/F}$ for some Galois extension $F \subseteq E$ and an F-algebra homomorphism $f : R \to S$. The tensor power $S^{\otimes i} = S \otimes_R \cdots \otimes_R S$ is an R-algebra which is also in

$\text{Fét}_{E/F}$. Furthermore, $\text{Sym}_R^i S$ is a subalgebra of $S^{\otimes i}$. Now $\bigwedge_R^i S$ is a quotient of $S^{\otimes i}$, so we may view $\bigwedge_F^i S$ as a $\text{Sym}_R^i S$-module. This induces an F-algebra homomorphism

$$\rho_i : \text{Sym}_R^i S \to \text{End}_R(\bigwedge_R^i S)$$

taking x to the multiplication-by-x map.

The map $f : R \to S$ gives S the structure of a free R-module of finite rank, say n. Thus $\bigwedge_R^n S \cong R$, in which case $\text{End}_R(\bigwedge_R^n S) \cong R$. Composing ρ_n with this isomorphism results in an F-algebra homomorphism

$$\nu_f : \text{Sym}_R^n S \to R$$

called the *norm* of $f : R \to S$.

Exercise 4.2. For a finite field extension $F \subseteq K$, the norm function $N_{K/F} : K \to F$ is the function which assigns the determinant of the multiplication-by-$x \in K$ map to x. If $F \subseteq K$ is a Galois extension, $N_{K/F}(x) = \prod_{\sigma \in \text{Gal}(K/F)} \sigma(x)$. Check that if $[K : F] = n$, then $\nu_{F \subseteq K}(x^{\otimes n}) = N_{K/F}(x)$. *Hint*: The determinant of an F-linear map $f : K \to K$ is "the same thing" as $\bigwedge_F^n f : \bigwedge_F^n K \to \bigwedge_F^n K$.

Take $R, S \in \text{Fét}_{E/F}$ and an F-algebra homomorphism $f : R \to S$ with $n = \dim_R S$. If M is a finitely generated (necessarily free) S-module, the *norm* of M along f is

$$\nu_f(M) := \text{Sym}_R^n M \otimes_{\text{Sym}_R^n S} R$$

where the $\text{Sym}_R^n S$-module structure on R is induced by $\nu_f : \text{Sym}_R^n S \to R$.

Now suppose that M also carries an S-bilinear form $B : M \times M \to S$. The form

$$B^{\otimes n} : M^{\otimes n} \times M^{\otimes n} \to S^{\otimes n}$$

restricts to a form

$$\text{Sym}_R^n B : \text{Sym}_R^n M \times \text{Sym}_R^n M \to \text{Sym}_R^n S.$$

Thus $\text{Sym}_R^n B \otimes_{\text{Sym}_R^n S} R$ is an R-bilinear form

$$N_f(B) : \nu_f(M) \times \nu_f(M) \to R.$$

The *norm* of (M, B) along f is defined to be $(\nu_f(M), N_f(B))$.

Exercise 4.3. If $f : K \to L \in \text{Sub}(F \subseteq E)$, then $N_f \langle a \rangle_L = \langle N_{L/K}(a) \rangle_K$ for all $a \in L^\times$.

Exercise 4.4. I believe that the following statments are true. Either prove them, or modify them so that they are true and then prove them:

If $f : K \to L \in \text{Sub}(F \subseteq E)$ and V is an L-vector space, then

$$\nu_f(V) \cong \left(\bigotimes_{\sigma \in \text{Gal}(L/K)} V^\sigma \right)^{\text{Gal}(L/K)}$$

where $\otimes = \otimes_L$ and V^σ is the L-vector space with "σ-twisted" scalar multiplication $(\lambda, v) \mapsto \lambda \bullet v := \sigma(\lambda) v$ for $\lambda \in L$ and $v \in V$.

If (V, B) is an L-bilinear space, there is a form B^σ on V^σ is defined by $B^\sigma(u, v) = \sigma^{-1}(B(u, v))$. The form $N_f(B)$ becomes $\bigotimes_{\sigma \in \text{Gal}(L/K)} B^\sigma$ via the above isomorphism. (*A priori*, the codomain of $\bigotimes_{\sigma \in \text{Gal}(L/K)} B^\sigma$ is $\bigotimes_{\sigma \in \text{Gal}(L/K)} L^\sigma$, so part of the statement here is that the form lands in Galois-fixed points when restricted to Galois fixed points and $\left(\bigotimes_{\sigma \in \text{Gal}(L/K)} L^\sigma \right)^{\text{Gal}(L/K)} \cong K$.)

Exercise 4.5. Determine $N_f : \mathrm{GW}(\mathbb{C}) \to \mathrm{GW}(\mathbb{R})$ and $N_g : \mathrm{GW}(\mathbb{F}_{q'}) \to \mathrm{GW}(\mathbb{F}_q)$ for the field extensions $f : \mathbb{R} \to \mathbb{C}$ and $g : \mathbb{F}_q \to \mathbb{F}_{q'}$.

Exercise 4.6. How does the norm construction interact with sums? For a quadratic extension $f : F \to E = F(\sqrt{a})$, Wittkop proves that $N_f(\langle x, y\rangle) = \langle N_{E/F}x\rangle + \langle \mathrm{tr}_f(x\overline{y})\rangle + \langle N_{E/F}y\rangle$ where $\overline{b + c\sqrt{a}} = b - c\sqrt{a}$. This permits inductive computation of $N_f(\langle x_1, \ldots, x_n\rangle)$ in terms of the norm and transfer of unary forms. Is there a similar formula for arbitrary Galois extensions?

5. Galois Tambara functors

We have already seen that a Galois Mackey functor consists of two functors from $\mathrm{Fét}_{E/F}$ to Abelian groups agreeing on objects and satisfying certain compatability axioms. To get a Galois Tambara functor, we will add in a third functor (landing in commutative monoids instead of Abelian groups) and more compatabilities.

We first need the notion of an *exponential diagram* in $\mathrm{Fét}(E/F)^{\mathrm{op}}$. Given F-algebra homomorphisms $A \xrightarrow{f} B \xrightarrow{q} C$ between finite étale F-subalgebras, we claim there are natural maps e, p, r such that

$$\begin{array}{ccccc} B & \xrightarrow{q} & C & \xrightarrow{e} & \nu_f(C) \otimes_A B \\ {\scriptstyle f}\uparrow & & & & \uparrow{\scriptstyle p} \\ A & = & \nu_f(B) & \xrightarrow[r]{} & \nu_f(C) \end{array}$$

commutes. Indeed, we take $r = \nu_f(q)$ and [ADD: e, p descriptions].

Definition 5.1. A *Galois Tambara functor* T for a Galois extension $F \subseteq E$ consists of data

(a) a ring $T(A)$ for each $A \in \mathrm{Fét}_{E/F}$ and
(b) maps $\mathrm{res}_f : T(A) \to T(B)$, $\mathrm{tr}_f, N_f : T(B) \to T(A)$ for each F-algebra homomorphism $f : A \to B$, $A, B \in \mathrm{Fét}_{E/F}$

subject to the following conditions:

(i) res_f is a ring homomorphism, tr_f is a homomorphism of additive monoids, and N_f is a homomorphism of multiplicative monoids;
(ii) res and tr give T the structure of a Galois Mackey functor;
(iii) res and N also satisfy the Mackey axiom; and
(iv) given F-algebra homomorphisms $A \xrightarrow{f} B \xrightarrow{q} C$ for $A, B, C \in \mathrm{Fét}_{E/F}$, the diagram

$$\begin{array}{ccccc} T(B) & \xleftarrow{\mathrm{tr}_q} & T(C) & \xrightarrow{\mathrm{res}_e} & T(\nu_f(C) \otimes_A B) \\ {\scriptstyle N_f}\downarrow & & & & \downarrow{\scriptstyle N_p} \\ T(A) & = & T(\nu_f(B)) & \xleftarrow[\mathrm{tr}_r]{} & T(\nu_f(C)) \end{array}$$

commutes (where e, p, r come from the exponential diagram generated by f, q).

Theorem 5.2. *The restriction, transfer, and norm maps make* GW *a Galois Tambara functor.*

Remark 5.3. The norm does not play well with $\mathbb{H}$ and W is *not* a Galois Tambara functor.

6. Orderings, signatures, and prime ideals

One of the problems we are interested in is determining the Tambara prime ideals of GW. To approach this, we will first want to know the prime ideals of $\mathrm{GW}(F)$. This content is based on Chapter VIII of Lam.

6.1. **Orderings and signatures.** The spectrum of $\mathrm{GW}(F)$ is determined by the orderings of F, so we will study those first.

Definition 6.1. An *ordering* on a field F is a proper subset $P \subsetneq F$ (called the *positive cone* of the ordering) such that
(a) $P + P \subseteq P$,
(b) $P \cdot P \subseteq P$,
(c) $P \cup (-P) = F$.
Given such a set P, we shall say that F is *ordered by* P, or that (F, P) is an *ordered field*.

Given an ordering P, we write $x \leq_P y$ when $y - x \in P$. The reader may check that $\leq_P$ is a total ordering of F, and that $P \mapsto \leq_P$ is a bijection between positive cones and total orderings with inverse $\leq \mapsto \{x \in F \mid 0 \leq x\}$.

The following proposition records some basic facts about orderings that I won't prove in these notes. Write $\sigma(F)$ for the set of sums of squares in F, and $\sigma^\times(F)$ for the nonzero sums of squares in F. We call a field *formally real* when $-1 \notin \sigma(F)$.

Proposition 6.2. Let (F, P) be an ordered field. Then
(a) $\sigma(F) \subseteq P$,
(b) $-1 \notin P$ and $P \cap (-P) = \{0\}$,
(c) F is formally real,
(d) $P^\times := P \smallsetminus \{0\}$ is a subgroup of index 2 in $F^\times$, and
(e) if P' is another ordering of F and $P' \subseteq P$, then $P = P'$.

It is possible to strengthen part (c) of the above proposition to the following statement.

Theorem 6.3 (Artin-Schreier Criterion)**.** *A field has an ordering if and only if it is formally real.*

Given a formally real field F, it will be useful to pass to the largest formally real field containing it.

Definition 6.4. A field F is called *real-closed* if F is formally real, but no proper algebraic extension of F is formally real.

It turns out that real-closed field are always *Euclidean* (formally real with $[F^\times : F^{\boxtimes}] = 2$) with $F(\sqrt{-1})$ quadratically closed. They have a unique ordering given by the positive cone $F^\square = F^{\boxtimes} \cup \{0\}$.

Definition 6.5. Let (F, P) be an ordered field. An extension $F \subseteq R$ is called a *real-closure* of F relative to P if
(a) R is real-closed,
(b) R is algebraic over F, and
(c) $P = R^\square \cap F$.

The final condition tells us that the unique ordering on R restricts to P. Thankfully, real-closures exist:

Theorem 6.6. *Every ordered field (F, P) possesses a real-closure which is unique up to order-preserving isomorphism.*

We are very familiar with a particular real-closed field, namely $\mathbb{R}$. You might recall that $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ is algebraically closed. This phenomenon is generic:

Theorem 6.7. *If R is a real-closed field, then $C = R(\sqrt{-1})$ is algebraically closed.*

FIGURE 5. Albrecht Pfister, b.1934. Professor Emeritus at the Johannes Gutenberg University of Mainz, the namesake of Pfister forms devoted his career to the study of quadratic forms.

For a field F, let X_F denote the (possibly empty) set of orderings on F. Given $\alpha \in X_F$ write P_α for the corresponding positive cone and $\leq_\alpha$ for the associated total ordering of F. For each $\alpha \in X_F$, fix a real-closure F_α of F with respect to α and let $r_\alpha : F \to F_\alpha$ be the inclusion map. The corresponding restriction map on Witt rings is $\mathrm{res}r_\alpha : \mathrm{W}(F) \to \mathrm{W}(F_\alpha)$. Looking back at our computation of $\mathrm{W}(\mathbb{R})$, we see that it goes through verbatim to give a canonical isomoprhism $\mathrm{W}(F_\alpha) \cong \mathbb{Z}$.

Definition 6.8. The composition of $\mathrm{res}r_\alpha$ with $\mathrm{W}(F_\alpha) \cong \mathbb{Z}$ is the *α-signature* homomorphism

$$\mathrm{sgn}_\alpha : \mathrm{W}(F) \to \mathbb{Z}.$$

Abusing notation, we will also denote the composite $\mathrm{GW}(F) \to \mathrm{W}(F) \to \mathbb{Z}$ by sgn_α.

It is simple to get our hands on $\mathrm{sgn}_\alpha(q)$: we simply diagonalize q, count the number n_+ of α-positive elements and n_- of α-negative elements, and finally have $\mathrm{sgn}_\alpha(q) = n_+ - n_-$. In this way, it is easy to see that sgn_α is always surjective.

Letting α range through X_F, we get the *total singature* homomorphism

$$\mathrm{sgn} : \mathrm{W}(F) \to \prod_{\alpha \in X_F} \mathbb{Z}$$

sending $q \mapsto (\mathrm{sgn}_\alpha(q))_\alpha$.

Theorem 6.9 (Pfister's local-global principle)**.** *For any field F, $\ker(\mathrm{sgn}) = \mathrm{W}_{\mathrm{tors}}(F)$, the torsion subgroup of $\mathrm{W}(F)$; moreover, every element of $\mathrm{W}_{\mathrm{tors}}(F)$ is 2-primary torsion.*[7]

Since we have gone to the trouble of defining real-closures, signatures, and trace forms, we may as well state the following incredible theorem of Olga Taussky-Todd from 1968:

[7]This means that the additive order of every torsion element is a power of 2.

FIGURE 6. Olga Taussky-Todd, 1906–1995. The Czech-American (née Austrian) mathematician Olga Taussky-Todd studied number theory under Furtwängler in Vienna and became a faculty member at Caltech in 1957. She was responsible for correcting the collected papers of David Hilbert and made many contributions to number and matrix theory.

Theorem 6.10. *Suppose that (F, P) is an ordered field with real closure R and $f \in F[t]$ is a separable polynomial with coefficients in F. Set $A = F[t]/(f)$. Then*

$$\operatorname{sgn}_P(\operatorname{tr}_{A/F}\langle 1\rangle_A)$$

is the number of roots of f in R.

6.2. **Prime ideals in $\mathrm{GW}(F)$.** For a commutative ring A, let $\operatorname{Spec} A$ denote the set of prime ideals in A. We call $\operatorname{Spec} A$ the *Zariski spectrum* of A. It carries a topology in which the closed sets are those of the form

$$V(I) = \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \supseteq I\}.$$

A subbasis for this topology is given by the sets

$$D(f) = \{\mathfrak{p} \in \operatorname{Spec} A \mid f \notin \mathfrak{p}\}$$

where $f \in A$.

If $\mathfrak{p} \in \operatorname{Spec} A$, then $A/\mathfrak{p}$ is an integral domain and the quotient map $A \to A/\mathfrak{p}$ has kernel $\mathfrak{p}$. By the first isomorphism theorem, we can construct $\operatorname{Spec} A$ by taking kernels of surjective maps $A \to R$ where R is some integral domain. In nice cases (such as $A = \mathrm{GW}(F)$), we can get away with only looking at surjective ring maps $A \to \mathbb{Z}$ and $A \to \mathbb{Z}/p\mathbb{Z}$.

Before we state the main theorem, we need to put a topology on X_F, the set of orderings of F. Note that each $\alpha \in X_F$ induces a function $F^\times \to \{\pm 1\}$ taking α-positive elements to 1 and α-negative elements to -1. Thus there is an injection

$$X_F \hookrightarrow \{\pm 1\}^{F^\times}.$$

We give $\{\pm 1\}$ the discrete topology, and $\{\pm 1\}^{F^\times}$ the induced product topology. Finally, the *Harrison topology* on X_F is the subspace topology relative to the above embedding.

Exercise 6.11. The product topology on $\{\pm 1\}^{F^\times}$ has subbasis consisting of the sets

$$H_{a,\varepsilon} := \{f : F^\times \to \{\pm 1\} \mid f(a) = \varepsilon\}$$

where $a \in F^\times$ and $\varepsilon = \pm 1$. The complement of $H_{a,\varepsilon}$ is $H_{a,-\varepsilon}$, so $H_{a,\varepsilon}$ is both open and closed.

As such, X_F has a subbasis consisting of sets of the form $H_{a,\varepsilon} \cap X_F$, and these are also open and closed.

Topologies with clopen subbases are automatically *Stone spaces*: compact totally disconnected Hausdorff spaces. Note that X_F is discrete if and only if $|X_F| < \infty$.

Let $X_F^* = X_F \amalg \{\infty\}$ denote the Harrison space of orderings X_F with a separated point ∞. Let sgn_α denote the α-signature for $\alpha \in X_F$, and let $\mathrm{sgn}_\infty = \dim$. Let $\mathrm{Sgn} : \mathrm{GW}(F) \to \prod_{X_F^*} \mathbb{Z}$ denote the *ultra-total signature* $\prod_{\alpha \in X_F^*} \mathrm{sgn}_\alpha$.

Theorem 6.12. *The ultra-total signature induces the quotient map*

$$\mathrm{Sgn}^* : X_F^* \times \mathrm{Spec}\,\mathbb{Z} \to \mathrm{Spec}\,\mathrm{GW}(F)$$

that glues all elements of the form $(\alpha, (2))$ *together. In particular, the prime ideals of* $\mathrm{GW}(F)$ *are all of the form*

$$\mathfrak{p}_{\alpha,p} = \{x \in \mathrm{GW}(F) \mid \mathrm{sgn}_\alpha(x) \equiv 0 \pmod{p}\}$$

where $\alpha \in X_F^*$ *and* p *is* 0 *or a rational prime number. We have* $\mathfrak{p}_{\alpha,2} = \mathfrak{p}_{\beta,2}$ *for all* $\alpha, \beta \in X_F^*$

Proof sketch. The proof is almost identical to the one Lam gives for $\mathrm{Spec}\,\mathrm{W}(F)$ in VII.7. Indeed, since $\mathrm{W}(F) = \mathrm{GW}(F)/\mathbb{Z} \cdot \mathbb{H}$, we know that $\mathrm{Spec}\,\mathrm{W}(F)$ may be viewed as a closed subspace of $\mathrm{GW}(F)$ in bijection with prime ideals for which $\alpha \neq \infty$. One then computes $\mathrm{GW}(F)[1/\mathbb{H}] \cong \mathbb{Z}[1/2]$ to get the open complement of the image of $\mathrm{Spec}\,\mathrm{W}(F)$ in $\mathrm{Spec}\,\mathrm{GW}(F)$. This isomorphism follows from the identity $q \otimes \mathbb{H} = (\dim q)\mathbb{H} \in \mathrm{GW}(F)$, which tells us that after inverting $\mathbb{H}$, every form is identified with $(\dim q)\langle 1\rangle$.

Alternatively, we can view the isomorphism $\mathrm{GI}(F) \cong \mathrm{I}(F)$ as telling us that we have a pullback square of commutative rings

$$\begin{array}{ccc} \mathrm{GW}(F) & \xrightarrow{\dim} & \mathbb{Z} \\ \downarrow & & \downarrow \\ \mathrm{W}(F) & \xrightarrow[\dim_0]{} & \mathbb{Z}/2\mathbb{Z}. \end{array}$$

Applying Spec turns this into a pushout square in which $\mathrm{Spec}\,\mathrm{W}(F)$ and $\mathrm{Spec}\,\mathbb{Z}$ are glued together at their characteristic 2 primes. □

Remark 6.13. We can think of $\mathrm{Spec}\,\mathrm{GW}(F)$ as an X_F^*-indexed bouquet of copies of $\mathrm{Spec}\,\mathbb{Z}$, all glued together at the prime (2).

We conclude by mentioning an elaboration of Pfister's local-global principle. One can show that for an F-quadratic form q, the map $\hat{q} : X_F \to \mathbb{Z}$ taking $\alpha \mapsto \mathrm{sgn}_\alpha(q)$ is continuous (*i.e.*, locally constant). It follows that the image of the total signature homomorphism $\mathrm{sgn} : \mathrm{W}(F) \to \prod_{X_F} \mathbb{Z} = \mathbb{Z}^{X_F}$ actually lands in the set of continuous functions $C(X_F, \mathbb{Z})$ from X_F to $\mathbb{Z}$.

Theorem 6.14. *If we view* sgn *as a map* $\mathrm{W}(F) \to C(X_F, \mathbb{Z})$*, then its kernel and cokernel are* 2*-primary torsion groups with* $\ker(\mathrm{sgn}) = \mathrm{W}_{\mathrm{tors}}(F)$.

The new content here is the cokernel portion of the statement. We can deduce that, as an Abelian group, $\mathrm{W}(F) \cong \mathrm{W}_{\mathrm{tors}}(F) \oplus G$, where G is a free Abelian group with rank matching that of $C(X_F, \mathbb{Z})$. Also note that upon inverting 2 we get an isomorphism $\mathrm{W}(F)[1/2] \cong C(X_F, \mathbb{Z}[1/2])$.

7. Research questions

There are a lot of exciting new questions we can ask about GW when we think of it as a Tambara functor. The following subsections outline several projects we can attack.

7.1. **Computations.** Given an explicit Galois extension $F \subseteq E$, we can attempt to explicate all of the restriction, transfer, and norm maps in the associated Tambara functor GW. By material presented in Angélica's lectures, we know it suffices to determine these maps on subextensions $F \subseteq K \subseteq L \subseteq E$ along with certain exponential diagram data. We can hope to make such a computation explicit as long as we know the structure of $\mathrm{Gal}(E/F)$ and $\mathrm{GW}(K)$ for each $K \in \mathrm{Sub}(F \subseteq E)$. Our first example should be $\mathbb{R} \subseteq \mathbb{C}$, and the result should be isomorphic to the Burnside Tambara functor of C_2. A more interesting example would be the algebraic closure of a finite field, $\mathbb{F}_q \subseteq \overline{\mathbb{F}}_q$. If we succeed at this, we might look at the algebraic closure of a local field (such as $\mathbb{Q}_p \subseteq \overline{\mathbb{Q}}_p$).

An important lemma in any such computations would likely be a formula for the norm of a binary form. See Exercise 4.6, which includes Wittkop's formula for quadratic extensions. I do not believe that any formulas for proper nonquadratic extensions are known. Note, though, that a general addition formula in Tambara functors is given in Section 4 of Tambara's *On multiplicative transfer*, and it should be able to specialize this result to GW. There are also some interesting formulas in Section 1.4.1 of Kristen Mazur's thesis and Section 2 of Hill–Mazur, *An equivariant tensor product on Mackey functors*.

7.2. **Prime ideals.** By work of Nakaoka, quotient Tambara functors of GW correspond to Tambara ideals in GW. Distinguished amongst these are the prime Tambara ideals, the collection of which is called the *Tambara spectrum* of GW. Determine the Tambara spectrum of GW and its relation to the Zariski spectrum of classical prime ideals $\operatorname{Spec} \mathrm{GW}(F)$. What can we say about non-prime Tambara ideals of GW?

In a purely equivariant direction, we could also try to determine the Tambara spectrum of the Burnside functor. By work of Nakaoka, this is known when the group of equivariance is C_{p^n}, p prime. As a first case, we might consider cyclic groups which are not p-primary.

7.3. **The Dress map.** For a profinite group G, let $\hat{A}$ denote the Dress–Siebeneicher Burnside Tambara functor. For a Galois extension $F \subseteq E$ with Galois group G, there is a natural homomorphism of Tambara functors $D : \hat{A} \to \mathrm{GW}$ called the *Dress map*. For $K \in \mathrm{Sub}(E \subseteq F)$, we know that $K = E^U$ for some open subgroup $U \leq G$. Then $\hat{A}(G/U) \to \mathrm{GW}(K)$ is the map taking $U/V \mapsto \mathrm{tr}_{K \subseteq E^V} \langle 1 \rangle_{E^V}$ for $V \leq U$ open. The map D is surjective level-wise with kernel called the *trace ideal* T. This is a Tambara ideal in $\hat{A}$ about which little is known. Previously, T has only been studied using Mackey functor structure (in fact, we should write a proof that D respects norms), but perhaps we can say more by invoking the Tambara structure.

This project connects with the previous one since a surjection of Tambara functors $A \to B$ induces an open embedding $\operatorname{Spec} B \to \operatorname{Spec} A$. What is $\operatorname{Spec} \hat{A}$, and how does $\operatorname{Spec} \mathrm{GW}$ sit inside of it?

FIGURE 7. Andreas Dress, b.1938. Dress received his PhD from the University of Kiel in 1962. His early contributions were in representation theory where he first introduced the notion of a Mackey functor. Dress currently studies computational biology and phylogenetic combinatorics.

APPENDIX A. SOME FIELD AND GALOIS THEORY

Below we review splitting fields, minimal polynomials, separable and Galois extensions, the Galois correspondence, and some Galois group computations. As a reference and learning tool, I highly recommend Keith Conrad's field and Galois theory expository notes, available here.

A.1. **Splitting fields.** For a field F, take $f \in F[t]$ a nonconstant polynomial with coefficients in F. Since $F[t]$ is a unique factorization domain, $f = \prod_{i=1}^{d} f_i$ with each $f_i \in F[t]$ irreducible. Set $F_0 := F$ and define $F_1 := F_0[t]/(f_1)$. The inclusion of coefficients $F_0 \to F_1$ makes F_1 a field extension of F_0. Let $\alpha_1 = t + (f_1)$. Then $f_1(\alpha_1) = 0 \in F_1$, hence $f(\alpha_1) = 0 \in F_1$. Thus $f(t) = (t - \alpha_1)g(t)$ for some $g \in F_1[t]$. This g has a factorization into irreducible polynomials in $F_1[t]$, and we may repeat the process to form $F_2 := F_1[t]/(g_1) \cong F_1(\alpha_2) = F(\alpha_1, \alpha_2)$. Continuing inductively, we create a chain of fields $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n$ with $F_i \cong F(\alpha_1, \ldots, \alpha_i)$. The process terminates once f factors as a product of linear polynomials in F_n. We call F_n a *splitting field* for f over F.

Theorem A.1. *Let F be a field and $f \in F[t]$ be nonconstant. If E, E' are splitting fields for f over F, then $[E : F] = [E' : F]$, there is a field isomorphism $E \to E'$ fixing F pointwise, and the number of such isomorphisms $E \to E'$ is $[E : F]$.*

A nice inductive proof may be found here.

A.2. **Minimal polynomials.** Let $F \subseteq E$ be a field extension and take $\alpha \in E$. The *minimal polynomial* of α over F is the monic[8] polynomial of least degree in $F[t]$ with α as a root. It should be clear that the monic and minimal degree conditions guarantee that the minimal polynomial is unique.

Proposition A.2. If m_α is the minimal polynomial of α over F, then m_α is irreducible in $F[t]$.

Proof. If we could factor m_α, then one of its factors would have α as a root and have smaller degree than m_α, a contradiction. □

When $f \in F[t]$ is nonconstant and irreducible, $F[t]/(f)$ is a field. We write $F(\alpha) := F[t]/(m_\alpha)$ for m_α the minimal polynomial of α over F. Note that $[F(\alpha) : F] = \deg m_\alpha$, and that a basis for $F(\alpha)$ as an F-vector space is given by $1, \alpha, \alpha^2, \ldots, \alpha^{\deg(m_\alpha)-1}$. If $m_\alpha(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$, then the fact that $m_\alpha(\alpha) = 0$ allows us to write

$$\alpha^n = -a_0 - a_1\alpha - a_2\alpha^2 - \cdots - a_{n-1}\alpha^{n-1}$$

and we can think of this as a "rewrite rule" for powers of α larger than $n - 1$.

A.3. **Separable extensions.** There are several related concepts that go under the name "separable."

Definition A.3. A nonzero polynomial $f \in F[t]$ is *separable* when it has distinct roots in a splitting field over K. If f has a multiple root, we call f *inseparable*.

Definition A.4. For a field extension $F \subseteq E$, an algebraic element $\alpha \in E$ is *separable over* F when its minimal polynomial over F is separable; otherwise, α is called *inseparable over* F.

Theorem A.5. *A nonzero polynomial in $f \in F[t]$ is separable if and only if f and f' (the formal derivative of f) are relatively prime in $F[t]$.*

Exercise A.6. Fix $a \in F^\times$ and use the theorem to prove that $x^n - a \in F[t]$ is separable if and only if $n \neq 0 \in F$. (The final condition is equivalent to $\operatorname{char} F \nmid n$.)

Definition A.7. A finite extension $F \subseteq E$ is *separable* if every element of E is separable over F; otherwise the extension is *inseparable*.

Theorem A.8. *Let $F \subseteq E$ be a finite extension with $E = F(\alpha_1, \ldots, \alpha_r)$. Then $F \subseteq E$ is separable if and only if each α_i is separable over F.*

Theorem A.9 (Primitive element theorem)**.** *Any finite separable extension of F is of the form $F(\alpha)$ for some α.*

Theorem A.10. *An extension $F \subseteq E$ is separable if and only if $\operatorname{Tr}_{E/F}$ is not the constant function 0.*

A.4. **Normal and Galois extensions.** We need a condition beyond separability in order to have a Galois extension.

Definition A.11. An algebraic extension $F \subseteq E$ is *normal* if every irreducible polynomial in $F[t]$ with a root in E splits completely in $E[t]$.

[8] A polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is *monic* when $a_n = 1$. When $a_n \neq 0$, we call it the *leading coefficient*, so we can also say that monic polynomials are those with leading coefficient 1.

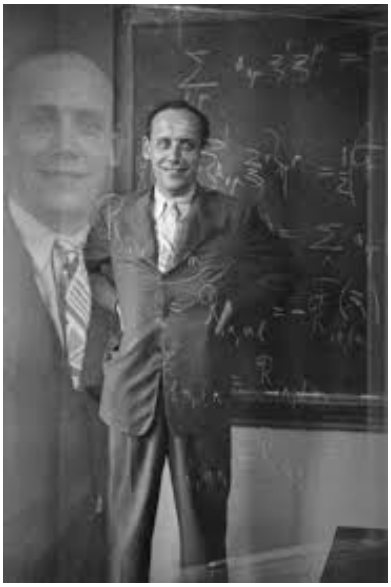


FIGURE 8. Emil Artin, 1898–1962. Born in Austria, Artin made essential contributions to algebraic number theory, especially class field theory and L-functions. His 1944 exposition of Galois theory was the first such text in English and remains extremely influential. He was a vocal opponent of the Nazi regime and was forced out of his position at the University of Hamburg in 1937 because his wife was half Jewish. He emigrated to the U.S., taking positions at Notre Dame and then Princeton. He moved back to Germany in 1957.

There are plenty of separable, non-normal extensions, *e.g.*, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$. The polynomial $t^3 - 2$ is irreducible over $\mathbb{Q}$ and has the root $\sqrt[3]{2}$ in $\mathbb{Q}(\sqrt[3]{2})$, but is missing the roots $e^{2\pi i/3}\sqrt[3]{2}$ and $e^{4\pi i/3}\sqrt[3]{2}$.

Definition A.12. An algebraic field extension $F \subseteq E$ is a *Galois extension* if it is normal and separable.

If $F \subseteq E$ is Galois, then every $\alpha \in E$ has separable minimal polynomial which splits completely in E.

A.5. **The Galois correspondence.** Galois theory is essentially the study of automorphisms of Galois extensions. For a general field extension $F \subseteq E$, we define $\mathrm{Aut}(E/F)$ to be the collection of field homomomorphisms (necessarily isomorphisms) $E \to E$ that fix F pointwise. If $[E : F] = n < \infty$, then it is also the case that $|\mathrm{Aut}(E/F)| \leq n$.

Theorem A.13 (Emil Artin)**.** *A finite extension $F \subseteq E$ of degree n is Galois if and only if $|\mathrm{Aut}(E/F)| = n$ if and only if E is a splitting field of a separable polynomial with coefficients in F.*

We have already discussed the Galois correspondence in the main text, but recall that for $F \subseteq E$ a finite Galois extension we have inverse bijections

$$\begin{aligned} \mathrm{Sub}(F \subseteq E) &\leftrightarrows \{H \leq G\} \\ K &\mapsto \mathrm{Gal}(G/K) \\ E^H &\hookleftarrow H. \end{aligned}$$

Example A.14. Fix $a \in F^\times \smallsetminus F^{\boxtimes}$ and set $E = F(\sqrt{a})$. Clearly $\sqrt{a}$ is a root of $t^2 - a = (t - \sqrt{a})(t + \sqrt{a})$, and this polynomial is separable as long as $\mathrm{char}\, F \neq 2$. Thus E is a separable field extension of degree 2 (since $t^2 - a$ has degree 2 and is the minimal polynomial of $\sqrt{a}$). Also observe that the assignment $\overline{(\,)} : E \to E$ taking $x + y\sqrt{a} \mapsto x - y\sqrt{a}$ is in $\mathrm{Aut}(E/F)$, so $|\mathrm{Aut}(E/F)| = 2 = [E : F]$. We conclude that $F \subseteq E$ is Galois with Galois group $\{\mathrm{id}, \overline{(\,)}\} \cong C_2$. The corresponding lattice of subgroups / subextensions is $e \subseteq C_2$ / $E \supseteq F$.

Example A.15. Let $q = p^m$ be a prime power and consider the field extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$. The Frobenius map $\mathrm{Frob}_q : x \mapsto x^q$ is an element of $\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ and in fact

$$\mathrm{id}, \mathrm{Frob}_q, \mathrm{Frob}_{q^2}, \ldots, \mathrm{Frob}_{q^{n-1}}$$

are all distinct elements of this group. Since $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, we conclude that $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$ is a Galois extension with Galois group $\langle \mathrm{Frob}_q \rangle \cong C_n$. The corresponding lattices of subgroups / subextensions are the same as the divisibility poset for n (or its dual).

Keith Conrad has written down several explicit examples of the Galois correspondence here.

REED COLLEGE
E-mail address: ormsbyk@reed.edu