ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 17, Number 1, Winte 1987

THE ARITHMETIC RING AND THE KUMMER RING OF A COMMUTATIVE RING

D. K. HARRISON

The Witt ring of a commutative ring is a functorial construction which: (1) gives a commutative ring for a commutative ring; (2) has nontrivial value at the field $\mathbf{Q}$, or at any number field; and (3) has value at $\mathbf{Q}$, or a number field, which is equivalent to a basic circle of successful ideas from classical number theory (see [5] and its references). The purpose of this note is to package another problem of classical number theory in this way.

We begin with a general construction, then define what we call the "Kummer ring", $K(R)$, and finally define what we call the "arithmetic ring", $A(R)$. For the special case of R a field whose multiplicative group has an element of order n, for all positive integers n, $A(R)$ is naturally isomorphic to $K(R)$, by the Merkurev-Suslin theorem ([6]). We use "ring" (respectively "ring homomorphism") to mean "ring with one" (respectively "ring homomorphism taking one to one").

Let m be a nonnegative integer.

Let X, Y, Z be functors from the category of commutative rings to the category of $(\mathbf{Z}/m\,\mathbf{Z})$-modules. For each commutative ring R, suppose we have a $(\mathbf{Z}/m\,\mathbf{Z})$-bilinear map

$$\phi_R\colon X(R) \times Y(R) \to Z(R)$$

which is functorial in R. By this we mean, if $f : R \to k$ is a homomorphism of commutative rings, then

$$Z(f)\,(\phi_R(x, y)) = \phi_k(X(f)(x),\ Y(f)(y)),$$

for all $x \in X(R)$, $y \in Y(R)$. First let $m = 0$. We define $M(R)$ to be

$$\mathbf{Z} \times X(R) \times Y(R) \times Z(R).$$

We define operations on $M(R)$ by

$$(n_1, x_1, y_1, z_1) + (n_2, x_2, y_2, z_2) = (n_1 + n_2, x_1 + x_2, y_1 + y_2, z_1 + z_2 + \phi_R(x_1, y_2) + \phi_R(x_2, y_1)),$$

Received by the editors on February 20, 1985.

$$(n_1, x_1, y_1, z_1) \cdot (n_2, x_2, y_2, z_2) = (n_1n_2,\ n_1x_2 + n_2x_1,\ n_1y_2 + n_2y_1,$$
$$n_1(n_1 - 1)\psi_R(x_2, y_2) + n_2(n_2 - 1)\psi_R(x_1, y_1) + (n_1n_2 + 1)\psi_R(x_1, y_2)$$
$$+ (n_1n_2 + 1)\psi_R(x_2, y_1)).$$

THEOREM 1. *With the above notation, $M(R)$ is a commutative ring. Also, $M(R)$ is functorial in R.*

PROOF. Define

$$V = V(R) = X(R) \oplus Y(R),$$
$$\phi: V \times V \to Z(R)$$

by $\phi((x_1, y_1), (x_2, y_2)) = \psi_R(x_1, y_2) + \psi_R(x_2, y_1)$. One checks that ϕ is biadditive and symmetric. Define

$$P = P(R) = V \times Z(R),$$
$$(v_1, z_1) + (v_2, z_2) = (v_1 + v_2, z_1 + z_2 + \phi(v_1, v_2)),$$
$$(v_1, z_1) \cdot (v_2, z_2) = (0, \phi(v_1, v_2)).$$

One checks a commutative prering (i.e., ring not necessarily with one) results and $n(v, z) = (nv, nz + (n(n - 1)/2)\phi(v, v))$, for all $n \in \mathbf{Z}$, $v \in V$, $z \in Z(R)$. One adjoins an identity in the usual fashion to get $M(R)$. Now let $f : R \to k$ be a homomorphism of commutative rings. Define

$$V(f) : V(R) \to V(k)$$

by $V(f)(x, y) = (X(f)(x), Y(f)(y))$. Define

$$P(f) : P(R) \to P(k)$$

by $P(f)(v, z) = (V(f)(v), Z(f)(z))$. Define

$$M(f) : M(R) \to M(k)$$

by $M(f)(n, w) = (n, W(f)(w))$. One checks that $M(f)$ is a ring homomorphism and that $k = R$ and $f = 1$ imply $M(f)$ is the identity map. If $t : k \to S$ is a homomorphism of commutative rings, one checks $M(t) \circ M(k) = M(t \circ k)$. The Theorem is proven.

We call the ring $M(R)$ of Theorem 1, the first version of the construction ring of $X(R)$, $Y(R)$, $Z(R)$, and ψ_R. We now define a second version, which it a little easier to work with because it does not involve ψ_R in the addition. $M(R)$ is the same set, but the operations are defined by

$$(n_1, x_1, y_1, z_1) + (n_2, x_2, y_2, z_2) = (n_1 + n_2, x_1 + x_2, y_1 + y_2, z_1 + z_2),$$

$$(n_1, x_1, y_1, z_1) \cdot (n_2, x_2, y_2, z_2) = (n_1n_2,\ n_1x_2 + n_2x_1,\ n_1y_2 + n_2y_1,$$
$$n_1z_2 + n_2z_1 + \psi_R(x_1, y_2) + \psi_R(x_2, y_1).$$

THEOREM 2. *With the above notation $M(R)$ is a commutative ring. Also, $M(R)$ is functorial in R.*

PROOF. This is easily checked along the lines of the proof to Theorem 1.

Let R be a commutative ring. Write $U(R)$ for the units of R and $S(R)$ for the set $\{\alpha \in U(R) \mid 1 - \alpha \in U(R)\}$. The permutation group S_3, has a natural action on $S(R)$ defined by

$$(12) \cdot \alpha = \alpha^{-1}, \qquad (23) \cdot \alpha = 1 - \alpha.$$

We write $D(R)$ for

$$(U(R) \otimes_{\mathbf{Z}} U(R) \otimes_{\mathbf{Z}} (\mathbf{Q}/\mathbf{Z}))/\mathrm{rel}(R),$$

where $\mathrm{rel}(R)$ is the subgroup generated by all $\alpha \otimes (23) \cdot \alpha \otimes (1/n+\mathbf{Z})$, for $\alpha \in S(R)$, n a positive integer. Note we are being forced to write $U(R)$ additively. Write ϕ_R for the natural map

$$\phi_R\colon U(R) \times (U(R) \otimes_{\mathbf{Z}} (\mathbf{Q}/\mathbf{Z})) \to D(R).$$

The second version construction ring of $U(R)$, $U(R) \otimes_{\mathbf{Z}} (\mathbf{Q}/\mathbf{Z})$, $D(R)$, and ϕ_R, is what we call the Kummer ring of R and denote by $K(R)$.

The arithmetic ring is more subtle. Write $T(R)$ for the abelian group $T(\mathbf{Q}/\mathbf{Z}, R)$ of **[2]**. $T(R)$ is functorial in R, and if R is a field, then the finite subgroups of $T(R)$ correspond bijectively with the finite Galois field extensions $\sigma\colon R \to K$ (up to isomorphism) which have abelian Galois groups, by σ goes to $\ker(T(\sigma))$. Write $B(R)$ for the Brauer group of R **[1]**. Let

$$\alpha \in U(R), \qquad y = [G, [A] \in T(R).$$

Then G is a finite subgroup of $\mathbf{Q}/\mathbf{Z}$, and A is a Galois $(G-R)$-extension. Let n be the cardinality of G, and write σ for

$$1/n + \mathbf{Z} \in \mathbf{Q} / \mathbf{Z}$$

which is a canonical generator of G. Write (σ, A, α) for the cyclic algebra

$$\sum Au^i,$$

where $i = 0, \ldots, n-1$, $u^n = \alpha \cdot u^0$, $u \cdot a = \sigma(a) \cdot u$, and write $\Psi_R(\alpha, y)$ for its Brauer class in $B(R)$. A long check gives that Ψ_R is biadditive and functorial in R. The construction ring of $U(R)$, $T(R)$, $B(R)$, and Ψ_R (second version) is what we call the arithmetic ring of R and denote by $A(R)$. For m a nonnegative integer, we replace $\mathbf{Z}$, $U(R)$ by $(\ \ )/m(\ \ )$ and $T(R)$, $B(R)$ by $(\ \ )_m$ to get $A(m, R)$.

In the definition of $K(R)$ replace $\mathbf{Z}$, $U(R)$ by $(\ \ )/m(\ \ )$, and with $D(R)$ make the obvious adjustment, to get $K(m, R)$. If R is a field which has a primitive m-th root of 1 (all of them if $m = 0$), then by **[6]** the natural isomorphisms of Kummer theory and of algebraic K-theory give a ring isomorphism between $K(m, R)$ and $A(m, R)$. This is natural, but rather complicated, so in the interest of brevity we simply refer to **[6]**.

The arithmetic ring $A(R)$ has a natural ideal which we denote by $B(R)$ and which may be identified with the Brauer group of R. It also has natural ideals $I(R)$, $J(R)$, and natural group homomorphisms

$$\ln : U(R) \to I(R),$$
$$\mathrm{tn} : T(R) \to J(R),$$

with obvious natural properties. If $f : R \to k$ is a homomorphism of commutative rings, and $t \in T(R)$, we have a group homomorphism from $U(R)$ to $B(k)$ which takes u to $A(f)$ $(\ln u) \cdot (\mathrm{tn}\ t))$. Hence we have a group homomorphism

$$\phi_f\colon T(R) \to \mathrm{Hom}(U(R), B(k)).$$

If R is a number field, and f varies over all the completions of R, this can be used to characterize $T(R)$, but this is both a very long story and equivalent to a more or less standard story. We end this note with a discussion of $A(\mathbf{Q})$, $K(\mathbf{Q})$, and $W(\mathbf{Q})$. For $W(\mathbf{Q})$, we draw from page 25 of [3], which is somewhat inaccessible.

We will state $X = U(\mathbf{Q})$, $Y = T(\mathbf{Q})$ (the group of Dirichlet characters), $Z = B(\mathbf{Q})$, $\phi = \phi_{\mathbf{Q}}$ explicitly and then apply the construction of Theorem 2. We use the fact that the non identity elements of X have an action by S_3 (i.e., is the $S(R)$ defined above, for $R = \mathbf{Q}$). Let P be the set of all prime numbers. Let $P^\# = P \cup \{-1\}$ and $\mathbf{N}^*$ be the set of all positive integers. To avoid confusion we write $u(p)$ for a p in $P^\#$ when considered in X (i.e., additively). Every $x \in X$ can be written uniquely

$$x = \sum v_p(x)u(p),$$

the sum over all $p \in P^\#$, where all but finitely many of the $v_p(x)$ are 0, for $p \in P$ each $v_p(x) \in \mathbf{Z}$, and $v_{-1}(x) \in Z_2$. For each $p \in P$, $n \in \mathbf{N}^\#$,

$$U(p, n) = \{0\} \cup \{x \in X \mid x \neq 0, \quad n \leqq v_p((23) \cdot x)\}$$

is a subgroup of X (even of ker v_p in which it is of finite index). According to **[4]**, Y can be characterized by the properties that follow. Y is a direct sum of subgroups D_p, one for each $p \in P$. For each $p \in P$ we have an infinite strictly increasing sequence

$$G(p, 1) \subset G(p, 2) \subset G(p, 3) \subset \cdots$$

of finite subgroups of D_p whose union is D_p. For each $p \in P^\#$ we have a biadditive map

$$\phi_p\colon U(\mathbf{Q}) \times Y \to \mathbf{Q}/\mathbf{Z}.$$

Furthermore:

(1) $\forall\, a \in U(\mathbf{Q})$, $\forall y \in Y$, $\psi_q(a, y) = 0$ for all but finitely many q, and

$$\sum \psi_q(a, y) = 0,$$

the sum over all $q \in P^{\#}$;

(2) $p \in P$, $d \in D_p$, $q \in P^{\#}$, $q \neq p$, $a \in \ker v_q$ imply

$$\psi_q(a, d) = 0;$$

(3) $p \in P$, $a \in \ker v_p$, $n \in \mathbf{N}^*$, imply

$$\psi_p(a, d) = 0 \quad \forall\, d \in G(p, n)$$

if and only if $a \in U(p, n)$; and

(4) $p \in P$, $d \in D_p$, $n \in \mathbf{N}^*$, imply

$$\psi_p(a, d) = 0 \quad \forall\, a \in U(p, n)$$

if and only if $d \in G(p, n)$.

For $p \in P^{\#}$, if $p = -1$, then write $(\mathbf{Q}/\mathbf{Z})_p$ for $\{0 + \mathbf{Z}, 1/2 + \mathbf{Z}\}$, and otherwise write $(\mathbf{Q}/\mathbf{Z})_p$ for $\mathbf{Q}/\mathbf{Z}$. $B(\mathbf{Q})$ is the set of all $b = (\ldots, b_p, \ldots)$ in the direct sum of the $(\mathbf{Q}/\mathbf{Z})_p$ such that $\sum b_p = 0$. For $a \in U(\mathbf{Q})$, $y \in Y$, one checks that

$$(\ldots, \psi_p(a, y), \ldots)$$

is in $B(\mathbf{Q})$; this is $\psi(a, y)$.

Using the theorem on page 101 of [7], one checks $D(\mathbf{Q}) = 0$. $U(\mathbf{Q})$, we have discussed above, and

$$U(\mathbf{Q}) \otimes_{\mathbf{Z}} (\mathbf{Q}/\mathbf{Z})$$

is obvious from it. Hence $K(\mathbf{Q})$ is obvious.

Let M (respectively N) be the set of all finite sets of prime numbers (respectively, of odd prime numbers). With symmetric difference both M and N are abelian groups, isomorphic respectively to

$$\mathbf{Z}_2 \otimes_{\mathbf{Z}} (\ker v_{-1}), \qquad \mathbf{Z}_2 \otimes_{\mathbf{Z}} (\ker v_{-1} \cap \ker v_2).$$

For $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_m\} \in M$, write $[A, B]$ for

$$\{p \in P \mid p \neq 2, (a_1 \ldots a_n, b_1 \ldots b_m; p) = -1\},$$

where (, ;) is the Hilbert symbol. Define operations on $M \times N$ by

$$(A, A') + (B, B') = (A + B, A' + B' + [A, B]),$$
$$(A, A') \cdot (B, B') = (\varnothing, [A, B]).$$

Let $\mathbf{Z} \times M \times N$ be the usual adjunction of a one; this is $W(\mathbf{Q})$. For $a \in U(\mathbf{Q})$, let

$$A(a) = \{p | v_p(a) \text{ is odd}\};$$

if $0 < a$, then $\langle a \rangle = (1, A(a), [A(a), A(a)])$ and $\langle -a \rangle = (-1, A(a), \phi)$.

REFERENCES

1. M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409.

2. D. K. Harrison, *Abelian extensions of commutative rings*, Mem. Amer. Math Soc. **52** (1965), 1–14.

3. ———: *Witt Rings*, Dept. of Math., U. of Kentucky, 1970.

4. ———: *The multiplicative rationals*, to appear in J. of Algebra.

5. M. Knebusch, *Grothendieck- und Wittringe von nicht ausgearteten symmetrischen Bilinearformen*, Sitzber. Akad. Wiss. **3**. Abh. (1969/70), 93–157.

6. A. S. Merkurev and A. A. Suslin, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism* (Russian), Izv. Akad. Nauk. S.S.S.R. Ser. Mat. **46** (1982), 1011–1046, 1135–1136.

7. J. Milnor, *Introduction to Algebraic K-theory*, Princeton, 1971.

UNIVERSITY OF OREGON, EUGENE, OR 97403