PACIFIC JOURNAL OF MATHEMATICS
Vol. 42, No. 3, 1972

A SEPARABLY CLOSED RING WITH NONZERO TORSION PIC

ANDY R. MAGID

We give an example of a ring and a rank one projective module over that ring such that the square of the module is free but the module does not become free over any separable extension of the ring.

Every ideal class in the ring of integers in a number field can be split by an unramified extension. Over a commutative ring which is an algebra over the rationals every torsion element of Pic of the ring is split by a separable extension [3]. These examples suggest the question: is the torsion part of Pic of a separably closed ring trivial? We will exhibit a ring which shows the answer is negative. The ring arises as a slight modification of an example of Swan [5].

For any commutative ring k, k^X denotes the group of units of k, $\mathrm{Cl}\,(k)$ denotes the divisor class group if k is a domain, and $Qu(k)$ denotes the group of quadratic extensions of k. We use Z for the integers and Q for the rationals.

DEFINITION. For any commutative ring k, let $k(S^1) = k[X_0, X_1]/(X_0^2 + X_1^2 - 1)$. Let t_i be the image of X_i in $k(S^1)$. $k(S^1)$ is graded mod 2; let $k(P^1)$ be the even graded piece and $L(k)$ the odd.

LEMMA 1. *$L(k)$ is a projective $k(P^1)$-module of rank 1 whose tensor square is free.*

Proof. It suffices to check the first assertion for $k = Z$. By the argument in [5, p. 271] $L(Z)$ is projective of rank 1. The multiplication in $k(S^1)$ defines a homomorphism

$$L(k) \otimes_{k(P^1)} L(k) \rightarrow k(P^1)$$

whose image contains $t_0^2 + t_1^2 = 1$ and is thus an isomorphism.

We will show that $L(Z)$ cannot be split by a separable extension of $Z(P^1)$. We begin by collecting some facts about the rings involved.

LEMMA 2. (a) *$Q(i)(P^1) = Q(i)[v, v^{-1}]$ where $v = (t_0 + it_1)^2$*
(b) $Q(P^1)^X = Q^X$
(c) *$Z/2Z(P^1)$ is a polynomial ring (in one variable) over $Z/2Z$*
(d) *$L(Z/2Z)$ is freely generated by $t_0 + t_1$*

Proof. Let $K = Q(i)$. Then $K(S^1) = K[u, u^{-1}]$ where $u = t_0 + it_1$.

$K[v, v^{-1}]$ is contained in $K(P^1)$ and $K[u, u^{-1}]$ is separable of rank two over both rings. Thus $K[v, v^{-1}] = K(P^1)$; this gives (a). Let g be the automorphism of $K(P^1)$ defined by $g(i) = -i$ (so $g(v) = v^{-1}$). Then the ring of g-invariants is $Q(P^1)$. Since $K(P^1)^X = K^X\{v\}$, the only invariant units are in Q^X, whence (b). For (c), we observe that $Z/2Z[X_0, a]$ where $a^2 = 1$ is isomorphic to $Z/2Z(S^1)$ when X_0 is sent to t_0 and a to $t_0 + t_1$. This isomorphism is graded and under it, $Z/2Z(P^1)$ corresponds to $Z/2Z[X_0, a]$. For (d), let $f_i = t_i(t_0 + t_1)$. Then $f_i(t_0 + t_1) = t_i$, so $t_0 + t_1$ generates $L(Z/2Z)$.

We remark that (c) implies that $Z/2Z(P^1)^X = \{1\}$ and (b) implies that $Z(P^1)^X = \{\pm 1\}$.

PROPOSITION 3. *$Z(P^1)$ is a normal domain with* Pic $(Z(P^1)) = \{1, L(Z)\}$.

Proof. We begin by establishing analogous assertions for $Q(P^1)$. Let K, v, g be as in the proof of Lemma 2 and let $G = \{1, g\}$. Then $K(P^1)$ is a Galois extension of $Q(P^1)$ with group G. Let $U = X(P^1)^X$. Since by Lemma 2 (a) $K(P^1)$ is a UFD, $Q(P^1)$ is normal and there is an isomorphism $\mathrm{Cl}\,(Q(P^1)) \rightarrow H^1(G, U)$ [4, p. 55]. To compute the latter group, we use the exact sequence of G-modules

$$1 \longrightarrow V \longrightarrow U \longrightarrow K^X \longrightarrow 1$$

where V is the subgroup generated by v. Since by Lemma 2 (b) $U^G = Q^X = (K^X)^G$ and since $H^1(G, K^X) = 1$ by Hilbert's Theorem 90, the cohomology sequence of the above sequence shows that $H^1(G, U)$ and $H^1(G, V)$ are isomorphic. Since V is G-isomorphic with Z with g acting by multiplication by -1, we see that $H^1(G, V)$ (and hence $\mathrm{Cl}\,(Q(P^1))$) is of order two. Now let S be the multiplicative set in $Z(P^1)$ generated by the integer primes. The integer primes remain prime in $Z(P^1)$ (for the odd primes this is trivial and for two it follows from Lemma 2 (c)). Since $S^{-1}Z(P^1) = Q(P^1)$ it follows from [4, p. 21] that $Z(P^1)$ is a normal domain with $\mathrm{Cl}\,(Z(P^1)) = \mathrm{Cl}\,(Q(P^1))$. By [5, Thm. 4, p. 271] $L(Z)$ cannot be generated by a single element. It follows that $\{1, L(Z)\} = \mathrm{Pic}\,(Z(P^1)) = \mathrm{Cl}\,(Z(P^1))$.

Next, we show that every connected Galois extension of $Z(P^1)$ is abelian.

LEMMA 4. *Let K be an algebraically closed field of characteristic zero. Then every connected Galois extension of $K[X, X^{-1}]$ is cyclic.*

Proof. We may assume K is the complex numbers. Let T be a connected Galois extension of $K[X, X^{-1}]$ and let E be the quotient field of T. Let M and P be the Riemann surfaces of E and $K(X)$

respectively (P is just the Riemann sphere, of course). The inclusion of $K(X)$ in E displays M as a local branched covering of P ramified only above 0 and ∞. The branching order formula [3, Cor. 3, p. 225] shows that M has genus zero and only one branch point over each of 0 and ∞. It follows that the covering map is the n^{th} power map, where $n = [T: K[X, X^{-1}]]$ and hence that $T = K[X, X^{-1}](\sqrt[n]{X})$. Then the Galois group of T is cyclic of order n.

PROPOSITION 5. *Every connected Galois extension of $Z(P^1)$ is cyclic.*

Proof. Let K be the algebraic closure of Q and R the ring of all algebraic integers. Let T be a connected Galois extension of $Z(P^1)$ with group G. Then $T \otimes_Z R$ is a Galois extension of $R(P^1)$, and hence is a product of copies of a connected Galois extension T_0 of $R(P^1)$. The Galois group H of T_0 is a subgroup of G. $T_0 \otimes_R K$ is a connected Galois extension of $K(S^1) = K[v, v^{-1}]$ and hence by Lemma 4 H is cyclic. Choose a homomorphism (necessarily an injection) of T into T_0. Then T^H is a separable $Z(P^1)$-subalgebra of $T_0^H = R(P^1)$. Thus T^H is contained in $S(P^1)$ where S is the ring of integers in some finite extension of Q. Since $S(P^1)$ is $Z(P^1)$-projective and T^H is $Z(P^1)$-separable, T^H is a T^H-summand of $S(P^1)$. Let f denote the evaluation $Z(S^1) \to Z$ (and also its restriction to $Z(P^1)$) at the point (1, 0). Then $T^H \otimes_f Z$ is a separable Z-subalgebra of $S(P^1) \otimes_f Z = S$. It follows that $T^H \otimes_f Z = Z$ and hence $Z(P^1) = T^H$.

THEOREM 6. *$L(Z)$ cannot be split by a separable extension of $Z(P^1)$.*

Proof. It will suffice to prove the theorem for connected Galois extensions; let T be such an extension with group G. If T splits $L(Z)$ then by Lemma 3 $\text{Pic}(Z(P^1)) = H^1(G, T^X)$. It follows that G has even order. Since by Proposition 5 G is cyclic, it will suffice to show that $Z(P^1)$ has no connected quadratic extensions. Since for any normal domain k with quotient field L the map $Qu(k) \to Qu(L)$ is injective, $Qu(Z(P^1))$ is contained in $Qu(Q(P^1))$. To compute this latter group, we use the exact sequence of [1, p. 129] valid for any ring k containing 1/2:

$$1 \longrightarrow k^X/(K^X)^2 \longrightarrow Qu(k) \longrightarrow 2\text{-Pic}(k) \longrightarrow 1$$

where the first map sends a to $k[X]/(X^2 - a)$, the second sends T to T/k and the fourth group in the sequence is the two-torsion part of Pic. Let T be a quadratic extension of $Z(P^1)$ and let $I = T/Z(P^1)$. Let $T_0 = T \otimes_Z Q$ and let $I_0 = T_0/Q(P^1)$. If $I = 1$ and thus also $I_0 = 1$, the above exact sequence shows that $T_0 = Q(\sqrt{a})(P^1)$ for some a

in Q, since by Lemma 2 (b) $Q(P^1)^X = Q^X$. Let $f\colon Z(P^1) \to Z$ and $h\colon Q(P^1) \to Q$ be induced by evaluation at (1, 0). Then $T \otimes_f Z \otimes_z Q = T_0 \otimes_h Q$, *since the first is* $Q \times Q$ *and the second* $Q(\sqrt{a})$, a *is in* Q *and* T_0 and therefore T must be the trivial extension. To treat the case $I = L(Z)$ we use the following exact sequence, which is part of a sequence due to Small [6]: for any ring k ,

$$Qu(k) \longrightarrow \operatorname{Pic}_{(2)}(k) \longrightarrow U'(k)$$

where the middle group is those two-torsion elements of Pic (k) which become free over $k/2k$ and the end group is $(k/4k)^X$ modulo the subgroup generated by the squares and the image of k^X; the first map sends T to T/k and the second sends I to the class of $g(m, m)$ where $g\colon I \otimes_k I \to I$ is an isomorphism and m is in I with the image of m becoming a basis for $I/2I$. By Lemma 2 and the remarks following we see that $U'(Z(P^1)) = Z/4Z(P^1)^X/\{\pm 1\}$, and by Lemma 2$d$ and Proposition 3 we see that $\operatorname{Pic}_{(2)}(Z(P^1)) = \{1, L(Z)\}$. To compute the image of $L(Z)$ in $U'(Z(P^1))$ we choose for g the multiplication map (Lemma 1) and for m the element $t_0 + t_1$ (Lemma 2 (d)). Then $g(m, m) = 1 + 2t_0t_1$ has non-trivial image in $Z/4Z(P^1)$. Thus the case $I = L(Z)$ does not occur.

We conclude with some remarks: one can define $k(P^n)$ and $k(S^n)$ in a similar manner for n larger than 1. The arguments given here can be extended to cover these rings, except for Lemma 4. Presumably the *analogue of* Theorem 6 *remains valid, however.*

REFERENCES

1. H. Bass, *Lectures on Topics in Algebraic K-Theory,* Tata Institute of Fundamental Research, Bombay, 1967
2. L. Childs, *Abelian Galois extensions of rings containing roots* of unity, Illinois J. Math., **15** (1971).
3. R. Gunning, *Lectures on Riemann Surfaces,* Princeton University Press, Princeton, 1966
4. P. Samuel, *Lectures on Unique Factorization Domains,* Tata Institute of Fundamental Research, Bombay, 1964.
5. R. Swan, *Vector bundles and projective modules,* Trans. Amer. Math. Soc., **105** *(1962)*
6. C. Small, *The group of quadratic extensions* (to appear)

Received June 11, 1971 and in revised form December 9, 1971.

COLUMBIA UNIVERSITY