J. Eur. Math. Soc. 16, 1881–1913

DOI 10.4171/JEMS/478

Manjul Bhargava · Matthew Satriano

On a notion of "Galois closure" for extensions of rings

Received November 7, 2010 and in revised form August 4, 2012

Abstract. We introduce a notion of "Galois closure" for extensions of rings. We show that the notion agrees with the usual notion of Galois closure in the case of an S_n degree n extension of fields. Moreover, we prove a number of properties of this construction; for example, we show that it is functorial and respects base change. We also investigate the behavior of this Galois closure construction for various natural classes of ring extensions.

Keywords. Galois closure, ring extension, field extension, étale extension, monogenic extension, S_n-representation

1. Introduction

Let A be any *ring of rank n over a base ring B*, i.e., a B-algebra that is free of rank n as a B-module. In this article, we investigate a natural definition for the "Galois closure" $G(A/B)$ of the ring A as an extension of B.[1]

The definition is as follows. For an element $a \in A$, let

$$P_a(x) = x^n - s_1(a)x^{n-1} + s_2(a)x^{n-2} + \cdots + (-1)^n s_n(a) \tag{1}$$

be the *characteristic polynomial* of a, i.e., the characteristic polynomial of the B-module transformation $\times a : A \to A$ given by multiplication by a. Furthermore, for an element $a \in A$, let $a^{(1)}, a^{(2)}, \ldots, a^{(n)}$ denote the elements $a \otimes 1 \otimes 1 \otimes \cdots \otimes 1$, $1 \otimes a \otimes 1 \otimes \cdots \otimes 1, \ldots, 1 \otimes 1 \otimes 1 \otimes \cdots \otimes a$ in $A^{\otimes n}$ respectively. Let $I(A, B)$ denote the ideal in $A^{\otimes n}$ generated by all expressions of the form

$$s_j(a) \;-\; \sum_{1 \le i_1 < \cdots < i_j \le n} a^{(i_1)} \cdots a^{(i_j)} \tag{2}$$

where $a \in A$ and $j \in \{1, \ldots, n\}$. Note that the symmetric group S_n naturally acts on $A^{\otimes n}$ by permuting the tensor factors, and the ideal $I(A, B) \subset A^{\otimes n}$ is preserved under this

M. Bhargava: Department of Mathematics, Fine Hall, Washington Road, Princeton, NJ 08544-1000, USA; e-mail: bhargava@math.princeton.edu

M. Satriano: Department of Mathematics, University of Michigan, 2074 East Hall, Ann Arbor, MI 48109-1043, USA; e-mail: msatriano@gmail.com

Mathematics Subject Classification (2010): Primary 11R32; Secondary 13B05

[1] All rings are assumed to be commutative with unity.

S_n-action. We are interested in imposing on $A^{\otimes n}$ the relations in $I(A, B)$ defined by (2) because they are precisely the relations that the conjugates $a^{(i)}$ of a generic element a in a separable field extension of degree n would satisfy in a normal closure. Alternatively, they are the general relations that the eigenvalues $a^{(i)}$ of a linear transformation of a vector space of dimension n would satisfy.

We define

$$G(A/B) = A^{\otimes n}/I(A, B), \tag{3}$$

and we call $G(A/B)$ the *S_n-closure* of A over B. Since $I(A, B)$ is S_n-invariant, we see that the action of S_n on $A^{\otimes n}$ also descends to an S_n-action on $G(A/B)$. One easily checks (or see Theorem 2 below) that if A/B is a degree n extension of fields having associated Galois group S_n, then $G(A/B)$ is indeed simply the Galois closure of A as a field extension of B. Thus our definition of S_n-closure in a sense naturally extends the usual notion of Galois closure to rank n ring extensions.

In fact, our definition above also naturally extends to B-algebras A that are *locally free of rank n*. A B-module M is said to be locally free of rank n if there exist $b_1, \ldots, b_m \in B$ such that $\sum Bb_i = B$ and $B_{b_i} \otimes_B M$ is free of rank n over the localization B_{b_i}.[2] For such M, we have a natural isomorphism

$$M \otimes_B \mathrm{Hom}_B(M, B) \to \mathrm{End}_B(M), \tag{4}$$

where for B-modules N, N' we use $\mathrm{Hom}_B(N, N')$ to denote the set of B-module homomorphisms from N to N', and we use $\mathrm{End}_B(N)$ to denote $\mathrm{Hom}_B(N, N)$. Indeed, (4) gives an isomorphism locally on B_{b_i} (since $B_{b_i} \otimes_B M$ is free over B_{b_i}), and hence it is an isomorphism globally. Next, if f is any B-module endomorphism of M, then the trace of f is defined to be the image of f under the canonical map

$$\mathrm{Tr} : \mathrm{End}_B(M) \cong M \otimes_B \mathrm{Hom}_B(M, B) \to B.$$

Finally, if A is a B-algebra which is locally free of rank n, then given an element $a \in A$, we obtain a B-module endomorphism of A given by $\times a : A \to A$. We let $s_j(a)$ be the trace of the induced B-module endomorphism of $\bigwedge^j A$. Note that for such A, it makes sense to speak of the characteristic polynomial P_a of an element $a \in A$, and that the *Cayley–Hamilton Theorem* carries over to this setting as $P_a(a)$ is locally zero, hence globally zero. We can then define $I(A, B)$ and $G(A/B)$ as in (2) and (3).

The notion of S_n-closure has a number of interesting properties, which we consider in this article. First, we note that the S_n-closure construction is clearly functorial in A for B-algebra morphisms. The first nontrivial property that should be mentioned is that the S_n-closure construction commutes with base change:

[2] The condition that *M is locally free of rank n as a B-module* is also equivalent to either of the following two natural conditions: (a) M is finitely generated and projective of constant rank n as a B-module; (b) M is finitely presented and $M_{\mathfrak{m}}$ is free of rank n as a $B_{\mathfrak{m}}$-module for all maximal ideals $\mathfrak{m}$ of B. (See, e.g., [15, Thm. 4.6].)

Theorem 1. *If A is a ring of rank n over B, and C is a B-algebra, then there is a natural isomorphism*

$$G(A/B) \otimes_B C \simeq G((A \otimes_B C)/C)$$

of C-algebras.

Next, in the case of an extension of fields, we have

Theorem 2. *Let B be a field, and suppose A is a separable field extension of B of degree n. Let $\widetilde{A}$ be a Galois closure of A over B, and let $r = n!/\deg(\widetilde{A}/B)$. Then*

$$G(A/B) \cong \widetilde{A}^r$$

as B-algebras.

In particular, if $\deg(\widetilde{A}/B) = n!$ (i.e., $\mathrm{Gal}(\widetilde{A}/B) = S_n$), then $G(A/B) \cong \widetilde{A}$ as B-algebras.

We next consider the case where B is *monogenic* over A, i.e., A is generated by one element as a B-algebra. Then we have

Theorem 3. *Suppose A is a ring of rank n over B such that $A = B[\alpha]$ for some $\alpha \in A$. Then $G(A/B)$ is a ring of rank $n!$ over B. More generally, if A is locally free of rank n over B and is locally generated by one element, then $G(A/B)$ is locally free of rank $n!$ over B.*

Now, if B is any ring, then we may examine the ring $A = B^n$ having rank n over B. More generally, we may consider those locally free rings A of rank n that are *étale* over B, i.e., the determinant of the bilinear form $\langle a, a'\rangle = \mathrm{Tr}(aa')$—called the *discriminant* $\mathrm{Disc}(A/B)$ of A over B—is a unit in B (equivalently, the map $\Phi : A \to \mathrm{Hom}_B(A, B)$ given by $a \mapsto (a' \mapsto \mathrm{Tr}(aa'))$ is a B-module isomorphism). We prove:

Theorem 4. *For any ring B, we have $G(B^n/B) \cong B^{n!}$. If A is étale and locally free of rank n over B, then $G(A/B)$ is étale and locally free of rank $n!$ over B.*

In fact, if B has no nontrivial idempotents, we may explicitly describe the Galois set associated to $G(A/B)$ in terms of that associated to A (see Section 5).

Thus for either étale or locally monogenic ring extensions of rank n, the S_n-closure construction always yields locally free ring extensions of rank $n!$. For general rings that are locally free of small rank over a base B—even those that might not be étale or (locally) monogenic—the S_n-closure still always yields locally free rings of rank $n!$ over B:

Theorem 5. *Suppose A is locally free of rank $n \leq 3$ over B. Then $G(A/B)$ is locally free of rank $n!$ over B.*

For example, if one takes an order A in a noncyclic cubic field K, then its S_3-closure yields a canonically associated order $\tilde{A} = G(A/\mathbb{Z})$ in the sextic field $\widetilde{K}$. We will prove in Section 7 that this sextic order satisfies $\mathrm{Disc}(\tilde{A}/\mathbb{Z}) = \mathrm{Disc}(A/\mathbb{Z})^3$.

We may ask how the notion of S_n-closure behaves under general products. We prove:

Theorem 6. *If $A_1, \ldots, A_k$ are locally free rings of rank $n_1, \ldots, n_k$, respectively, over B, then*

$$G(A_1 \times \cdots \times A_k/B) \cong [G(A_1/B) \otimes \cdots \otimes G(A_k/B)]^{\binom{n}{n_1,\ldots,n_k}}. \tag{5}$$

Theorem 6 implies that if $A_1, \ldots, A_k$ are locally free rings of rank $n_1, \ldots, n_k$ over B such that each A_j has S_{n_j}-closure over B that is locally free of the expected rank $n_j!$, then the product $A = A_1 \times \cdots \times A_k$ (which is locally free of rank $n = n_1 + \cdots + n_k$ over B) also has S_n-closure that is locally free of the expected rank $n!$ over B.

One might imagine that for more complicated ring extensions, however, the analogues of the rank assertions in Theorems 3–5 might not hold. Indeed, one finds in rank 4 that there exist algebras over fields for which the S_4-closure need not have rank $4! = 24$. For instance, we will show in Section 9 that the S_4-closure of the ring $K[x, y, z]/(x, y, z)^2$ has dimension 32 over K for any field K.

This has consequences over $\mathbb{Z}$ as well. For example, suppose K is a quartic field and A is the ring of integers in K. Consider the suborder $A' = \mathbb{Z} + pA$ for some prime p. Since $A'/pA' \cong \mathbb{F}_p[x, y, z]/(x, y, z)^2$, we see already that the minimal number of generators for $G(A'/\mathbb{Z})$ as an abelian group is at least 32 by Theorem 1. Since $A' \otimes \mathbb{Q} = K$, we see that the torsion-free rank of A' is $4! = 24$, but one finds that there are also eight dimensions of p-torsion! Although this may seem unsightly at first, for a number of reasons this additional information contained in the p-torsion is important to retain in studying the "Galois closure" of the order A' (the most prominent reason being perhaps the property of commuting with base change.) We study this example more carefully in Section 10. The example will illustrate that there is no natural further quotient of $G(A'/\mathbb{Z})$ that has 24 generators as a $\mathbb{Z}$-module and also respects base change (see Theorem 20). This gives further evidence that allowing the rank to be higher than $n!$ when constructing S_n-closures can be important when considering somewhat more "degenerate" ring extensions.

Remark 7. It is possible to obtain a natural Galois closure-type object of rank $n!$ for any order A in a degree n number field K, by constructing $G(A/\mathbb{Z})$ as defined above, and then quotienting by all torsion. This quotient was used for convenience in, e.g., [2] and [3]. Although quite convenient in many contexts, such a quotienting procedure will NOT commute with base change!

It is an interesting question as to what the possible dimensions are for the S_n-closure of a dimension n algebra over a field K. In Section 11, we show that the largest possible dimensions occur for the "maximally degenerate" rank n algebra over K, namely $R_n = K[x_1, \ldots, x_{n-1}]/(x_1, \ldots, x_{n-1})^2$:

Theorem 8. *Let K be a field and $R_n = K[x_1, \ldots, x_{n-1}]/(x_1, \ldots, x_{n-1})^2$. Then for all K-algebras A of dimension n, we have* $\dim_K G(A/K) \le \dim_K G(R_n/K)$.

In addition to their interest due to Theorem 8, the algebras R_n are of interest in their own right as they arise (with $K = \mathbb{F}_p$) as the reductions modulo p of orders R in number fields that are *imprimitive* at p, i.e., $R = \mathbb{Z} + pR'$ for some order R'. For these reasons, we study the S_n-closures of these algebras in more detail in Section 12, and show:

Theorem 9. *Let K be a field of characteristic* 0 *or coprime to* $n!$*, and let $R_n = K[x_1, \ldots, x_{n-1}]/(x_1, \ldots, x_{n-1})^2$. Then the dimension of $G(R_n/K)$ over K is strictly greater than* $n!$ *for $n > 3$.*

In particular, we find for $n = 1, 2, 3, 4, 5$, and 6 that $\dim_K G(R_n/K) = 1, 2, 6, 32, 220$, and 1857 respectively. These ranks thus give the maximal possible ranks for the S_n-closures of rank n rings over K for these values of n. Theorem 9 will in fact follow from a more general structure theorem for these rings $G(R_n/K)$ (see Theorem 27). The techniques used to prove Theorem 9 are primarily those of representation theory of S_n.

As we now describe, our notion of Galois closure can also easily be adapted to the more general situation of a morphism $X \to Y$ of schemes, where $\mathcal{A}$ is a locally free sheaf of $\mathcal{O}_Y$-algebras of rank n and $X = \underline{\mathrm{Spec}}_Y\, \mathcal{A}$. We then say that X/Y is an *n-covering*.

Recall that if $\mathcal{E}$ is a locally free sheaf of rank n on a scheme Y and f is a local section of $\mathcal{E}nd(\mathcal{E})$, then the trace of f is the image of f under the canonical morphism

$$\mathcal{E}nd(\mathcal{E}) \cong \mathcal{E} \otimes_{\mathcal{O}_Y} \mathcal{E}^\vee \to \mathcal{O}_Y.$$

If X/Y is an n-covering and $\mathcal{A}$ is as above, then for any $a \in \mathcal{A}(U)$ we can define the coefficients $s_j(a)$ of the "characteristic polynomial" P_a of a as follows. We obtain an $\mathcal{O}_U$-module endomorphism of $\mathcal{A}|_U$ given by multiplication by a. We let $s_j(a)$ be the trace of the induced endomorphism of $\bigwedge^j \mathcal{A}|_U$. We can then define a sheaf of ideals $\mathcal{I}(\mathcal{A}, \mathcal{O}_Y)$ of $\mathcal{A}^{\otimes n}$ generated by the local expressions as in (2) and let

$$G(\mathcal{A}/\mathcal{O}_Y) = \mathcal{A}^{\otimes n}/\mathcal{I}(\mathcal{A}, \mathcal{O}_Y).$$

We define

$$G(X/Y) = \underline{\mathrm{Spec}}_Y\, G(\mathcal{A}/\mathcal{O}_Y).$$

Even in this more general context of n-coverings of schemes, we still have the analogues of Theorems 1, 3, 4, and 5. More precisely,

Theorem 1′. *If X/Y is an n-covering and $Z \to Y$ is a morphism of schemes, then there is a natural isomorphism*

$$G(X/Y) \times_Y Z \cong G(X \times_Y Z/Z).$$

Theorem 3′. *If X/Y is an n-covering defined by a locally free sheaf $\mathcal{A}$ of $\mathcal{O}_Y$-algebras which is locally generated as an $\mathcal{O}_Y$-algebra by one element, then $G(X/Y)$ is an $n!$-covering of Y.*

Theorem 4′. *If X/Y is an n-covering which is étale, then $G(X/Y)$ is an $n!$-covering of Y which is étale.*

Theorem 5′. *If X/Y is an n-covering defined by a locally free sheaf $\mathcal{A}$ of $\mathcal{O}_Y$-algebras and $n \leq 3$, then $G(X/Y)$ is an $n!$-covering of Y.*

Theorems 1′, 3′, 4′, and 5′ follow directly from Theorems 1, 3, 4, and 5, due to the local nature of our definitions. Hence we will concentrate primarily on the proofs of Theorems 1–9, in cases of locally free ring extensions of rank n.

We note that the notion of S_n-closure considered here arises at least incidentally or in special cases in other works. For example, it occurs in the monogenic case in Grothendieck [11, Lem. 1] and in Katz–Mazur [14, §1.8.2]. The construction for general rings is also mentioned in [6, §5.2] (comment of O. Gabber), although no properties are proven there.

We end the introduction by noting that the S_n-closure construction can also be characterized by a universal property in terms of a key notion of Katz and Mazur [14, 1.8.2]: if B is a ring and A is a B-algebra which is locally free of rank n, then B-algebra maps $p_1, \dots, p_n : A \to B$ form a *full set of sections* if for every B-algebra C and every $f \in A \otimes_B C$,

$$P_f(x) = \prod_{i=1}^{n} (x - (p_i \otimes \mathrm{id})(f)).$$

Then Theorem 1 implies:

Theorem 10. *Let B be any ring and A any B-algebra that is locally free of rank n. Then $G(A/B)$ is the universal B-algebra over which A admits a full set of n sections.*

Indeed, Theorem 1 shows that the $G(A/B)$-algebra maps $p_i : A \otimes_B G(A/B) \to G(A/B)$ defined by $p_i(a \otimes \gamma) = a_i \gamma$ form a full set of sections, where a_i denotes the image of $a^{(i)}$ in $G(A/B)$. It is then immediate from the relations (2) defining $I(A, B)$ that this family is universal.

2. S_n-closure commutes with base change

Let A be any ring of rank n over a base ring B. In this section, we show that the ideal $I(A, B)$ in $A^{\otimes n}$ is generated by the relations (2), where *a ranges over a basis of A as a module over B*. As such a basis remains a basis of $A \otimes_B C$ as a module over C for any ring C, Theorem 1 will then follow.

To prove our assertion about $I(A, B)$, we require:

Lemma 11. *Let $\mathbb{Z}\langle X, Y\rangle$ denote the noncommutative polynomial ring over $\mathbb{Z}$ generated by X and Y. Then there exists a unique sequence $f_0(X, Y)$, $f_1(X, Y), \dots$ of polynomials in $\mathbb{Z}\langle X, Y\rangle$ such that in $\mathbb{Z}\langle X, Y\rangle[[T]]$ we have*

$$1 - (X + Y)T = (1 - XT)(1 - YT) \prod_{k=0}^{\infty} (1 - f_k(X, Y)XYT^{k+2}). \tag{6}$$

Furthermore, $f_m(X, Y)$ is a homogeneous polynomial in X and Y of degree m.

Proof. We first prove by induction on m that the value of $f_m(X, Y)$ is completely determined by (6). Indeed, to see the assertion for $m = 0$, we take (6) modulo T^3 to obtain

$$1 - (X + Y)T \equiv (1 - XT)(1 - YT)(1 - f_0(X, Y)XYT^2) \pmod{T^3}$$

implying

$$1 - XT - YT \equiv 1 - XT - YT + (1 - f_0(X, Y))XYT^2 \pmod{T^3}$$

and so we must have $f_0(X, Y) = 1$.

Similarly, assuming that $f_0(X, Y), \dots, f_{m-1}(X, Y)$ have been determined from (6), the polynomial $f_m(X, Y)$ can then also be determined from (6) by taking (6) modulo T^{m+3}:

$$1 - (X + Y)T \equiv (1 - XT)(1 - YT) \prod_{k=0}^{m} (1 - f_k(X, Y)XYT^{k+2}) \pmod{T^{m+3}}; \tag{7}$$

equating the coefficients of T^{m+2} in (7) yields

$$
\begin{aligned}
&f_m(X,Y)\,XY \\
&\quad = \left[\text{coefficient of } T^{m+2} \text{ in } (1-XT)(1-YT)\prod_{k=0}^{m-1}(1-f_k(X,Y)XYT^{k+2})\right]. \qquad (8)
\end{aligned}
$$

Inspection shows that every term on the right hand side of (8) is right-divisible by XY; dividing on the right by XY on both sides of (8) now gives the desired expression for $f_m(X,Y)$.

We have shown that the sequence $\{f_m(X,Y)\}$ is uniquely determined from (6) via the recursive formula in (8). Moreover, the equation in (6) is true for this latter sequence $\{f_m(X,Y)\}$ of polynomials because it is true modulo T^i for every i. This concludes the proof. □

Remark 12. This beautiful lemma (Lemma 11) was pointed out to us by Bart de Smit. See also [1], [18] for related results.

Remark 13. The first few polynomials $f_k(X,Y)$ are given as follows:

$$
\begin{aligned}
f_0(X,Y) &= 1,\\
f_1(X,Y) &= X+Y,\\
f_2(X,Y) &= X^2+YX+Y^2,\\
f_3(X,Y) &= X^3+XYX+XY^2+YX^2+Y^2X+Y^3,\\
f_4(X,Y) &= X^4+XYX^2+XY^2X+XY^3+YX^3+Y^2X^2+Y^3X+Y^4.
\end{aligned} \qquad (9)
$$

We now return to our assertion about $I(A,B)$. Given $a\in A$, let $Q_a(T)=\det(1-aT)$ $=1-s_1(a)T+s_2(a)T^2-\cdots$ be the reverse characteristic polynomial of a. Then given any elements $x,y\in A$, by Lemma 11 we have

$$
1-(x+y)T=(1-xT)(1-yT)\prod_{n=0}^{m-2}(1-(f_n(x,y)xy)T^{n+2}) \pmod{T^{m+1}}. \qquad (10)
$$

Taking determinants of both sides of (10), and equating powers of T^m, yields an expression for $s_m(x+y)$ as an integer polynomial in $s_i(x)$ $(0\le i\le m)$, $s_i(y)$ $(0\le i\le m)$, and $s_i(g_j(x,y))$ $(0\le i\le m/2)$ for various integer polynomials g_j. When $A=B^n$, the $s_m(z)$ (where $z=(z_1,\dots,z_n)\in A$) become the m-th elementary symmetric polynomials $e_m(z_1,\dots,z_n)$ in $z_1,\dots,z_n$; thus our identities involving the s_m turn into polynomial identities in the elementary symmetric polynomials e_m in this case (indeed, since they hold with $x,y\in B^n$ for any ring B, they must hold identically as polynomial identities over the integers).

Remark 14. For example, we have:

$$
\begin{aligned}
s_1(x+y) &= s_1(x)+s_1(y),\\
s_2(x+y) &= s_2(x)+s_1(x)s_1(y)+s_2(y)-s_1(xy),\\
s_3(x+y) &= s_3(x)+s_2(x)s_1(y)+s_1(x)s_2(y)+s_3(y)+s_1(xxy)+s_1(xyy)\\
&\quad -(s_1(x)+s_1(y))s_1(xy).
\end{aligned}
$$

Since for any $b \in B$ and $k \in \mathbb{N}$ we have $s_k(bx) = b^k s_k(x)$, it follows by induction on m that the values of all expressions of the form $s_m(a)$ $(0 \le m \le n)$ for $a \in A$ are determined by the values of s_i $(i \le m)$ on a basis for A as a B-module. As the elementary symmetric polynomials e_i also satisfy these same general relations as the s_i, we conclude that the ideal $I(A, B)$ in $A^{\otimes k}$ is generated by the relations (2), where a ranges over a B-basis of A. In particular, Theorem 1 follows in the case where we are considering only ring extensions A that are free of rank n over B.

Of course, the above argument can be modified slightly to handle the case where A is locally free of rank n over B. Indeed, in this case A is still a finitely-generated B-module (see Footnote 2). The above argument then shows that $I(A, B)$ is generated by the relations (2) where a runs through any set of generators for A as a B-module. The assertion of Theorem 1 then follows in this generality as well.

3. The case $A = B^n$

3.1. A B-basis for $G(B^n/B)$

Suppose A is the rank n ring B^n over B. Let

$$e_1 = (1, 0, \dots, 0), \quad e_2 = (0, 1, \dots, 0), \; \dots, \; e_n = (0, 0, \dots, 1)$$

be the standard basis for B^n over B. As in the introduction, for $a \in A$, we let $a^{(i)}$ denote the element $1 \otimes \cdots \otimes a \otimes \cdots \otimes 1$ of $A^{\otimes n}$ with a in the i-th tensor factor. Then a natural B-basis for $(B^n)^{\otimes n}$ is given by

$$\{e_{i_1}^{(1)} \cdots e_{i_n}^{(n)}\} \tag{11}$$

where $i_1, \dots, i_n$ each range between 1 and n.

We claim that a natural B-basis for $G(B^n/B)$ is also given by (11), but where $(i_1, \dots, i_n)$ now ranges over all *permutations* of $(1, \dots, n)$.

To see this, we first note that any general element of the form $e_{i_1}^{(1)} \cdots e_{i_n}^{(n)} \in (B^n)^{\otimes n}$ such that $(i_1, \dots, i_n)$ is *not* a permutation of $(1, \dots, n)$, is in fact zero in $G(B^n/B)$. Indeed, let $i \in \{1, \dots, n\}$ be any element such that $i \notin \{i_1, \dots, i_n\}$. Then since $\sum_{j=1}^n e_i^{(j)}$ equals $\mathrm{Tr}(e_i) = 1$ in $G(B^n/B)$, we deduce

$$e_{i_1}^{(1)} \cdots e_{i_n}^{(n)} = \sum_{j=1}^n [e_i^{(j)} \cdot e_{i_1}^{(1)} \cdots e_{i_n}^{(n)}] = 0$$

in $G(B^n/B)$, as desired.

On the other hand, if $(i_1, \dots, i_n)$ is a permutation of $(1, \dots, n)$, then $e_{i_1}^{(1)} \cdots e_{i_n}^{(n)}$ is nonzero in $G(B^n/B)$. To prove this, consider the B-algebra homomorphism $\phi_{(i_1,\dots,i_n)}$: $(B^n)^{\otimes n} \to B$ defined by

$$\phi_{(i_1,\dots,i_n)}\big(e_i^{(j)}\big) = \begin{cases} 1 & \text{if } i = i_j, \\ 0 & \text{otherwise.} \end{cases}$$

Then it is evident that the kernel of $\phi_{(i_1,\dots,i_n)}$ contains $I(B^n, B)$, so that ϕ descends to a map

$$\bar{\phi}_{(i_1,\dots,i_n)} : G(B^n/B) \to B.$$

Moreover, we have $\bar{\phi}_{(i_1,\dots,i_n)}(e_{i_1}^{(1)} \cdots e_{i_n}^{(n)}) = 1$. We conclude that $e_{i_1}^{(1)} \cdots e_{i_n}^{(n)}$ is nonzero in $G(B^n/B)$.

Finally, note that $e_{i_1}^{(1)} \cdots e_{i_n}^{(n)}$ is an idempotent for any permutation $(i_1, \dots, i_n)$, and if $(j_1, \dots, j_n)$ is any other permutation of $(1, \dots, n)$, then

$$e_{i_1}^{(1)} \cdots e_{i_n}^{(n)} \cdot e_{j_1}^{(1)} \cdots e_{j_n}^{(n)} = 0.$$

Hence the set (11), where $(i_1, \dots, i_n)$ ranges over all permutations of $(1, \dots, n)$, forms a set of nonzero orthogonal idempotents that spans $G(B^n/B)$ as a B-module. We conclude that it forms a basis for $G(B^n/B)$, as claimed.

Finally, since this basis for $G(B^n/B)$ has $n!$ elements, and consists entirely of idempotents, we conclude that $G(B^n/B) \cong B^{n!}$ as B-algebras, as desired.

We have proven the first assertion of Theorem 4.

3.2. The action of S_n on $G(B^n/B)$

It is interesting to consider the natural action of S_n on $(B^n)^{\otimes n}$, and on $G(B^n/B)$, obtained by permuting the tensor factors. From this point of view, we see that

$$G(B^n/B) \cong B[S_n]$$

as $B[S_n]$-modules. The isomorphism is given by $e_{i_1}^{(1)} \cdots e_{i_n}^{(n)} \mapsto \sigma$, where $\sigma \in S_n$ denotes the permutation $j \mapsto i_j$. If we write $e_\sigma := e_{i_1}^{(1)} \cdots e_{i_n}^{(n)}$, then the action of an element $g \in S_n$ on $G(B^n/B)$ is given by

$$g \cdot e_\sigma = e_{g\sigma}.$$

Let $A = B^n$. Under the action of S_n on $G(A/B)$, the ring $A^{(1)} \subset G(A/B)$ given by the image of $A \otimes 1 \otimes \cdots \otimes 1$ is fixed by $S_{n-1}^{(1)}$, the subgroup of S_n fixing 1. Note that $A^{(1)} \cong A$. Similarly, as in Galois theory, the other “conjugate” copies of A in $G(A/B)$, namely $A^{(j)} = 1 \otimes \cdots \otimes A \otimes \cdots \otimes 1$ (where the A is in the j-th tensor factor) for $j = 2, \dots, n$ are fixed by the conjugate subgroups $S_{n-1}^{(j)} \subset S_n$ fixing j for $j = 2, \dots, n$, respectively.

In terms of these subgroups $S_{n-1}^{(j)} \subset S_n$, we may express the idempotents $e_i^{(j)}$ in terms of our orthogonal basis $\{e_\sigma\}_{\sigma \in S_n}$ of idempotents for $G(A/B)$ as follows:

$$e_i^{(j)} = \sum_{\sigma \in S_{n-1}^{(j)} g_{ji}} e_\sigma, \tag{12}$$

where g_{ji} denotes any element in S_n taking i to j. That is, $e_i^{(j)}$ corresponds to the sum of e_σ over a right coset of $S_{n-1}^{(j)}$, namely, the one consisting of elements in S_n taking i to j. For an extension of these results to general products of rings $A = A_1 \times \cdots \times A_k$, see Section 8.

4. The case of fields

Before proving Theorem 2, we begin by recalling the correspondence between finite étale extensions of a field and Galois sets. Let K be a field and fix a separable closure $\bar{K}$ of K. Then, given a finite étale extension L/K, consider the set $S_{L/K}$ of K-algebra homomorphisms from L to $\bar{K}$. We see that $G_K := \mathrm{Gal}(\bar{K}/K)$ acts on $S_{L/K}$ by composition: if $\tau \in G_K$ and $\psi \in S_{L/K}$, then $\tau \circ \psi \in S_{L/K}$. Moreover, this action is continuous when G_K is given the profinite topology and $S_{L/K}$ is given the discrete topology, i.e., the action of G_K factors through a finite quotient of G_K. We therefore obtain a functor

$$(\text{finite étale } K\text{-algebras}) \to (\text{finite sets with continuous } G_K\text{-action}) \tag{13}$$

sending L to $S_{L/K}$, which is in fact an equivalence of categories (see, e.g., [15, Thm. 2.9]).

Note that if L/K is finite étale of degree n, then $\bar{K} \otimes_K L$ is isomorphic to $\bar{K}^n$ as a $\bar{K}$-algebra. More canonically, we have an isomorphism

$$\bar{K} \otimes_K L \to \bar{K}^{S_{L/K}} := \prod_{s \in S_{L/K}} \bar{K}, \qquad 1 \otimes \ell \mapsto (s(\ell))_{s \in S_{L/K}}, \tag{14}$$

of $\bar{K}$-algebras. The Galois group G_K acts on $\bar{K} \otimes_K L$ through the left tensor factor, and therefore induces an action on $S_{L/K}$ via (14); this is precisely the G_K-action on $S_{L/K}$ in (13).

We now turn to the problem of describing the Galois set $S_{G(L/K)/K}$ in terms of the Galois set $S_{L/K}$, where L/K is a finite étale extension of degree n. By Theorem 1,

$$\bar{K} \otimes_K G(L/K) \cong (\bar{K}^{S_{L/K}})^{\otimes n} / I(\bar{K}^{S_{L/K}}, \bar{K})$$

as $\bar{K}$-algebras. The G_K-action on the left tensor factor of $\bar{K} \otimes_K G(L/K)$ yields an action on $(\bar{K}^{S_{L/K}})^{\otimes n} / I(\bar{K}^{S_{L/K}}, \bar{K})$ defined by

$$\tau(e_s^{(i)}) = e_{\tau(s)}^{(i)},$$

where $\tau \in G_K$, $s \in S_{L/K}$, and e_s denotes the element $(\delta_{ss'})_{s'}$ of $K^{S_{L/K}}$, where δ is the Kronecker delta.

Given two sets T and T', we let $\mathrm{Bij}(T, T')$ denote the set of bijections $f : T \to T'$. Let $[n]$ denote the set $\{1, \ldots, n\}$. Then Section 3.2 shows that

$$\bar{K}[\mathrm{Bij}([n], S_{L/K})] \xrightarrow{\cong} (\bar{K}^{S_{L/K}})^{\otimes n} / I(\bar{K}^{S_{L/K}}, \bar{K})$$

as $\bar{K}$-algebras, where $\pi \in \mathrm{Bij}([n], S_{L/K})$ is sent to $e_{\pi(1)}^{(1)} \cdots e_{\pi(n)}^{(n)}$. We then see that the action of G_K on $\bar{K} \otimes_K G(L/K)$ induces an action on $\mathrm{Bij}([n], S_{L/K})$ where G_K acts on $\mathrm{Bij}([n], S_{L/K})$ via its action on $S_{L/K}$; that is, $\tau \in G_K$ acts on $\pi \in \mathrm{Bij}([n], S_{L/K})$ by

$$(\tau(\pi))(j) = \tau(\pi(j)).$$

Hence, the Galois set corresponding to $G(L/K)$ is given by $\mathrm{Bij}([n], S_{L/K})$ with this action of G_K.

We now prove Theorem 2. Let L be a finite separable field extension of K of degree n, and let M be the Galois closure of L/K in $\bar{K}$. Let G denote the Galois group of M/K; thus G acts faithfully and transitively on $S_{L/K}$, and so G sits naturally inside $\mathrm{Bij}(S_{L/K}, S_{L/K})$. Note that $\mathrm{Bij}(S_{L/K}, S_{L/K})$ carries a G_K-action via post-composition. Since M is the Galois closure of L/K, this action of G_K restricts to an action on G. The set G equipped with this action is the Galois set corresponding to M. Since the action of G on $S_{L/K}$ is faithful and transitive, we see that as Galois sets,

$$\mathrm{Bij}(S_{L/K}, S_{L/K}) = \coprod_r G = S_{M^r/K}.$$

Therefore, choosing a bijection of $[n]$ and $S_{L/K}$ yields an isomorphism $S_{G(L/K)/K} \cong S_{M^r/K}$ of Galois sets. As a result, $G(L/K)$ and M^r are isomorphic as K-algebras.

5. The étale case

We have already proven the first assertion of Theorem 4. Suppose, more generally, that A is any ring that is étale and locally free of rank n over B. Then we claim that $G(A/B)$ is an étale B-algebra which is locally free of rank $n!$; this is the second assertion of Theorem 4.

To prove the claim, we first require a definition. An étale B-algebra C is called an *étale cover* of B if the induced morphism $\mathrm{Spec}\, C \to \mathrm{Spec}\, B$ is surjective. The key fact we use in proving the second assertion of Theorem 4 is the following well-known lemma:

Lemma 15. *Let R be any B-algebra that is finitely generated as a B-module. Then R is étale and locally free of rank n over B if and only if there exists an étale cover C of B such that $R \otimes_B C \cong C^n$ as C-algebras.*

Proof. First, the proof of [16, Thm. 11.4] shows that R is locally free of rank n over B if and only if there exists an étale cover C of B such that $R \otimes_B C \cong C^n$ as C-modules.

Now if C is an étale cover of B as in the statement of the lemma, then $R \otimes_B C$ is an étale C-algebra. By étale descent, R is then an étale B-algebra (see, e.g., [21, Prop. 1.15(x)]), and it is also locally free of rank n over B by the previous paragraph.

Conversely, if R is étale and locally free of rank n over B, then R is an étale cover of B. There then exists an R-algebra R' such that we have an isomorphism of R-algebras $R \otimes_B R \cong R \times R'$ (see, e.g., [7, Remark after Lemma 1.1.17]). Since $R \otimes_B R$ is étale and locally free of rank n over R, it follows that R' is étale and locally free of rank $n-1$ over R. By induction on n, we conclude that there exists an étale cover C of B such that $R \otimes_B C \cong C^n$ as C-algebras. ◻

Since A is étale and locally free of rank n over B, by Lemma 15 we see that there exists an étale cover C of B such that $A \otimes_B C \cong C^n$ as C-algebras. By Theorem 1, we then have

$$G(A/B) \otimes_B C \cong G(C^n/C) \cong C^{n!}$$

as C-algebras. Applying Lemma 15 once again, we conclude that $G(A/B)$ is étale and locally free of rank $n!$ over B, as desired.

We can say more in terms of the underlying Galois sets when Spec B is connected. Recall that there is an equivalence of categories between finite étale extensions of B and finite sets equipped with a continuous action by a certain profinite group $\pi_1^{\text{ét}}(B)$ called the *étale fundamental group* of B (see, e.g., [15, Thm. 1.11]). When $B = K$ is a field, $\pi_1^{\text{ét}}(K)$ is nothing other than G_K. By the same argument as in the case of fields, one shows that if A/B is a finite étale extension of degree n corresponding to a finite set S with a continuous action by $\pi_1^{\text{ét}}(B)$, then $G(A/B)$ corresponds to the set $\mathrm{Bij}([n], S)$ with $\pi_1^{\text{ét}}(B)$-action induced by the action on S.

6. The monogenic case

In this section, we examine the situation where B is monogenic over A. We prove:

Theorem 16. *Let f be a monic polynomial with coefficients in B, and let $A = B[x]/f(x)$ denote the corresponding monogenic ring of rank n over B. Then $G(A/B)$ is a ring of rank $n!$ over B, a basis of it being all monomials of the form*

$$\prod_{i=1}^{n} x_i^{e_i} \tag{15}$$

where the exponents e_i satisfy $0 \le e_i < i$; here $x_1, \dots, x_n$ denote the images in $G(A/B)$ of $x^{(1)}, \dots, x^{(n)} \in A^{\otimes n}$ respectively.

Proof. If $A = B[x]$, then $I(A, B)$ is generated by the relations (2) where $a = x$. This is because the powers $1, x, x^2, \dots, x^{n-1}$ of x form a basis for A over B, and the elementary symmetric functions $s_i(x^j)$ of powers x^j of x are integer polynomials in the elementary symmetric functions $s_i(x)$ of x (by the *Newton–Girard identities*; see, e.g., [20, pp. 99–101]). Hence the relations (2) for $a = x^j$ $(j > 1)$ are implied by those for which $a = x$.

Now let the characteristic polynomial of $\times x : A \to A$ be given by $P_x(T) = T^n - s_1(x)T^{n-1} + s_2(x)T^{n-2} + \cdots + (-1)^n s_n(x)$. Then a direct construction of $G(A/B)$ is as follows. By the symmetric function theorem, the ring $R = \mathbb{Z}[X_1, \dots, X_n]$ is a free module of rank $n!$ (with basis given as above) over the polynomial ring $S = \mathbb{Z}[\Sigma_1, \dots, \Sigma_n]$, where the Σ_i denote the elementary symmetric polynomials: $\Sigma_1 = X_1 + \cdots + X_n$, etc. Using the coefficients of P_x, we get a map $\psi : S \to B$ defined by sending Σ_i to $s_i(x)$. This allows us to construct the B-algebra $R \otimes_S B$, which is then free over B of rank $n!$.

We claim that the algebra $R \otimes_S B$ is isomorphic to $G(A/B)$. Indeed, we may define a map

$$\phi : A^{\otimes n} = B[x^{(1)}, \dots, x^{(n)}] \to R \otimes_S B$$

by sending $x^{(i)} \mapsto X_i \otimes 1$. Then, by the definition of $R \otimes_S B$, the kernel of ϕ consists of all polynomials in $B[x^{(1)}, \dots, x^{(n)}]$ that are symmetric in the $x^{(i)}$ (so can be expressed as polynomials in the elementary symmetric functions $e_j(x^{(1)}, \dots, x^{(n)})$) and that evaluate to 0 when $e_j(x^{(1)}, \dots, x^{(n)})$ is replaced by $s_j(x)$ for every j. But these polynomials are precisely the elements of the ideal $I(A, B)$, and thus $G(A/B) = A^{\otimes n}/I(A, B) \cong R \otimes_S B$, as desired. $\square$

Remark 17. This construction in the monogenic case is more or less given in Grothendieck [11, Lemme 1 and corollary next page].

In the case where A is monogenic over the base ring B, we may use Theorem 16 to compute the discriminant $\mathrm{Disc}(G(A/B))$ of the S_n-closure of A in terms of the discriminant $\mathrm{Disc}(A)$ of A. The definition of $\mathrm{Disc}(A) \in B$ as given in the introduction (prior to Theorem 4) is unique only up to factors in $B^{\times 2}$. However, if A is a *based ring* of rank n over B—i.e., A comes equipped with a basis of size n over B—then $\mathrm{Disc}(A/B)$ is well-defined as an element of B, namely as the determinant of the trace form $\mathrm{Tr}(xy)$ on A expressed as an $n \times n$ matrix over B in terms of this chosen basis. We then find that, for $n \geq 2$, we have

$$\mathrm{Disc}(G(A/B)) = \mathrm{Disc}(A)^{n!/2} \tag{16}$$

as discriminants of based rings over B; here A is equipped with its power basis and $G(A/B)$ is given the basis as in Theorem 16.

To see this, note that it suffices again to prove this identity in the case $B = \mathbb{Z}[\Sigma_1, \ldots, \Sigma_n]$, $A = B[X_1]$, and $G(A/B) = \mathbb{Z}[X_1, \ldots, X_n]$. The identity (16) is trivial for $n = 2$, while for general n it follows by induction. Indeed, we have the equalities $A = \mathbb{Z}[X_1][\Sigma_1', \ldots, \Sigma_{n-1}']$ and $G(A/B) = A[X_2, \ldots, X_n]$, where $\Sigma_1', \ldots, \Sigma_{n-1}'$ denote the elementary symmetric polynomials in $X_2, \ldots, X_n$. The proof of Theorem 16 now implies that $G(A/B) = G(A[X_2]/A)$, so that $G(A/B)$ is free of rank $(n-1)!$ over A. The induction hypothesis then gives

$$\mathrm{Disc}(G(A/B)/A) = \mathrm{Disc}(A[X_2]/A)^{(n-1)!/2}.$$

In the tower of ring extensions $G(A/B) \,/\, A \,/\, B$, we then see that

$$\begin{aligned} \mathrm{Disc}(G(A/B)) &= \mathbf{N}_B^A(\mathrm{Disc}(G(A/B)/A)) \cdot \mathrm{Disc}(A)^{(n-1)!} \\ &= \mathrm{Disc}(A)^{(n-2)\cdot(n-1)!/2} \cdot \mathrm{Disc}(A)^{(n-1)!} \\ &= \mathrm{Disc}(A)^{n!/2}, \end{aligned}$$

proving (16).

7. Ranks $k \leq 3$

The cases $k = 1, 2$ in Theorem 5 follow from Theorem 3. So we consider the case $k = 3$ in this section.

Theorem 18. *Assume that A is free of rank 3 over B with basis $1, x, y$. Let x_1, x_2, x_3 and y_1, y_2, y_3 denote the images in $G(A/B)$ of the elements $x^{(1)}, x^{(2)}, x^{(3)}$ and $y^{(1)}, y^{(2)}, y^{(3)} \in A^{\otimes 3}$ respectively. Then the ring $G(A/B)$ is free of rank 6 over B with basis $1, x_1, y_1, x_2, y_2, x_1y_2$.*

Proof. It is known that, by translating x and y by appropriate B-multiples of 1, the multiplication table of A as a ring over B can be expressed in the form

$$\begin{aligned} xy &= \quad ad, \\ x^2 &= -ac + bx + ay, \\ y^2 &= -bd + dx + cy, \end{aligned} \tag{17}$$

for some elements $a, b, c, d \in B$ (see [9, Prop. 4.2]).

In terms of these elements, the characteristic equations of x, y, and $x + y$ are given by

$$T^3 - bT^2 + acT - a^2d = 0,$$
$$T^3 - cT^2 + bdT - ad^2 = 0,$$

and

$$T^3 - (b+c)T^2 + (ac+bc+bd-3ad)T - (a^2d+ac^2+b^2d+ad^2-2abd-2acd) = 0$$

respectively.

Note first that the trace relations $x_1 + x_2 + x_3 = b$ and $y_1 + y_2 + y_3 = c$ are equivalent to

$$x_3 = b - x_1 - x_2, \tag{18}$$
$$y_3 = c - y_1 - y_2. \tag{19}$$

Hence $G(A/B)$ is generated as a B-module by the nine elements $\{1, x_1, y_1\} \cdot \{1, x_2, y_2\}$, and we need to find three additive relations to relate $x_1x_2, x_1y_2, x_2y_1, y_1y_2$.

Since all other trace relations are B-linear combinations of the trace relations for x and y, they do not yield any further new relations. Instead, we now take the quadratic identities $x_1x_2 + x_1x_3 + x_2x_3 = ac$, $y_1y_2 + y_1y_3 + y_2y_3 = bd$, and $(x_1 + y_1)(x_2 + y_2) + (x_1 + y_1)(x_3 + y_3) + (x_2 + y_2)(x_3 + y_3) = ac + bc + bd - 3ad$, which reduce to

$$x_1x_2 = a(c - y_1 - y_2), \tag{20}$$
$$y_1y_2 = d(b - x_1 - x_2), \tag{21}$$
$$y_1x_2 = bc - ad - b(c - y_1 - y_2) - c(b - x_1 - x_2) - x_1y_2. \tag{22}$$

These identities show that $G(A/B)$ is spanned over B by the six elements claimed in the theorem.

It remains to show that these six elements are in fact linearly independent. By Theorem 1, it suffices to consider the case when $B = \mathbb{Z}[a, b, c, d]$ is a free polynomial ring over $\mathbb{Z}$ in variables a, b, c, d, and A is free of rank 3 over B with basis 1, x, y, and multiplication table given by (17).

In that case, let K be the quotient field of B. If the six elements $1, x_1, x_2, y_1, y_2, x_1y_2$ satisfy a linear relation over B, then they also satisfy a linear relation over K. We show that this is not the case. Since $\mathrm{Disc}((A \otimes_B K)/K)$ is a nonzero polynomial in a, b, c, and d, it is invertible in K and hence $(A \otimes_B K)/K$ is étale. In fact, $A \otimes_B K$ is a field. If it were not, then the cubic polynomial $f(x)$ defining the extension $(A \otimes_B K)/K$ would have a root in K. As A/B is the universal based cubic ring extension having first basis element 1, this would imply that every cubic polynomial over $\mathbb{Q}$ has a rational root, which is not true.

Now, by Theorem 1, the elements $1, x_1, x_2, y_1, y_2, x_1 y_2$ also span $G((A \otimes_B K)/K) \cong G(A/B) \otimes_B K$. Since $A \otimes_B K$ is a field, Theorem 2 implies that $G((A \otimes_B K)/K)$ is a 6-dimensional vector space over K. It follows that $1, x_1, x_2, y_1, y_2$, and $x_1 y_2$ are linearly independent over K, and hence over B, as desired. □

Thus to any cubic ring A over B with basis $1, x, y$, there is naturally associated a canonical sextic ring $\tilde{A}$ over B, given by $G(A/B)$. We show that in fact we have the formula

$$\operatorname{Disc}(\tilde{A}) = \operatorname{Disc}(A)^3 \tag{23}$$

as discriminants of based rings.

To see this, it again suffices to check this in the case where the base ring B is $\mathbb{Z}[a, b, c, d]$. In this case, it is clear that the multiplication table for $\tilde{A}$, in terms of our chosen basis $1, x_1, x_2, y_1, y_2, x_1 y_2$ for $\tilde{A}$, will involve only polynomials in a, b, c, d with coefficients in $\mathbb{Z}$. Thus the discriminant $\operatorname{Disc}(\tilde{A})$ of $\tilde{A}$ will also be an integer polynomial in a, b, c, d. Furthermore, this polynomial $\operatorname{Disc}(\tilde{A})$ must remain invariant under changes of the basis x, y via transformations in $\mathrm{GL}_2(\mathbb{Z})$, which changes a, b, c, d by the action of $\mathrm{GL}_2(\mathbb{Z})$ on the binary cubic form $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ (by [9, Prop. 4.2]). It is known (see, e.g., [12, Lec. XVII]) that the only $\mathrm{GL}_2(\mathbb{Z})$-invariant polynomials in a, b, c, d under this action must be polynonomials in $\operatorname{Disc}(f) = \operatorname{Disc}(A)$, and thus $\operatorname{Disc}(\tilde{A})$ must be a polynomial in $\operatorname{Disc}(A)$.

To determine this polynomial, we may then restrict to the case where $a = 1$ or $d = 1$; that is, we may assume the rank 3 ring A is monogenic over B, in which case $\operatorname{Disc}(\tilde{A}) = \operatorname{Disc}(A)^3$ by (16). Formula (23) therefore follows for general rank 3 rings A over B that have a basis of the form $1, x, y$.

In particular, if A is a cubic order in a noncyclic cubic field K, then $G(A/\mathbb{Z})$ provides a canonically associated sextic order $\tilde{A}$ in the Galois closure $\tilde{K}$ satisfying $\operatorname{Disc}(\tilde{A}) = \operatorname{Disc}(A)^3$.

We may now deduce the more general Theorem 5 from Theorem 18. Indeed, let A be any locally free ring of rank 3 over B. Then it follows from [10, Lemma 1.1] that, for any maximal ideal M of B, the localization A_M is free of rank 3 over B_M *with a basis of the form* $1, x, y$ (essentially an application of Nakayama's Lemma). We then conclude, by Theorem 18, that the localization $G(A/B)_M$ is free of rank 6 over B_M, for all maximal ideals M of B.

Since A is finitely presented as a B-module (being locally free; see Footnote 2 on p. 1882) and the ideal $I(A, B)$ is finitely generated (a set of generators being the relations (2), where a ranges over a spanning set for A over B; see Section 2), we conclude that $G(A/B)$ too is finitely presented as a B-module.

Finally, since $G(A/B)$ is finitely presented as a B-module, and the localization $G(A/B)_M$ is free of rank 6 over B_M for all maximal ideals M of B, by Footnote 2 on p. 1882, we conclude that $G(A/B)$ is locally free of rank 6 over B, and Theorem 5 follows.

8. Behavior under products

Suppose $A_1, \dots, A_k$ are locally free rings of rank $n_1, \dots, n_k$, respectively, over B. Then $A = A_1 \times \cdots \times A_k$ is locally free of rank $n = n_1 + \cdots + n_k$ over B. To prove Theorem 6, we wish to understand $G(A/B)$ in terms of $G(A_j/B)$ for $j \in \{1, \dots, k\}$.

To this end, let $[k]$ denote the set $\{1, \dots, k\}$. For each $j \in [k]$, we define $e_j \in A$ by $e_1 = (1, 0, \dots, 0)$, $e_2 = (0, 1, 0, \dots, 0)$, and so on. For an n-tuple $i = (i_1, \dots, i_n) \in [k]^n$, define $T_i \subset A^{\otimes n}$ to be the B-subalgebra generated by all pure tensors $a_1^{(1)} \cdots a_n^{(n)} \in A^{\otimes n}$, where $a_m \in A_{i_m} e_{i_m}$ for all $m \in \{1, \dots, n\}$ (so $T_i \cong A_{i_1} \otimes \cdots \otimes A_{i_n}$ as B-algebras). Then we have the decomposition

$$A^{\otimes n} = \prod_{i \in [k]^n} T_i \tag{24}$$

as B-algebras, where the T_i factor in (24) corresponds to the idempotent $e_i := e_{i_1}^{(1)} \cdots e_{i_n}^{(n)}$ in $A^{\otimes n}$. We then also have a corresponding decomposition

$$I(A, B) = \prod_{i \in [k]^n} I_i(A, B), \tag{25}$$

where $I_i(A, B) = e_i I(A, B)$ is an ideal of the B-algebra T_i.

Let S denote the subset of all n-tuples $i = (i_1, \dots, i_n) \in [k]^n$ such that n_1 of the i_m's are equal to 1, n_2 of the i_m's are equal to 2, etc. (Thus, for any $i \in S$, we have an isomorphism $T_i \cong A_1^{\otimes n_1} \otimes \cdots \otimes A_k^{\otimes n_k}$ as B-algebras, obtained by appropriately permuting the tensor factors.) For any n-tuple $i \notin S$, we claim that $I_i(A, B) = T_i$. Indeed, for such an $i \notin S$, let $j \in [k]$ be an element that appears fewer than n_j times as an entry in i. Then since e_j has characteristic polynomial $x^{n-n_j}(x-1)^{n_j}$, we have the relation

$$1 - \sum_{1 \le r_1 < \cdots < r_{n_j} \le n} e_j^{(r_1)} \cdots e_j^{(r_{n_j})} \in I(A/B). \tag{26}$$

Multiplying (26) by any element of T_i, and noting that any pure tensor in T_i has fewer than n_j tensor factors in $A_j e_j$, yields

$$T_i \subseteq I_i(A, B) \tag{27}$$

and so $T_i = I_i(A, B)$ as claimed.

To determine $I_i(A, B)$ when $i \in S$, it suffices by symmetry (via the S_n-action on $A^{\otimes n}$) to consider the case $i = (i_1, \dots, i_n)$, where $i_1 = \cdots = i_{n_1} = 1$, $i_{n_1+1} = \cdots = i_{n_1+n_2} = 2$, etc. To obtain generators for $I_i(A, B)$ for this particular $i \in S$, we take generators of $I(A, B)$ and project them onto T_i by multiplying them by the idempotent e_i. A natural generating set for $I(A, B)$ (by the work of Section 2) is the set of all elements of the form

$$s_m(a) - \sum_{1 \le r_1 < \cdots < r_m \le n} a^{(r_1)} \cdots a^{(r_m)}, \tag{28}$$

where $a = a_j e_j$ for some $a_j \in A_j$ and $j \in [k]$. If $a = a_j e_j \in A_j e_j$ is such an element, then multiplying the element (28) in $I(A, B)$ by the idempotent $e_i = e_{i_1}^{(1)} \cdots e_{i_n}^{(n)} \in T_i$, we obtain 0 unless $m \leq n_j$, in which case we obtain

$$s_m(a_j) - \sum_{n_1+\cdots+n_{j-1}+1 \leq r_1 < \cdots < r_m \leq n_1+\cdots+n_j} a^{(r_1)} \cdots a^{(r_m)}. \tag{29}$$

Thus the ideal in T_i generated by all such elements is simply $I(A_1, B) \otimes \cdots \otimes I(A_k, B) \subset T_i = A_1^{\otimes n_1} \otimes \cdots \otimes A_k^{\otimes n_k}$. It follows that $T_i / I_i(A, B) \cong G(A_1/B) \otimes \cdots \otimes G(A_k/B)$ for this particular i, and thus for any $i \in S$.

Therefore, if for each $i \in S$ we write $R_i := T_i / I_i(A, B)$, then we have shown that

$$G(A/B) = \prod_{i \in S} R_i \tag{30}$$

as B-algebras, and moreover $R_i \cong G(A_1/B) \otimes \cdots \otimes G(A_k/B)$ for all $i \in S$, yielding Theorem 6.

Note that the proof shows that the S_n-action on the B-module $G(A_1 \times \cdots \times A_k/B)$ is induced from the $S_{n_1} \times \cdots \times S_{n_k}$-action on $G(A_1/B) \otimes \cdots \otimes G(A_k/B)$; i.e., we have

$$G(A_1 \times \cdots \times A_k/B) \cong B[S_n] \otimes_{B[S_{n_1} \times \cdots \times S_{n_k}]} [G(A_1/B) \otimes \cdots \otimes G(A_k/B)]$$

as $B[S_n]$-modules.

9. An example of a ring of rank 4 whose S_4-closure has rank $32 > 4!$

In this section, we give an example of a ring A of rank 4 over B—namely $A = B[x, y, z]/(x, y, z)^2$—such that $G(A/B)$ has rank $32 > 4!$ over B.

Proposition 19. *Let B be a ring, and let A be the ring $B[x, y, z]/(x, y, z)^2$ having rank 4 over B. Then $G(A/B)$ is free of rank 32 over B.*

Proof. Motivated by the relations (2) for $G(A/B)$, we give a direct construction of a ring R over B, which we will then show to be naturally isomorphic to $G(A/B)$. Precisely, we construct R to have a B-module decomposition of the form

$$\begin{aligned} R = B &\oplus [T(x) \oplus T(y) \oplus T(z)] \oplus [U(x) \oplus U(y) \oplus U(z)] \\ &\oplus [V(x, y) \oplus V(y, z) \oplus V(x, z)] \oplus W(x, y, z), \end{aligned} \tag{31}$$

where $T(\cdot)$, $U(\cdot)$, $V(\cdot, \cdot)$, and $W(x, y, z)$ are free B-modules having ranks 3, 2, 5, and 1, respectively. Therefore, R (and thus $G(A/B)$) will have B-rank $1 + 3 \cdot 3 + 3 \cdot 2 + 3 \cdot 5 + 1 = 32$. The constructions of these B-modules $T(\cdot)$, $U(\cdot)$, $V(\cdot, \cdot)$, and $W(\cdot, \cdot, \cdot)$ are as follows.

First, $T(x)$ is the B-module spanned by x_1, x_2, x_3, x_4 modulo the relation $x_1 + x_2 + x_3 + x_4 = 0$; $T(y)$ and $T(z)$ are defined similarly, and hence each is three-dimensional.

Second, $U(x)$ is defined as the symmetric square of $T(x)$ modulo the relations

$$x_1^2 = x_2^2 = x_3^2 = x_4^2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = 0.$$

Now $x_1 + x_2 + x_3 + x_4 = 0$ in $T(x)$, so multiplying by x_1 and x_2 respectively shows that

$$x_1x_2 + x_1x_3 + x_1x_4 = 0 \quad \text{and} \quad x_1x_2 + x_2x_3 + x_2x_4 = 0$$

in $U(x)$; this in turn implies that

$$x_2x_3 + x_3x_4 + x_2x_4 = 0 \quad \text{and} \quad x_1x_3 + x_3x_4 + x_1x_4 = 0$$

in $U(x)$. Subtracting the first and last of the latter four relations gives $x_1x_2 = x_3x_4$, and similarly $x_1x_3 = x_2x_4$ and $x_1x_4 = x_2x_3$. We thus find that $U(x)$ is spanned over B by the images of any two of the three nonzero elements x_1x_2 (or x_3x_4), x_1x_3 (or x_2x_4), and x_1x_4 (or x_2x_3), and any two of these are independent over B. The B-modules $U(y)$ and $U(z)$ are defined in the analogous manner, and are thus also two-dimensional.

Third, $V(x, y)$ is defined as the product $T(x) \otimes T(y)$ modulo the relations

$$x_1y_1 = x_2y_2 = x_3y_3 = x_4y_4 = 0$$

(where we have suppressed the tensor symbols). As $T(x) \otimes T(y)$ is a rank 9 module over B, we see that $V(x, y)$ is five-dimensional. The B-modules $V(y, z)$ and $V(x, z)$ are defined analogously, and hence are also five-dimensional.

Finally, $W(x, y, z)$ is the space $T(x) \otimes T(y) \otimes T(z)$ modulo the relations

$$x_iy_iz_j = x_jy_iz_i = x_iy_jz_i = 0$$

for all i and j, and the further relations

$$x_iy_jz_k = \mathrm{sgn}(i, j, k)x_1y_2z_3$$

for all permutations (i, j, k) of $(1, 2, 3)$, We have imposed the latter relations in $W(x, y, z)$ because we have the relations

$$0 = (x_4y_4)z_3 = (-x_1 - x_2 - x_3)(-y_1 - y_2 - y_3)z_3 = x_1y_2z_3 + x_2y_1z_3$$

in $I(A, B)$, implying $x_2y_1z_3 = -x_1y_2z_3$, etc. With these relations, we see that the rank of $W(x, y, z)$ over B is 1, and it is spanned over B by $x_1y_2z_3$.

We have not defined any B-module components in R involving quadruple products of x_i, y_j, z_k $(1 \le i, j, k \le 3)$ because these we would like to be zero due to the relations $x_iy_i = x_iz_i = y_iz_i = 0$ in A. Similarly, there are no B-module components involving triple products of only x_i and y_j $(1 \le i, j, k \le 3)$, since the analogues of such products in $G(A/B)$ would be zero:

$$0 = x_1(y_1y_2 + y_2y_3 + y_1y_3) = x_1y_2y_3,$$

and similarly all such triple products would be zero in $G(A/B)$. Thus we keep only those components $T(\cdot)$, $U(\cdot)$, $V(\cdot, \cdot)$, and $W(\cdot, \cdot, \cdot)$ appearing in (31).

The product structure on R is defined simply in terms of the natural maps $T(x) \otimes T(x) \to U(x)$, $T(x) \otimes T(y) \to V(x, y)$, $T(x) \otimes T(y) \otimes T(z) \to W(x, y, z)$, $T(x) \otimes V(y, z) \to W(x, y, z)$, and so on. All other products (such as $T(x) \otimes V(x, y)$) are defined to be zero. With this product structure, it is immediate that R is a ring.

To see that $G(A/B) \cong R$, we note that there is a natural surjective map

$$A \otimes A \otimes A \otimes A \to R,$$

sending $x^{(i)} \mapsto x_i$, $y^{(i)} \mapsto y_i$, and $z^{(i)} \mapsto z_i$. Furthermore, the kernel of this map is, by design, contained in $I(A, B)$. To see that it contains $I(A, B)$, one may simply check that it contains the elements (2) on a basis of A over B, and so on the basis elements 1 (trivial), x, y, and z. By symmetry of x, y, and z, we then only need to check that the elements (2) are in the kernel for $a = x$ and $j = 1, 2, 3$, and this is again immediate.

We conclude that $G(A/B) \cong R$ has rank 32 over B. $\square$

10. Why do we need to allow the rank of S_n-closures to exceed $n!$?

It is natural to ask if it is possible to enlarge the ideal $I(A, B)$ defined in (2) to an ideal $I'(A, B)$ such that: (i) for any ring A that is locally free of rank n over a ring B, the quotient $G'(A/B) := A^{\otimes n}/I'(A, B)$ is always locally free of rank $n!$ over B; and (ii) the construction $G'(A/B)$ commutes with base change. As the following theorem shows, the answer is no:

Theorem 20. *Let $n \geq 4$. As B ranges over all rings and A ranges over all rings that are locally free of rank n over B, there cannot exist corresponding rings $G'(A/B)$ that are locally free of rank $n!$ over B and B-algebra maps $i_1, \ldots, i_n : A \to G'(A/B)$ such that:*

(a) *for every A and B, the images of $i_1, \ldots, i_n$ generate $G'(A/B)$ as a B-algebra;*
(b) *$G'(A/B)$ and $i_1, \ldots, i_n$ are functorial in A;*
(c) *$G'(A/B)$ and $i_1, \ldots, i_n$ respect base change, i.e., for all B-algebras C, there is a functorial choice of isomorphism $G'(A/B) \otimes_B C \xrightarrow{\sim} G'((A \otimes_B C)/C)$ which commute with the i_j; and*
(d) *if A/B is an S_n-extension of fields of degree n, then $G'(A/B)$ is isomorphic to the usual Galois closure of A over B, and the i_j correspond to the n distinct embeddings of A.*

Remark 21. Note that $G(A/B)$ satisfies all the essential properties (a)–(d) of the theorem (the map i_j corresponds to $a \mapsto a^{(j)}$) but, as we have already seen, it does not always have rank $n!$ over B. In the usual Galois closure $\tilde{A}$ of an S_n-extension A/B of fields of degree n, the maps i_j correspond to the embeddings $A \hookrightarrow \tilde{A}$ whose images generate $\tilde{A}$ as an algebra over B.

Proof of Theorem 20. We consider first the case $n = 4$. Let K be an S_4-quartic extension of $\mathbb{Q}$, and let $\mathcal{O}_K$ denote the ring of integers of K. Fix a prime $p \geq 5$, and let R be the ring $\mathbb{Z} + p\mathcal{O}_K$. Then $\bar{R} := R \otimes_{\mathbb{Z}} \mathbb{F}_p \cong \mathbb{F}_p[x, y, z]/(x, y, z)^2$.

We begin by showing that $G'(R/\mathbb{Z})$ is a quotient of $G(R/\mathbb{Z})$. The maps $i_1, \ldots, i_4 : R \to G'(R/\mathbb{Z})$ determine an R-algebra map $\pi' : R^{\otimes 4} \to G'(R/\mathbb{Z})$. By property (a), the images of the i_j generate $G(R/\mathbb{Z})$ as a ring, and so π' is surjective. Now $R^{\otimes 4} \subset K^{\otimes 4}$, and since $G'(R/\mathbb{Z})$ is free of rank 24 over $\mathbb{Z}$, by property (c) it is a full rank $\mathbb{Z}$-submodule of $G'(K/\mathbb{Q})$. Furthermore, $G'(K/\mathbb{Q})$ is isomorphic to $G(K/\mathbb{Q})$ by Theorem 2 and property (d). We thus see that

$$I(R/\mathbb{Z}) \subset R^{\otimes 4} \cap I(K/\mathbb{Q}) = R^{\otimes 4} \cap \ker(K^{\otimes 4} \to G'(K/\mathbb{Q})) \subset \ker(\pi')$$

and so the map π' factors through $R^{\otimes 4}/I(R,\mathbb{Z}) = G(R,\mathbb{Z})$, as claimed.

By Theorem 1 and Proposition 19, the $\mathbb{F}_p$-algebra $G(R/\mathbb{Z}) \otimes \mathbb{F}_p$ is isomorphic to $G(\bar{R}/\mathbb{F}_p)$ and so has rank 32 as an $\mathbb{F}_p$-module. Now, by functoriality of the S_4-closure, the $\mathbb{F}_p$-module $G(\bar{R}/\mathbb{F}_p)$ is naturally a representation of the group $\mathrm{Aut}_{\mathbb{F}_p}(\bar{R}) = \mathrm{GL}_3(\mathbb{F}_p)$, and also of S_4, over $\mathbb{F}_p$, and hence (since these actions commute) of the group $\Gamma = S_4 \times \mathrm{GL}_3(\mathbb{F}_p)$. Thus, by properties (b) and (c), we see that $G'(\bar{R}/\mathbb{F}_p) \cong G'(R/\mathbb{Z}) \otimes \mathbb{F}_p$ is a Γ-equivariant quotient of $G(\bar{R}/\mathbb{F}_p) \cong G(R/\mathbb{Z}) \otimes \mathbb{F}_p$.

We use $\underline{\mathrm{triv}}$ and $\underline{\mathrm{std}}$ to denote the trivial representation and the standard three-dimensional representation of $\mathrm{GL}_3(\mathbb{F}_p)$, respectively. Also, we write triv, sgn, std, std$'$, and std$_2$ to denote the trivial, sign, standard, standard $\otimes$ sign, and 2-dimensional S_3-standard representation of S_4, respectively. These representations are irreducible over $\mathbb{F}_p$ since $p \geq 5$. From the proof of Proposition 19, we have the following decomposition of $G(\bar{R}/\mathbb{F}_p)$ into irreducible Γ-representations:

$$\begin{aligned} G(\bar{R}/\mathbb{F}_p) \cong\ & (\mathrm{triv} \otimes \underline{\mathrm{triv}}) \oplus (\mathrm{std} \otimes \underline{\mathrm{std}}) \oplus (\mathrm{std}_2 \otimes \underline{\mathrm{std}}) \oplus (\mathrm{std}' \otimes \underline{\mathrm{std}}^\vee) \\ & \oplus (\mathrm{std}_2 \otimes \underline{\mathrm{std}}^\vee) \otimes (\mathrm{sgn} \otimes \underline{\mathrm{triv}}). \end{aligned} \tag{32}$$

The $\mathbb{F}_p$-dimensions of these irreducible summands are 1, 9, 6, 9, 6, and 1 respectively, giving a total of 32. The first triv $\otimes$ $\underline{\mathrm{triv}}$ corresponds to the subring $\mathbb{F}_p \subset \bar{R}$; we then observe that no sum of any subset of elements of $\{9, 6, 9, 6, 1\}$ adds up to 8, and thus $G(\bar{R}/\mathbb{F}_p)$ has no Γ-equivariant quotient ring of rank 24 over $\mathbb{F}_p$. This proves the theorem in the case $n = 4$.

A similar argument holds also when $n > 4$. Let K be a degree n field extension of $\mathbb{Q}$ with associated Galois group S_n, and let $\mathcal{O}_K$ denote the ring of integers of K. Let $p > n$ be a prime such that $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p^{n-4} \times Q$ for some quartic $\mathbb{F}_p$-algebra Q (such a prime p exists in any S_n-number field K of degree n by the Chebotarev density theorem). Then $\mathbb{F}_p^{n-3}$ is a subring of $\mathcal{O}_K/p\mathcal{O}_K$. Let T be the preimage of the subring $\mathbb{F}_p^{n-3} \subset \mathcal{O}_K/p\mathcal{O}_K$ in $\mathcal{O}_K$, and let R be the ring $T + p\mathcal{O}_K$. Then $\bar{R} := R \otimes \mathbb{F}_p \cong \mathbb{F}_p^{n-4} \times \mathbb{F}_p[x, y, z]/(x, y, z)^2$.

By the identical argument as in the case $n = 4$, we may deduce that $G'(R/\mathbb{Z})$ is a quotient of $G(R/\mathbb{Z})$. Furthermore, by Theorem 1, the $\mathbb{F}_p$-algebra $G(R/\mathbb{Z}) \otimes \mathbb{F}_p$ is isomorphic to $G(\bar{R}/\mathbb{F}_p)$, and hence it has rank $32(n!/24)$ as an $\mathbb{F}_p$-module by Proposition 19 and Theorem 6. By the proof of Theorem 6, the action of S_n on $G(\bar{R}/\mathbb{F}_p)$ is that induced from the action of S_4 on $G(\mathbb{F}_p[x, y, z]/(x, y, z)^2/\mathbb{F}_p)$. Let $G'_1, \ldots, G'_{n!/24}$ denote the images in $G'(\bar{R}/\mathbb{F}_p)$ of the $n!/24$ copies of $G(\mathbb{F}_p[x, y, z]/(x, y, z)^2/\mathbb{F}_p)$ in $G(\bar{R}/\mathbb{F}_p)$. Then G'_1 yields a Γ-equivariant quotient of $G(\mathbb{F}_p[x, y, z]/(x, y, z)^2/\mathbb{F}_p)$ having rank 24. This is again a contradiction. $\square$

11. The maximal rank of S_n-closures

The purpose of this section is to show that the analogues for general n of the maximally degenerate ring of rank 4 (considered in Section 9) form the rings whose S_n-closures have maximal rank. Thus we prove Theorem 8.

The idea of our proof is as follows. In a sense which we make precise below, the ring $R_n = K[x_1, \dots, x_{n-1}]/(x_1, \dots, x_{n-1})^2$ is the "maximally degenerate point" in the moduli space of all rank n rings over K. Since Theorem 1 shows that the S_n-closures of rank n rings fit together into a nicely behaved sheaf on the moduli space, an upper semicontinuity argument allows us to conclude that the rank of the S_n-closure is maximal at the degenerate ring R_n.

As in [17], let $\mathfrak{B}_n$ be the functor from $\mathbf{Schemes}^{\mathrm{op}}$ to **Sets** which assigns to any scheme S the set of isomorphism classes of pairs $(\mathcal{A}, \phi)$, where $\mathcal{A}$ is an $\mathcal{O}_S$-algebra and $\phi : \mathcal{A} \to \mathcal{O}_S^n$ is an isomorphism of $\mathcal{O}_S$-modules. By [17, Prop. 1.1], the functor $\mathfrak{B}_n$ is representable by an affine scheme of finite type over $\mathbb{Z}$.

The base change $\mathfrak{B}_{n,K}$ of $\mathfrak{B}_n$ to Spec K is affine. Write $\mathfrak{B}_{n,K} = \operatorname{Spec} B_n$. The identity morphism from $\mathfrak{B}_{n,K}$ to itself yields a distinguished isomorphism class of pairs (A_n, ϕ) with A_n a B_n-algebra and $\phi : A_n \to B_n^n$ an isomorphism. Let us choose an object (A_n, ϕ) of this isomorphism class. Since we are interested in proving a statement about dimension, this choice does not matter. Since the S_n-closure $G(A_n/K)$ of A_n is a finitely-generated B_n-module, it defines a coherent sheaf $\mathcal{F}_n$ on $\mathfrak{B}_{n,K}$. By Theorem 1, if we have a morphism $f : \operatorname{Spec} C \to \mathfrak{B}_{n,K}$ corresponding to the pair (R, ψ), then $f^*\mathcal{F}_n$ is isomorphic to $G(R/C)$.

Note that there is a natural $\mathrm{GL}_{n,K}$-action on $\mathfrak{B}_{n,K}$ and that Theorem 1 shows that it extends to an action on the sheaf $\mathcal{F}_n$. The proof of [17, Prop. 7.1] shows that the K-point corresponding to R_n is in the Zariski closure of the $\mathrm{GL}_{n,K}$-orbit of any other point. Upper semicontinuity therefore shows that the dimension of the fiber of $\mathcal{F}_n$ is maximal at the point corresponding to R_n, as desired.

12. The S_n-closures of the degenerate rings R_n

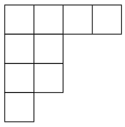
12.1. Preliminaries from S_n-representation theory

In this subsection, we collect several facts from S_n-representation theory that we use in the proof of Theorem 9 (made more precise in Theorem 27).

For us, given a positive integer n, a *partition of n* is an n-tuple $\lambda = (\lambda_1, \dots, \lambda_n)$ satisfying $n \geq \lambda_1 \geq \cdots \geq \lambda_n \geq 0$ and $\sum \lambda_i = n$. We often drop the $\lambda_i = 0$ in our notation, so that the partition $(3, 1, 0, 0)$ of 4, for example, is denoted simply as $(3, 1)$. Partitions of n play a key role in S_n-representation theory due to the following theorem (see, for example, [13, §2.1.12]).

Theorem 22. *If K is a field of characteristic 0 or of characteristic $p > n$, then there is a canonical bijection between the set of partitions of n and the set of isomorphism classes of irreducible S_n-representations over K.*

Given a partition μ, we denote by V_μ the corresponding irreducible S_n-representation. The V_μ are called Specht modules and can, in fact, be defined over the integers. We associate to μ a *Young diagram*, which consists of n rows of boxes with μ_i boxes on the i-th row. For example, the Young diagram of $\mu = (4, 2, 2, 1)$ is



A *generalized Young tableau of shape* μ is a function f which assigns a positive integer to every box of the Young diagram of μ. We depict f by drawing the Young diagram of μ and filling in each box with the positive integer assigned to it by f. For example,

1	2	1	2
3	2	4	
3	5		

is a generalized Young diagram of shape $(4, 3, 2)$. If λ is another partition of n, then we say f is a *Young tableau of shape* μ *and content* λ if f assigns the number i to exactly λ_i boxes. Such a Young tableau is called *semistandard* if the numbers assigned to the boxes of the Young diagram of μ weakly increase across rows and strongly increase down columns. For example, both

1	1	1	1	2
2	3	4		
3				

and

1	1	1	2	3
1	2	4		
3				

are Young tableaux of shape $(5, 3, 1)$ and content $(4, 2, 2, 1)$, but only the first is semistandard. The *Kostka number* $K_{\mu\lambda}$ is defined to be the number of semistandard Young tableaux of shape μ and content λ.

Definition 23. If λ and μ are two partitions of n, we say μ *dominates* λ and write $\mu \rhd \lambda$ if $\sum_{i=1}^{j} \mu_i \geq \sum_{i=1}^{j} \lambda_i$ for all j.

Note that in order for a Young tableau of shape μ and content λ to be semistandard, the λ_i boxes containing the number i must be in the first i rows. So, if μ does not dominate λ, then $K_{\mu\lambda} = 0$. The importance of the Kostka numbers is seen in Young's Rule below (for a proof, see [8, Cor. 4.39]).

Theorem 24 (Young's Rule). *If* λ *is a partition of* n*, then*

$$\mathrm{Ind}_{S_{\lambda_1} \times \cdots \times S_{\lambda_n}}^{S_n}(\mathrm{triv}) = \bigoplus_{\mu \rhd \lambda} K_{\mu\lambda} V_\mu.$$

In particular, since

$$K[S_n] = \mathrm{Ind}_{S_1\times\cdots\times S_1}^{S_n}(\mathrm{triv})$$

we see that $K_{\mu\lambda} = \dim V_\mu$, where $\lambda = (1, \ldots, 1)$.

There is a second combinatorial theorem we later make use of. This theorem, known as the hook formula, gives another way to relate $\dim V_\lambda$ to the Young diagram of λ.

Definition 25. The *hook number* of the j-th box in the i-th row of the Young diagram of λ is $1 + \lambda_i - j + |\{k : k > i, \lambda_k \geq \lambda_i\}|$. That is, it is the number boxes in the "hook" which runs up the j-th column, stops at the box in question, and continues across the i-th row to the right.

For example, replacing each box in the Young diagram of $(4, 2, 2, 1)$ by its hook number, we have

$$\begin{array}{|c|c|c|c|}\hline 7 & 5 & 2 & 1 \\ \hline 4 & 2 \\ \cline{1-2} 3 & 1 \\ \cline{1-2} 1 \\ \cline{1-1}\end{array}$$

Theorem 26 (Hook Formula). *Given a partition λ of n, let H be the product of the hook numbers of the boxes in the Young diagram of λ. Then* $\dim V_\lambda = n!/H$.

For a proof, see [19, Thm. 3.10.2].

12.2. A structure theorem for S_n-closures of degenerate rings

Throughout this subsection, K is a field of characteristic 0 or of characteristic $p > n$, and R_n denotes the degenerate ring $K[x_1, \ldots, x_{n-1}]/(x_1, \ldots, x_{n-1})^2$. Then $R_n^{\otimes n}$ is a K-vector space of dimension n^n with basis $x_{i_1} \otimes \cdots \otimes x_{i_n}$, where $i_j \in \{0, \ldots, n-1\}$ and $x_0 := 1$. For notational convenience, we drop the tensor signs and let $I := I(R_n, K)$. Our goal in this subsection is to prove

Theorem 27. *For each partition λ of n, let m_λ be the multinomial coefficient $\binom{n-1}{k_0;\ldots;k_{n-1}}$, where $k_j = |\{i : i \neq 1,\ \lambda_i = j\}|$. Then there is an isomorphism*

$$G(R_n/K) \cong \bigoplus_{\substack{\mu \rhd \lambda \\ \mu_1 = \lambda_1}} m_\lambda K_{\mu\lambda} V_\mu$$

of S_n-representations over K.

As we will show in Theorem 37, the theorem above implies that the dimension of $G(R_n/K)$ over K is greater than $n!$ for $n \geq 4$; that is, it implies Theorem 9. As a first step in proving Theorem 27, we begin by crudely decomposing $G(R_n/K)$ into certain naturally occurring S_n-representations parametrized by partitions of n.

Definition 28. Given an ordered partition $a = (a_0, a_1, \ldots, a_{n-1})$ of n, let M_a be the subrepresentation of $R_n^{\otimes n}$ spanned as a K-vector space by the elements $x_{i_1} \cdots x_{i_n}$ with $|\{j : i_j = k\}| = a_k$.

For example, writing x and y for x_1 and x_2, respectively, if $a = (1, 2, 1)$, then M_a spanned over K by the 12 elements $1xxy$, $1xyx$, $1yxx, \ldots, xx1y$, and $xxy1$. Note that

$$R_n^{\otimes n} = \bigoplus_a M_a$$

as S_n-representations.

Let $\gamma(x_i, x_{i_1} \cdots x_{i_n}) = \gamma_1(x_i, x_{i_1} \cdots x_{i_n}) \in R_n^{\otimes n}$ where, for any $j \in \{1, \ldots, n\}$, we set

$$\gamma_j(x_i, x_{i_1} \cdots x_{i_n}) \;=\; x_{i_1} \cdots x_{i_n} \cdot \sum_{1 \le i_1 < \cdots < i_j \le n} x_i^{(i_1)} \cdots x_i^{(i_j)}. \tag{33}$$

Note that all such $\gamma_j(x_i, x_{i_1} \cdots x_{i_n})$ are in I, because $s_j(x_i) = 0$.

Definition 29. Given an ordered partition a of n, let I_a be the K-vector subspace of I generated by all $\gamma(x_i, x_{i_1} \cdots x_{i_n}) \in M_a$ with $i > 0$.

For example, again writing x and y for x_1 and x_2, if $a = (1, 2, 1)$ then I_a is generated by the six elements $\gamma(y, 11xx), \gamma(y, 1x1x), \ldots, \gamma(y, xx11)$ as well as the 12 elements $\gamma(x, 11xy), \gamma(x, 1x1y), \ldots, \gamma(x, yx11)$.

Lemma 30. *If a is an ordered partition of n, then $I \cap M_a = I_a$, and so*

$$G(R_n/K) = \bigoplus_a M_a/I_a.$$

Proof. Clearly, I_a is contained in $I \cap M_a$. To prove the other containment, let $\beta \in I \cap M_a \subset I$. By Section 2, I is generated as an ideal by the elements $\gamma_j(x_i, 11 \cdots 1)$ with $i, j > 0$, and therefore as a K-vector space by the $x_{i_1} \cdots x_{i_n} \cdot \gamma_j(x_i, 11 \cdots 1) = \gamma_j(x_i, x_{i_1} \cdots x_{i_n})$ with $i, j > 0$. Since each $\gamma_j(x_i, x_{i_1} \cdots x_{i_n})$ is contained in $M_{a'}$ for some ordered partition a' of n, we see that β can be expressed as a K-linear combination of the various $\gamma_j(x_i, x_{i_1} \cdots x_{i_n}) \in M_a$.

To prove the lemma, it remains to show that the $\gamma_j(x_i, x_{i_1} \cdots x_{i_n}) \in I_a$ for $j \in \{1, \ldots, n\}$ can be expressed as K-linear combinations of the $\gamma(x_i, x_{i_1} \cdots x_{i_n}) \in I_a$. To see this, it suffices to note that $\gamma_j(x_i, x_{i_1} \cdots x_{i_n}) \in I_a$, for any $j \in \{1, \ldots, n\}$, can be expressed as

$$\gamma_j(x_i, x_{i_1} \cdots x_{i_n}) = \frac{1}{j} \cdot \gamma_{j-1}(x_i, x_{i_1} \cdots x_{i_n}) \cdot \sum_{k=1}^{n} x_i^{(k)}.$$

It follows by induction on j that any $\gamma_j(x_i, x_{i_1} \cdots x_{i_n}) \in M_a$ ($j \in \{1, \ldots, n\}$) can be expressed as a K-linear combination of the $\gamma(x_i, x_{i_1} \cdots x_{i_n}) \in I_a$, proving the lemma. □

Our next lemma shows that if $a_0 < a_k$ for some k, then $M_a = I_a$.

Lemma 31. *Let $i_1, \ldots, i_n \in \{0, 1, \ldots, n-1\}$. If there is some k such that*

$$|\{j : i_j = 0\}| < |\{j : i_j = k\}|,$$

then $x_{i_1} \cdots x_{i_n} \in I$.

Since the notation in the proof of this lemma is a bit cumbersome, we first illustrate the proof with a specific example. Denoting x_1, x_2, and x_3 by x, y, and z, respectively, let us show $1yx1xzyx \in I$. For $a, b, c \in S := \{1, 3, 4, 5, 8\}$, let $[a, b, c]$ denote $x_{i_1} \cdots x_{i_8}$ with $i_a = i_b = i_c = 1$, $i_2 = i_7 = 2$, $i_6 = 3$, and all other $i_j = 0$. For example, $[1, 3, 4] = xyxx1zy1$ and $[3, 5, 8] = 1yx1xzyx$. By the inclusion-exclusion principle, we have

$$\begin{aligned} 1yx1xzyx &= \sum_{\substack{a<b<c\\ a,b,c\in S}} [a,b,c] - \sum_{\substack{a<b\\ a,b\in S-\{1\}}} [1,a,b] - \sum_{\substack{a<b\\ a,b\in S-\{4\}}} [4,a,b] + \sum_{a\in S-\{1,4\}} [1,4,a] \\ &= \gamma_3(x, 1y111zy1) - \gamma_2(x, xy111zy1) - \gamma_2(x, 1y1x1zy1) + \gamma_1(x, xy1x1zy1). \end{aligned}$$

Hence $1yx1xzyx \in I$.

Proof of Lemma 31. Let $S = S_0 \cup S_k$, where $S_0 = \{j : i_j = 0\}$ and $S_k = \{j : i_j = k\}$. Then, by the inclusion-exclusion principle, we have

$$\begin{aligned} x_{i_1} \cdots x_{i_n} = \prod_j x_{i_j}^{(j)} &= \sum_{U \subset S_0} (-1)^{|U|} \sum_{\substack{U\subset T\subset S\\ |T|=|S_k|}} \prod_{j\in T} x_k^{(j)} \prod_{j\notin S} x_{i_j}^{(j)} \\ &= \sum_{U\subset S_0} (-1)^{|U|} \gamma_{|S_k|-|U|}\Big(x_k, \prod_{j\in U} x_k^{(j)} \prod_{j\notin S} x_{i_j}^{(j)}\Big). \qquad (34) \end{aligned}$$

Hence $x_{i_1} \cdots x_{i_n} \in I$. □

We see from Lemma 31 that

$$G(R_n/K) = \bigoplus_{\substack{a \text{ with}\\ a_0 \geq a_k \,\forall k}} M_a/I_a.$$

If σ is a permutation of $\{0, 1, \ldots, n-1\}$, and $a = (a_0, \ldots, a_{n-1})$ is an ordered partition of n, then let $\sigma(a) := (a_{\sigma^{-1}(0)}, \ldots, a_{\sigma^{-1}(n-1)})$. Note that if σ fixes 0, then it defines an isomorphism of S_n-representations $M_a \to M_{\sigma(a)}$ by sending $x_{i_1} \cdots x_{i_n}$ to $x_{\sigma(i_1)} \cdots x_{\sigma(i_n)}$. We remark that if σ does not fix 0, it still defines an isomorphism of vector spaces, but this is in general not an isomorphism of S_n-representations. Now let $a = (a_0, \ldots, a_{n-1})$ be an ordered partition of n such that $a_0 \geq a_k$ for all k. For all $j \in \{0, \ldots, n-1\}$, let $k_j = |\{i : i \neq 0,\ a_i = j\}|$. Then $\{\sigma(a) : \sigma(0) = 0\}$ has cardinality $\binom{n-1}{k_0;\ldots;k_{n-1}} = m_{\lambda(a)}$, where $\lambda(a) := (\lambda_1, \ldots, \lambda_n)$ is the (unordered) partition of n such that $\{\lambda_i : 1 \leq i \leq n\} = \{a_i : 0 \leq i \leq n-1\}$ as multisets.

Definition 32. For any partition λ of n, let M_λ and I_λ denote the isomorphism classes of the S_n-representations M_a and I_a, respectively, where $a = (a_0, \ldots, a_{n-1})$ is any ordered partition of n such that $a_0 = \lambda_1$ and $\{\lambda_i\} = \{a_i\}$ as multisets. This is well-defined as $\lambda(a) = \lambda(\sigma(a))$ for all σ fixing 0.

Since each partition λ corresponds to m_λ ordered partitions a in the above definition, we obtain

Proposition 33. *For all partitions λ of n, let m_λ be the multinomial coefficient $\binom{n-1}{k_0;\ldots;k_{n-1}}$, where $k_j = |\{i : i \neq 1,\ \lambda_i = j\}|$. Then there is an isomorphism*

$$G(R_n/K) \cong \bigoplus_\lambda m_\lambda M_\lambda/I_\lambda$$

of S_n-representations.

Given a partition λ of n, let $i_j = k$ if $\sum_{m=1}^{k-1} \lambda_m < j \leq \sum_{m=1}^{k} \lambda_m$. Then note that

$$M_\lambda = \mathrm{Ind}_{S_{\lambda_1}\times\cdots\times S_{\lambda_n}}^{S_n}(K \cdot x_{i_1}\cdots x_{i_n}).$$

Since $K \cdot x_{i_1}\cdots x_{i_n}$ is the trivial representation of $S_{\lambda_1}\times\cdots\times S_{\lambda_n}$, by Young's Rule we have

$$M_\lambda \cong \bigoplus_{\mu \rhd \lambda} K_{\mu\lambda} V_\mu, \tag{35}$$

where λ runs through the partitions of n. We have therefore reduced Theorem 27 to the following:

Theorem 34. *For all partitions λ of n, we have*

$$I_\lambda \cong \bigoplus_{\substack{\mu \rhd \lambda \\ \mu_1 > \lambda_1}} K_{\mu\lambda} V_\mu$$

as S_n-representations.

To prove Theorem 34, we show that I_λ contains $K_{\mu\lambda}$ copies of V_μ if $\mu \rhd \lambda$ and $\mu_1 > \lambda_1$, and that it contains no copy of V_μ if $\mu \rhd \lambda$ but $\mu_1 = \lambda_1$. These two statements are the content of Propositions 35 and 36, respectively.

Proposition 35. *If λ and μ are partitions of n with $\mu_1 > \lambda_1$, then the natural morphism of S_n-representations*

$$\mathrm{Hom}(V_\mu, I_\lambda) \to \mathrm{Hom}(V_\mu, M_\lambda)$$

is an isomorphism.

Proof. Given a semistandard Young tableau T of shape μ and content λ, if $i = j + \sum_{m=1}^{k-1} \lambda_m < \sum_{m=1}^{k} \lambda_m$ for $j > 0$, then let $T(i)$ be the number assigned to the j-th box on the k-th row of T. For example, $T(\lambda_1+1)$ is the number assigned to the first box of the second row. We can associate to T an element $\alpha(T) := x_{T(1)-1}\cdots x_{T(n)-1}$ of M_λ. Let A_T be the set of Young tableaux T' of shape μ and content λ such that for all i, the multiset of numbers in the i-th row of T' is the same as the multiset of numbers in the i-th row of T. Then by [19, 2.10.1], the image of any morphism $V_\mu \to M_\lambda$ of S_n-representations is contained in the S_n-subspace of M_λ generated by the elements $\sum_{T'\in A_T} \alpha(T')$ as T ranges over the semistandard Young tableaux of shape μ and content λ.

It therefore suffices to show $\sum_{T'\in A_T} \alpha(T') \in I_\lambda$ for every semistandard Young tableau T of shape μ and content λ. We define an equivalence relation on A_T by $T' \sim T''$

if $T'(i) = T''(i)$ for all $i > \mu_1$. This equivalence relation partitions A_T into a disjoint union of sets $S_1, \ldots, S_\ell$. For $i > \mu_1$, let $S_j(i) = T'(i)$ for any $T' \in S_j$. Since

$$\sum_{T' \in A_T} \alpha(T') = \sum_{j=1}^{\ell} \sum_{T' \in S_j} \alpha(T'),$$

it suffices to show that each $\sum_{T' \in S_j} \alpha(T')$ is in I_λ. Note that

$$\sum_{T' \in S_j} \alpha(T') = \delta \cdot (\underbrace{1 \cdots 1}_{\mu_1} x_{S_j(\mu_1+1)-1} \cdots x_{S_j(n)-1}),$$

where δ is the sum of all elements of the form $x_{i_1} \cdots x_{i_n}$ with

$$\{i_k\} = \{T(k) - 1 : 1 \le k \le \mu_1\} \cup \{\underbrace{0, \ldots, 0}_{n-\mu_1}\}$$

as multisets. Letting $a_m = |\{k : i_k = m\}|$ and noting that there is some $m \neq 0$ for which $a_m > 0$, we see that

$$\delta = \prod_{m=1}^{n-1} \gamma_{a_m}(x_m, 1 \cdots 1) \in I_\lambda,$$

which finishes the proof. □

Proposition 36. *If $\mu \rhd \lambda$ and $\mu_1 = \lambda_1$, then V_μ does not occur in I_λ.*

Proof. Let Γ_m be the subrepresentation of I_λ generated by the $\gamma(x_m, x_{i_1} \cdots x_{i_n}) \in I_\lambda$. Let ℓ be the smallest integer greater than or equal to m such that $\lambda_m = \lambda_\ell > \lambda_{\ell+1}$. If $\lambda_m = \lambda_j$ for all $j \ge m$, then let $\ell = n$. We define

$$\lambda' = (\lambda'_1, \ldots, \lambda'_n) = (\lambda_1 + 1, \lambda_2, \ldots, \lambda_{\ell-1}, \lambda_\ell - 1, \lambda_{\ell+1}, \ldots, \lambda_n).$$

Let $i_j = m$ if $\sum_{b=1}^{m} \lambda'_b < j \le \sum_{b=1}^{m+1} \lambda'_b$. Then note that

$$\Gamma_m = \mathrm{Ind}_{S_{\lambda'_1} \times \cdots \times S_{\lambda'_n}}^{S_n} (K \cdot \gamma(x_m, x_{i_1} \cdots x_{i_n})).$$

Since $K \cdot \gamma(x_m, x_{i_1} \cdots x_{i_n})$ is the trivial representation of $S_{\lambda'_1} \times \cdots \times S_{\lambda'_n}$, Young's Rule tells us that

$$\Gamma_m = \bigoplus_{\epsilon \rhd \lambda'} K_{\epsilon\lambda'} V_\epsilon.$$

Since $\lambda'_1 = \lambda_1 + 1$, any ϵ which dominates λ' must have $\epsilon_1 > \lambda_1$. Therefore V_μ does not occur in any of the Γ_m, and since I_λ is the K-vector space span of the Γ_m, we conclude that V_μ does not occur in I_λ. □

This concludes the proof of Theorem 34, and hence also of Theorem 27. We now turn to the following theorem, which implies Theorem 9.

Theorem 37. *The regular representation is a subrepresentation of* $G(R_n/K)$. *If* $n \geq 4$, *it is a proper subrepresentation.*

As the proof of this theorem shows, as n gets large, the regular representation is only a small subrepresentation, and so the bound in Theorem 9 is a weak one.

Lemma 38. *Let* ϵ *and* τ *be two partitions of* n. *Suppose* $\tau_{k-1} > \tau_k = 0$ *and* $\epsilon = (\tau_1, \ldots, \tau_{i-1}, \tau_i - 1, \tau_{i+1}, \ldots, \tau_{k-1}, 1)$ *for some* $i > 1$. *Let* E_1 *and* T_1 *be the products of the hook numbers of the boxes in the first rows of the Young diagrams of* ϵ *and* τ, *respectively. Then* $T_1 \geq E_1$.

Proof. Let h_1 and h_2 be the hook numbers of the first and the τ_i-th box, respectively, in the first row of the Young diagram of τ. Then

$$E_1 = T_1 \frac{(h_1+1)(h_2-1)}{h_1 h_2}.$$

Expanding $(h_1+1)(h_2-1)$, and noting that $h_1 > h_2$, yields the desired inequality. □

Proof of Theorem 37. We must show that

$$\sum_{\substack{\mu \rhd \lambda \\ \mu_1 = \lambda_1}} m_\lambda K_{\mu\lambda} \geq \dim V_\mu.$$

Fix μ and let $\lambda = (\mu_1, 1, \ldots, 1)$. We in fact prove that $m_\lambda K_{\mu\lambda} \geq \dim V_\mu$.

If $\mu = (n)$, then $\lambda = \mu$ and $m_\lambda K_{\mu\lambda} = 1 = \dim V_\mu$. Now suppose $\mu_1 < n$. Let $\mu' = (\mu_2, \ldots, \mu_n)$ and $\lambda' = (\lambda_2, \ldots, \lambda_n)$. Since $\mu_1 = \lambda_1$, the first row of every semistandard Young tableau of shape μ and content λ consists entirely of 1's. Therefore,

$$K_{\mu\lambda} = K_{\mu'\lambda'} = \dim V_{\mu'},$$

where the second equality comes from the paragraph following Theorem 24. Let H be the product of the hook numbers of the Young diagram of μ and let H_1 be the product of the hook numbers of the boxes in the first row. Since

$$\dim V_\mu = \frac{n!}{H} = \dim V_{\mu'} \cdot \frac{n!}{H_1 (n-\mu_1)!}$$

and $m_\lambda = \binom{n-1}{\mu_1 - 1}$, we need only show $H_1 \geq n(\mu_1 - 1)!$. Note that the product of the hook numbers of the boxes in the first row of the Young diagram of λ is $n(\mu_1 - 1)!$. The first part of the theorem therefore follows by successively applying Lemma 38.

Note that if $n \geq 4$, then letting $\mu = (n-2, 2)$ and $\lambda = (n-2, 1, 1)$, we obtain

$$\sum_{\substack{\mu \rhd \lambda \\ \mu_1 = \lambda_1}} m_\lambda K_{\mu\lambda} = m_\lambda K_{\mu\lambda} + m_\mu K_{\mu\mu} > \dim V_\mu,$$

which shows that the regular representation is a proper subrepresentation. □

12.3. Examples

In this section we illustrate Theorem 27 in the cases $n = 3$ and $n = 4$. The following table collects the relevant information when $n = 3$.

μ	$\dim V_\mu$	λ with $\lambda_1 = \mu_1$ and $\mu \rhd \lambda$	m_λ	$K_{\mu\lambda}$	$m_\lambda K_{\mu\lambda}$
$\ydiagram{3}$	1	$\ydiagram{3}$	1	1	1
$\ydiagram{2,1}$	2	$\ydiagram{2,1}$	2	1	2
$\ydiagram{1,1,1}$	1	$\ydiagram{1,1,1}$	1	1	1

We see that for each partition μ of 3, the dimension of V_μ agrees with $m_\mu K_{\mu\mu}$ and so Theorem 27 shows that $G(R_3/K)$ is the regular representation.

The cases $n \leq 3$ are rather uninteresting since for such n, whenever μ and λ are partitions of n with μ dominating λ and $\lambda_1 = \mu_1$, we in fact have $\mu = \lambda$. When $n = 4$, however, there exists a single pair (μ, λ) of partitions satisfying the above conditions for which μ and λ are distinct. As shown in Theorem 37, this forces $G(R_4/K)$ to properly contain a copy of the regular representation. The $n = 4$ case is summarized in the table below.

μ	$\dim V_\mu$	λ with $\lambda_1 = \mu_1$ and $\mu \rhd \lambda$	m_λ	$K_{\mu\lambda}$	$m_\lambda K_{\mu\lambda}$
$\ydiagram{4}$	1	$\ydiagram{4}$	1	1	1
$\ydiagram{3,1}$	3	$\ydiagram{3,1}$	3	1	3
$\ydiagram{2,2}$	2	$\ydiagram{2,2}$	3	1	3
		$\ydiagram{2,1,1}$	3	1	3
$\ydiagram{2,1,1}$	3	$\ydiagram{2,1,1}$	3	1	3
$\ydiagram{1,1,1,1}$	1	$\ydiagram{1,1,1,1}$	1	1	1

We then see from Theorem 27 that $G(R_4/K)$ contains exactly $\dim V_\mu$ copies of V_μ for every partition μ of 4 other than $\mu = (2, 2)$. We see, however, that $G(R_4/K)$ contains six copies of $V_{(2,2)}$. It follows that $G(R_4/K)$ is the regular representation direct sum of four copies of $V_{(2,2)}$. Since $V_{(2,2)}$ is 2-dimensional, we see $G(R_4/K)$ has dimension $24 + 8 = 32$.

Let us now reconcile the decomposition of $G(R_4/K)$ given by Theorem 27 with the explicit decomposition given in Section 9. We make no assumption here on the characteristic of K. Recall that $T(x)$ has generators x_i for $1 \leq i \leq 4$ satisfying the relation $\sum x_i = 0$ and that $\sigma \in S_4$ acts by $\sigma(x_i) = x_{\sigma(i)}$. We then see that $T(x)$ is the standard representation; that is, $T(x) \cong V_{(3,1)}$. Recall that $U(x)$ is a two-dimensional vector space generated by the equivalence classes of

$$x_1y_2 + x_2y_1 + x_3y_4 + x_4y_3 \quad \text{and} \quad x_1y_3 + x_3y_1 + x_2y_4 + x_4y_2$$

with S_4-action given by $\sigma(x_i) = x_{\sigma(i)}$ and $\sigma(y_i) = y_{\sigma(i)}$. Letting H be the subgroup of S_4 generated by $(12)(34)$ and $(13)(24)$, we see that $U(x)$ is the S_4-representation obtained from the quotient $S_4 \to S_4/H \cong S_3$ and the standard representation of S_3. Hence, $U(x)$ is $V_{(2,2)}$. It is clear that $W(x, y, z)$ is the sign representation $V_{(1,1,1,1)}$. Lastly, one easily checks that the composition factors of $V(x, y)$ and $V_{(2,2)} \oplus V_{(2,1,1)}$ are the same; this follows, e.g., from an explicit computation using Brauer characters (see [22, Chpt. 7, Def. 2.7]). We then see that $G(R_4/K)$ has the same composition factors as

$$V_{(4)} \oplus V_{(3,1)}^{\oplus 3} \oplus V_{(2,2)}^{\oplus 6} \oplus V_{(2,1,1)}^{\oplus 3} \oplus V_{(1,1,1,1)};$$

that is, if we weaken Theorem 27 to only require that the two S_n-modules have the same composition factors, then it holds in arbitrary characteristic for $n \leq 4$.

13. Open questions

There are several questions about S_n-closures that have not been treated in this article, which beg for further investigation. First, we have the natural question:

Question 1. Is there a geometric definition of the S_n-closure?

The definition we have given in the introduction is rather algebraic. A more geometric definition would perhaps make various properties of the S_n-closure (such as the fact that it commutes with base change!) more apparent.

Second, we have only proven Theorem 27 in the case where the field K has characteristic prime to $n!$. However, we saw in Section 9 that even when K has characteristic 2 or 3, the dimension of $G(R_4/K)$ remains 32, which is precisely what Theorem 27 would imply in good characteristic. In Section 12.3, we saw in fact that $G(R_4/K)$ possesses the same composition factors in any characteristic. Does the analogous statement hold for $G(R_n/K)$ for higher values of n?

Question 2. Is it true, for a field K of arbitrary characteristic, that

$$G(R_n/K) \quad \text{and} \quad \bigoplus_{\substack{\mu \rhd \lambda \\ \mu_1 = \lambda_1}} m_\lambda K_{\mu\lambda} V_\mu$$

possess the same composition factors?

We have shown that the S_n-closure of an algebra A of rank n over a field K has dimension $n!$ in many natural cases, and that this dimension in any case is always bounded above by $\dim_K(G(R_n/K))$. What about a lower bound? One would guess that the rank could never go *below* $n!$, although this does not seem trivial to prove.

Question 3. If A is a ring of rank n over a field K, is the rank of $G(A/K)$ at least $n!$?

While we do not know the answer to this question in general, we show below that the answer is “yes” provided that n is small and the characteristic of K is not 2 or 3:

Proposition 39. *If $n \leq 7$, and A is a ring of rank n over a field K having characteristic not 2 or 3, then $G(A/K)$ has rank at least $n!$.*

Proof. By [17, Cor. 6.7] and the fact that $\mathfrak{B}_{n,K}$ is irreducible ([4, Thm. 1.1], which assumes K does not have characteristic 2 or 3), we see that the étale locus is dense in $\mathfrak{B}_{n,K}$. Theorem 4 shows that if A is étale over K, then the rank of $G(A/K)$ is $n!$. Therefore, an upper semicontinuity argument, similar to the one given in Theorem 8, finishes the proof. □

The argument of Proposition 39 does not extend to higher values of n because it is known that the étale locus is *not* dense in $\mathfrak{B}_{n,K}$ for $n \geq 8$; see [17, Prop. 9.6].

Another question stems from the following. In the Galois theory of fields, one often constructs Galois closures through certain natural intermediate extensions. Namely, suppose $L = K[x]/f(x)$ is a separable field extension of degree n with associated Galois group S_n, and $\tilde{L}$ is the splitting field of f (and thus the Galois closure of L over K). Then f has a root α_1 in L, and f has n roots $\alpha_1, \ldots, \alpha_n$ in the splitting field $\tilde{L}$. We may thus construct $\tilde{L}$ through a tower of extensions

$$L = L^{(1)} \subset \cdots \subset L^{(n)} = \tilde{L}$$

where $L^{(r)} := L(\alpha_1, \ldots, \alpha_r)$ has degree $n(n-1)\cdots(n-r+1)$ over L. The fields $L^{(r)}$ are well-defined up to isomorphism and independent of the ordering of the roots $\alpha_1, \ldots, \alpha_r$ of f.

Question 4. Let A be a ring of rank n over B. Is there a construction of “intermediate S_n-closures”

$$A = G^{(1)}(A/B), \quad G^{(2)}(A/B), \quad \ldots, \quad G^{(n)}(A/B) = G(A/B),$$

which commute with base change and are such that in the case of an S_n-extension of fields L/K of degree n, we have $G^{(r)}(L/K) \cong L^{(r)}$?

A natural method to proceed would be to construct $G^{(r)}(A/B)$ as a quotient of $A^{\otimes r}$ by an appropriate ideal $I^{(r)}(A,B)$, where $I^{(n)}(A,B)$ coincides with $I(A,B) \subset A^{\otimes n}$.

Finally, it is natural to ask whether Galois type closures can be obtained for groups other than S_n. If $G \subset S_n$ is a permutation group on n elements, then there should be an analogous way to define a "G-closure" for rank n rings with appropriate properties. In the case of separable field extensions A/B where $\mathrm{Gal}(\tilde{A}/B) \subset G$, this should then yield a B-algebra isomorphic to $\tilde{A}^{|G|/\deg(A/B)}$ as in Theorem 2.

Question 5. If $G \subset S_n$ is a permutation group, what is the natural class of rings/ schemes for which functorial G-closures can be defined?

Acknowledgements. We thank O. Biesel, J. Blasiak, T. Church, B. de Smit, J. Ellenberg, D. Erman, W. Ho, K. Kedlaya, H. Lenstra, J. Parson, B. Poonen, J.-P. Serre, C. Skinner, N. Snyder, S. Sun, L. Taelman, B. Viray, and M. Wood for numerous valuable conversations, comments, and suggestions which helped shape this article. We also thank the anonymous referee for a very careful reading and extremely helpful comments.

This paper was presented at a special Intercity Number Theory Day held in Leiden in honor of the 60th birthday of Hendrik Lenstra, and it is a pleasure to dedicate this paper to him.

References

[1] Amitsur, S. A.: On the characteristic polynomial of a sum of matrices. Linear Multilinear Algebra **8**, 177–182 (1980) Zbl 0429.15006 MR 0560557

[2] Bhargava, M.: Higher composition laws III: The parametrization of quartic rings. Ann. of Math. **159**, 1329–1360 (2004) Zbl 1169.11045 MR 2113024

[3] Bhargava, M.: Higher composition laws IV: The parametrization of quintic rings. Ann. of Math. **167**, 53–94 (2008) Zbl 1173.11058 MR 2373152

[4] Cartwright, D., Erman, D., Velasco, M., Viray, B.: Hilbert schemes of 8 points. Algebra Number Theory **3**, 763–795 (2009) Zbl 1187.14005 MR 2579394

[5] Delone, B. N., Faddeev, D. K.: The Theory of Irrationalities of the Third Degree. Transl. Math. Monogr. 10, Amer. Math. Soc. (1964) Zbl 0133.30202 MR 0160744

[6] Ferrand, D.: Un foncteur norme. Bull. Soc. Math. France **126**, 1–49 (1998) Zbl 1017.13005 MR 1651380

[7] Franc, C., Masdeu, M.: Étale Fundamental Groups and Cohomology. http://warwick.ac.uk/~masmat/files/notes/etalenotes.pdf

[8] Fulton, W., Harris, J.: Representation Theory: A First Course. Grad. Texts in Math., 129, Springer, New York (1991) Zbl 0744.22001 MR 1153249

[9] Gan, W.-T., Gross, B. H., Savin, G.: Fourier coefficients of modular forms on G_2. Duke Math. J. **115**, 105–169 (2002) Zbl 1165.11315 MR 1932327

[10] Gross, B. H., Lucianovic, M. W.: On cubic rings and quaternion rings. J. Number Theory **129**, 1468–1478 (2009) Zbl 1166.11034 MR 2521487

[11] Grothendieck, A.: Anneaux de Chow. Sém. Chevalley 1958, 4–19

[12] Hilbert, D.: Theory of Algebraic Invariants. Cambridge Univ. Press (1993) Zbl 0801.13001 MR 1266168

[13] James, G., Kerber, A.: The Representation Theory of the Symmetric Group. Encyclopedia Math. Appl. 16, Addison-Wesley, Reading, MA (1981) Zbl 1159.20012 MR 0644144

[14] Katz, N., Mazur, B.: Arithmetic Moduli of Elliptic Curves. Ann. of Math. Stud. 108, Princeton Univ. Press, Princeton, NJ (1985) Zbl 0576.14026 MR 0772569

[15] Lenstra, H. W.: Galois Theory for Schemes. Electronic 3rd edition, http://websites.math.leidenuniv.nl/algebra/GSchemes.pdf

[16] Milne, J. S.: Lectures on Étale Cohomology. http://www.jmilne.org/math/CourseNotes/LEC.pdf

[17] Poonen, B.: The moduli space of commutative algebras of finite rank. J. Eur. Math. Soc. **10**, 817–836 (2008) Zbl 1151.14011 MR 2421162

[18] Reutenauer, C., Schützenberger, M.-P.: A formula for the determinant of a sum of matrices. Lett. Math. Phys. **13**, 299–302 (1987) Zbl 0628.15005 MR 0895292

[19] Sagan, B.: The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions. Grad. Texts in Math. 203, Springer, New York (2001) Zbl 0964.05070 MR 1824028

[20] van der Waerden, B. L.: Algebra. Springer (2003)

[21] Vistoli, A.: Notes on Grothendieck topologies, fibered categories and descent theory. arXiv:math/0412512v4 (2007)

[22] Weintraub, S.: Representation Theory of Finite Groups: Algebra and Arithmetic. Grad. Stud. Math. 59, Amer. Math. Soc., Providence, RI (2003) Zbl 1078.20009 MR 1984740