

1. Let \mathcal{M} denote the ideal generated by all the monomials of $R = R_\beta$ of positive degree. We'll show that \mathcal{M} is not finitely generated. Suppose (m_i, n_i) , $1 \leq i \leq h$ are such that the $\mu_i = x^{m_i}y^{n_i}$ are generators. Then we can choose $\gamma > \beta$ such that $n_i > \gamma m_i$ for all i . Choose a monomial $\mu = x^n y^m$ of least total degree in R such $\beta m < n < \gamma m$. (Such monomials exist: one can choose n if m is so large that $m(\gamma - \beta) > 1$.) If μ is in the ideal generated by the μ_i , it must occur among the monomial multiples of the μ_i , since expanding $\sum_i f_i \mu_i$ for $f_i \in R$ gives a K -linear combination of such monomial multiples. Say $\mu = \nu \mu_i$ where $\nu = x^r y^s$. Then ν has smaller degree than μ , and we must have $\beta r < s < \gamma r$: the first inequality holds because $\nu \in R$, and the second inequality holds because if we have $s \geq \gamma r$, then since $n_i > \gamma m_i$, we can add to get $n = s + n_i > \gamma(r + m_i) = \gamma m$ a contradiction. But now we have contradicted the choice of μ of least degree. \square

2. Let $R = \mathbb{C}[xu, xv, yu, yv] \subseteq \mathbb{C}[x, y, u, v]$, where x, y, u, v are indeterminates. Let the four generators of R be q, r, s, t , respectively. They have the relation $qt - rs = 0$. If we use the generators q, r', s, t . Then we have the equation $qt - (r' - s)s = 0$ which is monic in s over $\mathbb{C}[q, r', t]$. (This corresponds to a very simple change of variables in $\mathbb{C}[q, r, s, t]$; many other changes of variable work.) Thus, R is module-finite with module generators $1, s$ over $\mathbb{C}[q, r', t]$, and it suffices to see that $q = xu, r' = xv + yu$, and $t = yv$ are algebraically independent over \mathbb{C} . This will follow if R has dimension at least three, which in turn follows from the algebraic independence of xu, xv, yu over \mathbb{C} , which holds even if we first map to $\mathbb{C}[u, v, y]$ by letting $x \mapsto 1$: the elements become u, v, yu and $\mathbb{C}(u, v, yu) = \mathbb{C}(u, v, y)$, since $y = yu/u$.

3. Consider the homogeneous polynomial F consisting of all terms of f of highest degree, say $d = \deg(f)$. What we need is for x_n^d to occur with non-zero coefficient in the image of F , which is $F(x_1 + \lambda_1 x_n, \dots, x_{n-1} + \lambda_{n-1} x_n, \lambda_n x_n)$. But the coefficient of x_n^d in this homogeneous polynomial can be recovered by substituting $x_1 = \dots = x_{n-1} = 0$ and $x_n = 1$, which gives $F(\lambda_1, \dots, \lambda_n)$. Since the polynomial $x_n F$ is not identically 0, and since the field is infinite, there a choice of the λ_j for which it does not vanish (this is proved in the second paragraph of the proof of the Theorem on p. 2 of the Lecture Notes from October 8), and this gives the desired automorphism. (The extra factor x_n is needed to guarantee $\lambda_n \neq 0$.) \square

4. (a) If the union were finitely generated, each generator would be in an ideal of the chain, and of these finitely many ideals one would be largest and contain all the generators of the union. But then it would be equal to the union and so finitely generated, a contradiction. \square (It is not enough to consider only countable chains in Zorn's lemma: e.g. the countable subsets of \mathbb{R} have the property that the union of every countable chain is countable, but there is no maximal element in the set of countable subsets of \mathbb{R} .)

(b) If the ideal P is not prime, choose $x, y \notin P$ such that $xy \in P$. Then $P + xR$ and $P + yR$ are both strictly larger than P (the latter contains $P + Ry$), and so have finite sets of generators, say $i_1 + r_1 x, \dots, i_n + r_n x$ for $P + xR$, where the $i_t \in P$ and the $r_n \in R$, and j_1, \dots, j_m for $P + yR$. We claim that $i_1, \dots, i_n, xj_1, \dots, xj_m$, which are in P , generate

P . To see this, suppose that $u \in P$. The $u \in P + xR$, and u is an R -linear combination of $i_t + r_t x$, which means that we can write u as an R -linear combination of the i_t plus a multiple of x , say $i + rx$ where $i \in (i_1, \dots, i_n)R$. Then $rx = u - i \in P$, so that $r \in J$, and thus r is an R -linear combination of the j_s , so that rx is an R -linear combination of the elements xj_s . \square

5. (a) If there is no solution over K , the polynomials must generate the unit ideal over K , since otherwise they are contained in a maximal ideal of the form m_x by Hilbert's Nullstellensatz, and this means that x gives a simultaneous solution. But then they cannot vanish simultaneously over the large field, since 1 is still a linear combination of the polynomials. \square

(b) Consider a polynomial $f \in K[x_1, \dots, x_n] - \{0\}$. Suppose that the degrees of the factors over L are m and n , so that f has degree $m + n$, where $m \geq 1$, $n \geq 1$. We can write down a polynomial of degree m with indeterminates A_i as coefficients, one for each monomial of degree $\leq m$, and another of degree n with new indeterminates B_j as coefficients. When we multiply these two we get a polynomial whose coefficients are (quadratic) polynomials in the A_i, B_j . We can look for a factorization, whether over K or over L , into factors of the specified degrees by setting these coefficients equal to the given scalar coefficients of f , which are in K . The system of equations one gets has coefficients in K . Factoring f with factors of the specified degrees over L or over K is equivalent to solving this system of polynomial equations in the specified field. By part (a), a solution in L implies a solution in K . \square (Here's an example: to factor $x^2 + 7x + 12$ into linear factors write $x^2 + 7x + 12 = (A_1x + A_2)(B_1x + B_2)$, and one is led to the system $A_1B_1 = 1$, $A_1B_2 + A_2B_1 = 7$, $A_2B_2 = 12$. The general case will have many more terms and equations, but the basic idea is the same.)

6. Multiplying the elements g_1, \dots, g_n on the left by $g \in G$ permutes them, and so the action of g permutes $g_1(r_j), \dots, g_n(r_j)$. Therefore the action of g fixes each elementary symmetric function e_{ij} of these, and so $R_0 \subseteq R^G$. Since one of the g_i is the identity, r_j is among the roots of $(x - g_1(r_j)) \cdots (x - g_n(r_j)) = 0$, whose coefficients are, up to sign, the e_{ij} . This shows that every r_j is integral over R_0 , and these generate R over R_0 , since they generate R even over $A \subseteq R_0$. Since R is integral over R_0 and finitely generated as an algebra, R is module-finite over R_0 . Since R_0 is Noetherian by the Hilbert Basis Theorem, every R_0 -submodule of R is finitely generated as an R_0 -module: this includes R^G , which is therefore finitely generated over R_0 and, hence, as an algebra over A . \square

EXTRA CREDIT If $s \in S$ is not integral over R , consider the set of all expressions $s^n + r_{n-1}s^{n-1} + \cdots + r_0$ as n varies and the r_j vary in R . The fact that s is not integral over R is equivalent to the statement that this set does not contain 0. Because the product of two monic polynomials is monic, these expressions form a multiplicative system not containing 0. Choose Q prime in S not meeting that multiplicative system. Then the image of s in S/Q is still not integral over $R/(Q \cap R)$. \square