DEDEKIND DOMAINS AND GALOIS RESIDUE FIELD EXTENSIONS

KEITH CONRAD

When L/K is an extension of number fields, every residue field extension $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ is Galois since the residue fields are finite and all finite extensions of finite fields are Galois extensions. However, residue field extensions associated to prime ideals in general Dedekind domains need not be Galois or even separable since the residue fields need not be perfect.

Example 1. Let $K = \mathbf{Q}(u)$ be a rational function field over $\mathbf{Q}$ and $A = \mathbf{Q}[u]$. At each prime in A, its residue field contains $\mathbf{Q}$, so it has characteristic 0. For each finite extension L of K, the residue field at a prime ideal in the integral closure of A is separable over the residue field at the prime below it in A since finite extensions in characteristic 0 are separable.

An example where residue field extensions need not be Galois extensions is $L = \mathbf{Q}(\sqrt[3]{u})$. Since $\sqrt[3]{u}$ is trancendental over $\mathbf{Q}$, the ring $B = \mathbf{Q}[\sqrt[3]{u}]$ is a PID, hence integrally closed, so B is the integral closure of A in L. The way a prime ideal $(\pi(u))$ in A decomposes in B matches how $x^3 - u \bmod \pi(u)$ decomposes in $(\mathbf{Q}[u]/(\pi(u)))[x]$.

For instance, if m in $\mathbf{Z}$ is not a cube then $A/(u-m) \cong \mathbf{Q}$ and $x^3 - u = x^3 - m$ in $(A/(u-m))[x] \cong \mathbf{Q}[x]$, so $(u-m)B$ is prime in B and $B/(u-m)B = \mathbf{Q}[\sqrt[3]{u}]/(u-m) \cong \mathbf{Q}(\sqrt[3]{m})$. The residue field extension $(B/(u-m)B)/(A/(u-m))$ is $\mathbf{Q}(\sqrt[3]{m})/\mathbf{Q}$, which is separable but not Galois.

Example 2. Let F be an imperfect field of characteristic p, $K = F(u)$, and $A = F[u]$. We'll describe a Galois extension of K in which the integral closure of A has a prime ideal whose residue field is inseparable over the residue field of the prime below it in A.

Since F is not perfect, there is an $a \in F - F^p$. The polynomial $f(x) = x^p - u^{p-1}x - a$ is irreducible over K since its reduction mod u is $x^p - a$ in $(A/(u))[x] \cong F[x]$, which is irreducible due to it having no root in F. Note $f(x)$ is separable in $K[x]$ since $f'(x) = -u^{p-1}$ is a nonzero element of K.

Let $L = K(\alpha)$ where $f(\alpha) = 0$, so $[L : K] = p$. Then L/K is Galois since $f(x)$ is separable with roots $\{\alpha + cx : c \in \mathbf{F}_p\}$, which are all in L. Let B be the integral closure of A in L. We'll show (u) is totally ramified in B and the residue field at the unique prime in B lying over (u) is inseparable over the residue field $A/(u)$.

Let $k := A/(u) \cong F$, which is the residue field in A at (u), and let ℓ be the residue field at some prime in B lying over (u). Since $f(x) = x^p - a$ in $(A/(u))[x] = k[x] \cong F[x]$, the equation $f(\overline{\alpha}) = \overline{0}$ in ℓ shows $[\ell : k] \geq p$. Since $[\ell : k] \leq [L : K] = p$, we get $[\ell : k] = p$, so $\ell = k(\overline{\alpha})$, which is purely inseparable over k. Since residue field extensions at primes in A and B are possibly inseparable, the standard equality $[L : K] = \sum_{i=1}^{g} e_i f_i$ for an extension of number fields K and L is replaced by an inequality

$$[L : K] \geq \sum_{i=1}^{g} e_i f_i \tag{1}$$

for K and L in this example.[1] Applying the inequality (1) to the primes in B lying over (u), the left side of (1) is p and some f_i on the right side is p, so $g = 1$, $f_1 = p$, and $e_1 = 1$: there is one prime over (u) in B and its residue field degree over (u) is p while its ramification index over (u) is 1. Thus (u) is totally ramified in B.

We'll now show that for a finite Galois extension of fraction fields of Dedekind domains, most of the associated residue field extensions are Galois.

Lemma 3. *Let R be a Dedekind domain with fraction field M and $f(x)$ in $R[x]$ be monic and separable with $\operatorname{disc}(f(x)) \in R^\times$. In $M(\gamma)$, where $f(\gamma) = 0$, R has integral closure $R[\gamma]$.*

Proof. Let γ have minimal polynomial $\pi(x)$ over M. Then $\pi(x) \mid f(x)$ in $M[x]$. Since $\pi(x)$ is monic, $\pi(x) \in R[x]$ and $f(x) = \pi(x)g(x)$ for some $g(x) \in R[x]$. Then in R,

$$\operatorname{disc}(f(x)) = \operatorname{disc}(\pi(x)g(x)) = \operatorname{disc}(\pi(x))\operatorname{disc}(g(x))\operatorname{Res}(\pi(x), g(x))^2,$$

where $\operatorname{Res}(\pi(x), g(x))$ is a resultant. Since $\operatorname{disc}(f(x)) \in R^\times$, also $\operatorname{disc}(\pi(x)) \in R^\times$.

Let $\delta = \operatorname{disc}(\pi(x))$ and let S be the integral closure of R in $M(\gamma)$. Then

$$R[\gamma] \subset S \subset \frac{1}{\delta}R[\gamma].$$

Since $\delta \in R^\times$, $S = R[\gamma]$. □

Theorem 4. *Let A be a Dedekind domain, K be its fraction field, and L/K be a finite Galois extension that is the splitting field of the monic separable polynomial $f(x) \in A[x]$ with discriminant d.*

Let B be the integral closure of A in L, and write $f(x) = \prod_{i=1}^n (x - \alpha_i)$ in $B[x]$. For each nonzero prime ideal $\mathfrak{p}$ in A such that $\mathfrak{p} \nmid (d)$ and each prime ideal $\mathfrak{P}$ lying over $\mathfrak{p}$ in B, $B/\mathfrak{P} = (A/\mathfrak{p})(\overline{\alpha_1}, \ldots, \overline{\alpha_n})$ and $(B/\mathfrak{P})/(A/\mathfrak{p})$ is Galois.

Proof. The theorem is obvious if $n = 1$, so let $n \geq 2$.

The condition $\mathfrak{p} \nmid (d)$ implies $f(x) \bmod p$ is separable: in $A/\mathfrak{p}$,

$$\operatorname{disc}(\overline{f}(x)) = \overline{\operatorname{disc}(f(x))} = d \bmod \mathfrak{p} \neq \overline{0}.$$

Since $f(x) = \prod_{i=1}^n (x - \alpha_i)$ in $B[x]$, $\overline{f}(x) = \prod_{i=1}^n (x - \overline{\alpha_i})$ in $(B/\mathfrak{P})[x]$, so the reductions $\overline{\alpha_i}$ are distinct in $B/\mathfrak{P}$. If we show

$$B/\mathfrak{P} = (A/\mathfrak{p})(\overline{\alpha_1}, \ldots, \overline{\alpha_n}), \tag{2}$$

then $(B/\mathfrak{P})/(A/\mathfrak{p})$ is separable and normal, and thus it is Galois.

The residue fields $A/\mathfrak{p}$ and $B/\mathfrak{P}$ are unaffected by *localizing* at $\mathfrak{p}$: $B_\mathfrak{p}$ is the integral closure of $A_\mathfrak{p}$ in $M(\gamma)$ and the natural maps $A/\mathfrak{p} \to A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ and $B/\mathfrak{P} \to B_\mathfrak{p}/\mathfrak{P}B_\mathfrak{p}$ are field isomorphisms. So to show $B/\mathfrak{P} = (A/\mathfrak{p})(\overline{\alpha_1}, \ldots, \overline{\alpha_n})$ we can replace A with $A_\mathfrak{p}$ and B with $B_\mathfrak{p}$. Then A is a DVR with maximal ideal $\mathfrak{p}$ and $d = \operatorname{disc}(f(x))$ is a unit in A since $d \not\equiv 0 \bmod \mathfrak{p}$.

Apply Lemma 3 to $R = A$, $M = K$, $f(x)$ as in the theorem, and $\gamma = \alpha_1$. Since $d \in A^\times$, the integral closure of A in $K(\alpha_1)$ is $A[\alpha_1]$.

For $1 \leq i \leq n-1$, assume by induction on i that the integral closure of A in $K(\alpha_1, \ldots, \alpha_i)$ is $A[\alpha_1, \ldots, \alpha_i]$. Apply Lemma 3 to $R = A[\alpha_1, \ldots, \alpha_i]$, $M = K(\alpha_1, \ldots, \alpha_i)$, $f(x)$ as in the

[1] The inequality (1) can be turned into an equality by including an additional factor d_i in each term of the sum called the defect of the ith prime. The defect d_i is 1 when the ith residue field extension is separable. See https://www.mathi.uni-heidelberg.de/∼roquette/hist_val.pdf.

theorem, and $\gamma = \alpha_{i+1}$ to see that the integral closure of R in $M(\alpha_{i+1})$ is $R[\alpha_{i+1}] = A[\alpha_1, \dots, \alpha_{i+1}]$. Therefore the integral closure of A in $K(\alpha_1, \dots, \alpha_{i+1})$ is $A[\alpha_1, \dots, \alpha_{i+1}]$.

Taking $i = n$, we have $B = A[\alpha_1, \dots, \alpha_n]$, which implies (2), so we're done. □

Example 5. We return to the Galois extension L/K in Example 2, where the residue field extension at the prime over (u) is inseparable. We'll show all other residue field extensions are Galois.

A formula for the discriminant of a trinomial $x^n + bx + c$ over a general field is

$$\operatorname{disc}(x^n + bx + c) = (-1)^{n(n-1)/2}((-1)^{n-1}(n-1)^{n-1}b^n + n^n c^{n-1}).$$

Therefore over a field of characteristic p,

$$\operatorname{disc}(x^p + bx + c) = (-1)^{p(p-1)/2}((-1)^{p-1}(p-1)^{p-1}b^p) = \pm b^p.$$

So in $K[x]$ from Example 2,

$$\operatorname{disc}(x^p - u^{p-1}x - a) = \pm u^{p(p-1)} \in F[u] = A.$$

The only (monic) prime factor of this discriminant is u, so Theorem 4 tells us that in Example 2, for each nonzero prime ideal $\mathfrak{p}$ in A other than (u), the residue field at each prime ideal in B lying over $\mathfrak{p}$ is Galois over $A/\mathfrak{p}$.