GALOIS THEORY NOTES

1. Splitting fields and Normal extensions

Proposition 1.1. Let $K \leq L$ be fields. Suppose that $\alpha \in L$ is algebraic over K and let $p(x) \in K[x]$ be a minimal polynomial for α. Then there is a unique isomorphism $K[x]/(p(x)) \to K[\alpha] = K(\alpha)$ mapping x to α and fixing K.

Proof. There is a unique map $K[x] \to K[\alpha]$ mapping x to α and fixing K. It is surjective and its kernel is the ideal generated by $p(x)$. □

If $\sigma : K \to L$ is a homomorphism of fields and $f = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, then we let $f^\sigma = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n \in F[x]$.

Lemma 1.2. Suppose that $\sigma : K \to L$ is an isomorphism of fields and suppose $K' = K[\alpha]$ is an extension of K where $f \in F[x]$ the minimal polynomial of $\alpha \in K'$. Let $\sigma : K \to L$ be a field homomorphism.

- If $\sigma' : K' \to L$ extends σ, then $f^\sigma(\sigma(\alpha')) = 0$
- If $\beta \in L$ satisfies that $f^\sigma(\beta) = 0$, then there is precisely one extension of σ mapping α to β.

Proof. The first point is obvious. For the second point, let $\phi : K[x] \to L$ be given by $\phi(P) = P^\sigma(\beta)$. This is a ring homomorphism. Now observe that $\phi(f) = f^\sigma(\beta) = 0$, thus ϕ vanishes on the ideal generated by f and so there is a well defined field homomorpism $\phi : K[x]/(f) \to L$ mapping $x + (f)$ to β. Finally, we use the isomorphism $K' \cong K[x]/(f)$ that maps α to x and fixes K, giving the desired extension. The extension is clearly unique as $K' = K(\alpha)$.

□

Proposition 1.3. Let $K \leq K'$ be an algebraic field extension and suppose that $\sigma : K \to L$ is a field homomorphism where L is algebraically closed. Then there exists an extension $\sigma' : K' \to L$. Moreover, σ' must be an isomorphism if K' is algebraically closed and L is algebraic over $\sigma(K)$.

Proof. Use Zorn's lemma to construct a maximal subfield $K'' \subset K$ such that σ extends to K''. If $K'' \neq K'$ then choose $\alpha \in K' \setminus K''$. Now as K' ia algebraic over K we can let $f \in K[x]$ be a minimal polynomial of α over K. Now as f^σ has a root in L as L is algebraically closed, we can use the previous lemma to extend σ to $K''[\alpha]$, contradicting the maximality of K''. If K' is algebriacally closed, then so is $\sigma'(K')$ since any element of $\sigma'(K')[x]$ is of the form $f^{\sigma'}$ for some $f \in K'[x]$ and so we can let α be a root of f, giving that $\sigma'(\alpha)$ is a root of $f^{\sigma'}$. Now $\sigma'(K') \geq \sigma(K)$ so if L is algebraical over $\sigma(K)$, then L is also algebraic over $\sigma'(K')$. So if L is algebraically closed then $L = \sigma'(K')$, giving that σ' is surjective and thus an isomorphism (all field isomorphisms are injective). □

Corollary 1.4. The algebraic closure of a field K is unique upto an isomorphism fixing K.

Definition 1.5 (Splitting field)**.** Let $K \leq L$ be fields and let $\mathcal{F} \subset K[x]$ be a family of polynomials. We say that L is a splitting field for $\mathcal{F}$ over F if each $f \in \mathcal{F}$ splits into linear factors in $L[x]$ and L is the field generated by K and the roots of all polynomials in $\mathcal{F}$.

Proposition 1.6. A splitting field is unique upto an isomorphism fixing F.

Proof. Let $L \geq K$ and $L' \geq K$ be two splitting fields for a family $\mathcal{F} \subset K[x]$. We note that L' and L are both algebraic over K (as they are generated by roots). This means that we may use Proposition 1.3 to extend the identity map $K \to K$ to a field homomorphism $\sigma : L \to \widehat{L'}$ where $\widehat{L'} \geq L'$ is algebraically closed. However, note that $\sigma(L) \subset L'$ since σ maps each root of some $f \in \mathcal{F}$ to a root of f (as σ fixes K). So $\sigma : L \to L'$ is a homomorphism. It remains to show that σ is surjective. To see this, let $f \in \mathcal{F}$ and write $f(x) = \prod_i (x - \alpha_i)$ where $\alpha_i \in L$. Then $f = f^\sigma = \prod_i (x - \sigma(\alpha_i))$. This shows that any root in L' of any $f \in \mathcal{F}$ is in the image of σ (using the unique factorization property). Thus as L' is generated by these roots, the surjectivity of σ follows. $\square$

If K_1 and K_2 are two fields with a common subfield K, we say that a homomorphism $K_1 \to K_2$ is a K-homomorphism if it restricts to the identity on K.

Theorem 1.7. Let L be an algebraic extension of a field K. Then the following are equivalent.

(1) L is a splitting field for some family of polynomials in $K[x]$.
(2) Any K-homomorphism $L \to \overline{L}$, where $\overline{L} \geq L$ is an algebriac closure, restricts to an automorphism of L
(3) Any irreducible polynomial in $K[x]$ that has a root in L must decompose into linear factors in $L[x]$.

Proof. (i) $\implies$ (ii): If L is a splitting field for some polynomials in $K[x]$ and $\sigma : L \to \overline{L}$ is a K-homomorphism, then as in the proof of the uniqueness of splitting fields above, we see that σ maps into L. We also saw that it permutes the roots of a polynomial in $K[x]$ in L and thus the image of σ is L, thus σ is surjective and hence an automorphism.

(ii) $\implies$ (iii): Suppose $f \in K[x]$ is irreducible and has a root $\alpha \in L$. Now if $\alpha' \in \overline{L}$ is another root of f, then since f is irreducible we have an isomorphism $K[\alpha] \to K[\alpha']$ mapping α to α', which we may extend to an K-homomorphism $\sigma : L \mapsto \overline{L}$ by a previous Lemma. By condition (ii), we see that σ maps L to L and thus $\alpha' = \sigma(\alpha) \in L$. Hence L contains all the roots of f.

(iii) $\implies$ (ii): As L is algebraic, every element $\alpha \in L$ is the root of some irreducible polynomial $f \in K[x]$. We thus let $\mathcal{F} \subset K[x]$ be those irreducible polynomials with at least one root in L, which split into linear factors by assumption. Thus L is the splitting field of $\mathcal{F}$ over K.

$\square$

Definition 1.8. We say that an extension $K \leq L$ is normal if it is the splitting field of some family of polynomials.

Example 1.9. The extension $\mathbb{Q} \leq \mathbb{Q}[2^{1/3}]$ is not normal. To see this we use the characterization (iii) in the Theorem as follows: The polynomial $x^3 - 2$ is irreducible, has one root $2^{1/3}$ in our extension but not any other. Alternatively, we can use (ii) by noting that although there is $\mathbb{Q}$-homomorphism $\mathbb{Q}[2^{1/3}] \to \overline{\mathbb{Q}}$ mapping $2^{1/3}$ to $2^{1/3}e^{2\pi i/3}$, it does not restrict to an automorphism of $\mathbb{Q}[2^{1/3}]$.

Example 1.10. Normal is not transitive. As an example, consider the field extensions $\mathbb{Q} \leq \mathbb{Q}[\sqrt{2}] \leq \mathbb{Q}[2^{1/4}]$. The intermediate field extensions are normal (as they are of degree 2) but the extension $\mathbb{Q} \leq \mathbb{Q}[2^{1/4}]$ is not.

Definition 1.11. If $L \geq K$ is an algebraic extension, then we say that $L' \leq L \leq K$ is a normal closure of $L \geq K$ if $L' \geq K$ is a normal extension and any $L' \geq L'' \geq K$ such that $L'' \geq K$ is normal must satisfy $L'' = L'$. That is, the normal closure if a minimal normal extension.

Proposition 1.12. Every algebraic extension $L \geq K$ has a normal closure. More precisely, let $\mathcal{F}$ be the set of all irreducible polynomials in $K[x]$ such that each element of $L \setminus K$ is the root of some $f \in \mathcal{F}$. Then the splitting field of $\mathcal{F}$ is the normal closure of $L \geq K$.

Proof. Let $\overline{L} \geq L$ be the algebraic closure of L. Define $\overline{L} \geq L' \geq L$ to be the splitting field for the family $\mathcal{F} \subset K[x]$ of minimal polynomials for elements of L. We claim that L' is the normal closure. Thus suppose that $L \leq L'' \leq L'$ is such that $K \leq L''$ is normal. We must show that $L'' = L'$, and since L' is generated by the roots of elements of $\mathcal{F}$, we must show that any root $\alpha \in L'$ of a polynomial $f \in \mathcal{F}$ is in L''. To see this, note that by definition f is a minimal polynomial of some $\alpha' \in L$. There is a K-homomorphism $\sigma : K[\alpha'] \to \overline{L}$ mapping α' to $\alpha \in L$. As $L'' \geq L \geq K[\alpha']$, we may extend this K-homomorphism to $\sigma : L'' \to \overline{L}$. But by characterization (ii) of the normality of $K \leq L''$, we see that σ is an automorphism of L''. This means that $\alpha = \sigma(\alpha') \in L''$ as $\alpha' \in L \subset L''$. Thus this shows that $L' \subset L''$, and so $L' = L''$ as required. □

Proposition 1.13. If $K \leq L$ is an algebraic extension and $L \leq L_1, L_2 \leq \overline{L}$ are two normal extensions of K, then $L_1 \cap L_2$ is a normal extension of K. In particular, if L_1 and L_2 are both normal closures of $L \geq K$, then $L_1 = L_2$.

Proof. This follows from characterization (iii): If $f \in K[x]$ is irreducible and has a root in $\alpha \in L_1 \cap L_2$, then f decomposes to linear factors in $L_i[x]$ for $i = 1, 2$. By uniqueness of factorizations, this means that these linear factors are in $(L_1 \cap L_2)[x]$. □

Proposition 1.14. A normal closure of an algebraic extension $L \geq K$ is unique upto an L-automorphism.

Proof. By the previous construction, we have one such normal closure given by $L[\mathcal{R}]$ where

$$\mathcal{R} = \{r \in \overline{L} \mid f(r) = 0 \text{ for some } f \in \mathcal{F}\}$$

where $\mathcal{F} \subset K[x]$ is the set of all irreducible polynomials such that each element of L is the root of some $f \in \mathcal{F}$. We now let $L' \geq L$ be another field such that $L' \geq K$ is the normal closure of $L \geq K$. We now construct an isomorphism $L[\mathcal{R}] \to L'$ which fixes L. We extend the inclusion $L \to \overline{L'}$ to an L-homomorphism $\sigma : L[\mathcal{R}] \to \overline{L'}$. Note that $L'' = \sigma(L[\mathcal{R}]) = L[\sigma(\mathcal{R})]$ contains L and is the splitting field of $\mathcal{F}$ in $\overline{L'}$ over K. Thus L' and L'' are subfields of $\overline{L}$ that are normal extensions of K and both contain L. Moreover, L'' is also a normal closure of $L \geq K$ as it follows the construction given in Proposition 1.12 (i.e., it is a splitting field of minimal polynomials over $K[x]$ of elements in L). By the previous proposition, it follows that $L' = L''$, thus σ is an isomorphism. □

2. Seperable extensions

Lemma 2.1. An irreducible polynomial $f \in K[x]$ splits into distinct linear factors in some algebraic closure if and only if $f' = 0$.

Proof. By the product rule it follows that if $f(\alpha) = 0$ then α is a repeated root if and only if $f'(\alpha) = 0$. If f is irreducible, has a repeated root α and $f' \neq 0$ then $(X - \alpha) | gcd(f, f') | f$, which contradicts the irreducibility of f. $\square$

As a consequence, if $charK = 0$ then an irreducible polynomial must split into distinct linear factors.

Definition 2.2. We say that $f \in K[x]$ is seperable if f splits into distinct linear factors in some (hence any) algebraic closure of K.

Theorem 2.3. If $charK = p$ and $f \in K[x]$ is irreducible, then each root of f has multiplicity p^r where r is minimal non-negative integer such that $f(x) = g(x^{p^r})$ for some $g \in K[x]$.

Proof. Write $g(x) = \sum_j c_j x^j$. Since

$$g'(x) = \sum_j j c_j x^j$$

we observe that $g'(x)$ is not the zero polynomial as follows: If $g'(x) = 0$ then $c_j = 0$ whenever j is not divisible by p. From this it follows that $g(x) = \sum_k c_{kp} x^{kp} = h(x^p)$. It now follows that

$$f(x) = g(x^{p^r}) = h((x^{p^r})^p) = h(x^{p^{r+1}}),$$

which contradicts the maximality of r. Thus $g'(x) \neq 0$. This means that $g(x) = \prod_i (x - \alpha_i)$ where α_i are distinct. Write $\alpha_i = \beta_i^{p^r}$, which exists in an algebraic closure. Note that the β_i must also be distinct. Thus

$$f(x) = \prod_i (x^{p^r} - \beta_i^{p^r}) = \prod_i (x - \beta_i)^{p^r},$$

where the last equality follows from Freshman's dream in characteristic p. As the β_i are distinct, the proof is complete. $\square$

Definition 2.4. If $K \leq L$ is an algebraic field extension then $\alpha \in L$ is called seperable over K if the minimal polynomial is seperable (splits over linear factors in some, hence any, algebraic closure). We say that $K \leq L$ is seperable if all elemnts of L are separable over K.

Thus from above, in characteristic zero all algebraic extensions are seperable, as all irreducible polynomials are seperable.

Definition 2.5. If $K \leq L$ is an algebraic extension, then we let

$$Hom_K(L, \overline{K})$$

denote the set of all K-homomorphisms $L \to \overline{K}$. We let

$$|L : K|_s = |Hom_K(L, \overline{K})|$$

be the seperable degree of $K \leq L$, which does not depend on the choice of $\overline{K}$.

Proposition 2.6. If $K \leq L \leq M$ are algebraic extensions then there is a bijection

$$Hom_K(L, \overline{K}) \times Hom_L(M, \overline{K}) \to Hom_K(M, \overline{K}).$$

In particular

$$|M : K|_s = |L : K|_s |M : L|_s.$$

Proof. For each $\sigma \in Hom_K(L, \overline{K})$ we choose an arbitrary (there are many choices) $\phi(\sigma) : \overline{K} \to \overline{K}$ automorphism that extends σ, where we have used Proposition???. Now we define a mapping

$$Hom_K(L, \overline{K}) \times Hom_L(M, \overline{K}) \to Hom_K(M, \overline{K})$$

by

$$(\sigma, \tau) \mapsto \phi(\sigma) \circ \tau.$$

Let us first check that it is well defined. If $k \in K$ then

$$(\phi(\sigma) \circ \tau)(k) = \phi(\sigma)(\tau(k)) = \phi(\sigma)(k) = \sigma(k) = k,$$

so indeed $\phi(\sigma) \circ \tau$ is a K-homomorphism. To show injectivity, suppose that

$$\phi(\sigma) \circ \tau = \phi(\sigma') \circ \tau'.$$

Then for any $\ell \in L$ we have that

$$\phi(\sigma)(\tau(\ell)) = \phi(\sigma)(\ell) = \sigma(\ell)$$

and by the same arugment $\phi(\sigma')(\tau'(\ell)) = \sigma'(\ell)$. Thus $\sigma = \sigma'$. This means that $\phi(\sigma) = \phi(\sigma')$ and so by injectivity of field automorphisms, we must have that $\tau'(m) = \tau(m)$ for all $m \in M$. So $\tau = \tau'$. It now remains to show injectivity. Thus suppose that $\gamma \in Hom_K(M, \overline{K})$. Let σ be the restriction of γ to L and observe that $\sigma \in Hom_K(L, \overline{K})$. Now let

$$\tau = \phi(\sigma)^{-1} \circ \gamma : M \to \overline{K}.$$

If $\ell \in L$ then

$$\tau(\ell) = \phi(\sigma)^{-1}(\gamma(\ell)) = \phi(\sigma)^{-1}(\sigma(\ell)) = \phi(\sigma)^{-1}\phi(\sigma)(\ell) = \ell,$$

thus indeed $\tau \in Hom_L(M, \overline{K})$. This shows that $\gamma = \phi(\sigma) \circ \tau$ is in the image of our map, thus our map is surjective. □

Proposition 2.7. If $K \leq L$ is a finite extension then

(1) If K has characteristic zero then $|L : K| = |L : K|_s$
(2) If K has characteristic p then $|L : K| = p^r |L : K|_s$ for some integer $r \geq 0$.

Proof. By finiteness of this extension L can be obtained from K by finitely many simple extensions, so we only need to prove this when $L = K(\alpha)$ is a simple extension and then use the previous proposition to give the general case by induction. If $Char K = 0$ then we know that $|L : K| = deg f = |L : K|_s$ where $f \in K[x]$ is the minimal polynomial of α, where we have used the fact that f is seperable and there is a unique K-homomorphism mapping α to any given root of f. If $Char K = p$ then $|L : K| = deg f = p^r |L : K|_s$ where r is maximal integer such that $f(x) = g(x^{p^r})$ for some polynomial $g(x) \in K[x]$, as seen in a previously proven result. Thus completing the proof. □

Theorem 2.8. Let $K \geq L$ be a finite extension. The following are equivalent.

(1) $K \geq L$ is seperable.
(2) $L = K(a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n \in L$ that are separable over K
(3) $|L : K|_s = |L : K|$

Proof. (i) $\implies$ (ii) is trivial. (ii) $\implies$ (iii): Letting $K_i = K_{i-1}(a_i)$ we see that a_i is separable over $K_{i-1} \geq K$and thus $|K_i : K_{i-1}| = deg(f_i) = |K_i : K_{i-1}|_s$ where f_i is the minimal polynomial of a_i over K_{i-1}. We are now done by the multiplicativity formula. (iii) $\implies$ (i): We only need to focus on $Char K = p > 0$. If $a \in L$ is not seperable over K then

$$|K(a) : K|_s < |K(a) : K|$$

, but then

$$|L : K|_s = |L : K(a)|_s |K(a) : L|_s < |L : K(a)||K(a) : K| = |L : K|.$$

□

Corollary 2.9. If $K \leq L \leq M$ are algebraic extensions then $K \leq M$ is seperable if and only if $K \leq L$ and $L \leq M$ are seperable.

Proof. First suppose $K \leq M$ is seperable. Then clearly $K \leq L$ is seperable. Now for $a \in M$ we have that the minimal polynomial $f(x) \in K[x]$ of a over K splits into linear factors. If $g(x) \in L[x]$ is the minimal polynomial of a over L, then clearly $g(x)|f(x)$ as $f(x) \in L[x]$. Thus $g(x)$ also splits into linear factors.

Conversely, assume now that $K \leq L$ and $L \leq M$ are seperable. Fix $a \in M$. Then $|L(a) : L| = |L(a) : L|_s$ as $L \leq M$ is seperable. Now let $L' \leq L$ be the field generated by K and the coefficients of the minimal polynomial $f(x) \in L[x]$ of a over L. Thus $f(x) \in L'[x]$ which means that a is seperable over L' as well (as $f(x)$ splits into linear factors and $f(a) = 0$). Thus $|L'(a) : L'|_s = |L(a) : L|$. It now follows that

$$|L'(a) : K|_s = |L'(a) : L'|_s |L' : K|_s = |L'(a) : L||L' : K| = |L'(a) : K|,$$

hence be the previous theorem we have that $L'(a)$ is seperable over K, and thus a is seperable over K. □

Theorem 2.10 (Primitive element theorem)**.** If $K \leq L$ is a finite seperable extension, then $L = K(a)$ for some $a \in L$.

Proof. If L is finite, then this follows from the fact that the multiplicative group of a field is cyclic. Suppose thus that K and L are infinite. We may reduce to the case where $L = K(\alpha, \beta)$, as the general case then follows by induction (If $L = K(a_1, \ldots, a_n)$ then $L = K'(a_1, a_2)$ where $K' = K(a_3, \ldots, a_n)$ and certainly L is seperable over K'). For $c \in K$, we let $\gamma_c = \alpha + c\beta$. We will show that $L = K(\gamma_c)$ for infinitely many $c \in K$ as follows. If $L \neq K(\gamma_c)$ then definitely $\beta \notin K(\gamma_c)$. As L is seperable over $K(\gamma_c)$, this means that the minimal polynomial of β over $K(\gamma_c)$ has another root $\beta' \in \overline{K}$. Thus there exists a $K(\gamma_c)$-homomorphism $\sigma : L \to \overline{K}$ with $\sigma(\beta) = \beta' \neq \beta$. We thus get that

$$\sigma(\alpha) + c\sigma(\beta) = \alpha + c\beta$$

and thus

$$c = \frac{\sigma(\alpha) - \alpha}{\beta - \sigma(\beta)}.$$

But the right hand side has only finitely many choices (as there are only finitely many choices of σ) and so if we choose a c not of this form (as K is infinite) we see that $L = K(\gamma_c)$ as desired. □