21-238, Math Studies Algebra 2, Department of Mathematical Sciences, Carnegie Mellon University
Spring 2012: Monday, Wednesday, Friday, 10:30 am, Doherty Hall 1211.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

34- Monday April 16, 2012.

Lemma 34.1: (fundamental theorem of Galois theory) Let F be a finite Galois extension of E. Then
a) The mapping $K \mapsto Aut_K(F)$ for intermediate fields (i.e. $E \subset K \subset F$), and the mapping $H \mapsto Fix(H)$ for subgroups of $Aut_E(F)$ are inverse bijections.
b) For any intermediate field K, F is a Galois extension of K.
c) For an intermediate field K, K is a Galois extension of E if and only if K is a normal extension of E, or if and only if $Aut_K(F) \lhd Aut_E(F)$. In that case the mapping $\sigma \mapsto \sigma\big|_K$ maps $Aut_E(F)$ into $Aut_E(K)$, it is surjective with kernel $Aut_K(F)$, and it induces an isomorphism from $Aut_E(K)$ onto the quotient group $Aut_E(F)/Aut_K(F)$.
Proof: If H is a subgroup of $Aut_E(F)$, then H is finite since $|Aut_E(F)| = [F:E] < \infty$, so that if $K = Fix(H)$ one has $H = Aut_K(F)$ by Lemma 32.6. By Lemma 33.8, F is a splitting field extension for a separable $f \in E[x]$ over E. If K is an intermediate field, then F is a splitting field extension for f over K,[1] f is separable over K by Lemma 33.6, so that F is a Galois extension of K by Lemma 33.8, and this proves b); it means $K = Fix\big(Aut_K(F)\big)$, which ends the proof of a).

Since F is a separable extension of E, K is also a separable extension of E, and then K is a Galois extension of E if and only if it is a normal extension of E by Lemma 33.8. Each $\sigma \in Aut_E(F)$ permutes the roots of any polynomial $Q \in E[x]$, in particular if $a \in K$ has minimal (monic irreducible) polynomial $P_a \in E[x]$, $\sigma(a)$ is another root of P_a belonging to F; the restriction $\sigma\big|_K$ of σ to K is an homomorphism of K into F, and if all the roots of P_a belong to K, one has $\sigma\big|_K(a) \in K$.

Assuming that K is a Galois extension of E, K is a normal extension of E, i.e. all P_a split over K for $a \in K$, so that $\sigma\big|_K$ maps K into K, and it is an automorphism of K since it is a bijection in F, and $\sigma\big|_K \in Aut_E(K)$ because it fixes E. Moreover, the mapping which to $\sigma \in Aut_E(F)$ associates $\sigma\,|_K \in Aut_E(K)$ is an homomorphism, and its kernel corresponds to $\sigma\,|_K = id_K$, i.e. σ fixes K, or $\sigma \in Aut_K(F)$, which is then a normal subgroup of $Aut_E(F)$ as the kernel of an homomorphism. Also, the image of this homomorphism is contained in $Aut_E(K)$ whose order is $\leq [K:E]$, and the image has order $\frac{|Aut_E(F)|}{|Aut_K(F)|} = \frac{[F:E]}{[F:K]} = [K:E]$, so that the homomorphism is surjective, and the first isomorphism theorem gives $Aut_E(K)$ isomorphic to $Aut_E(F)/Aut_K(F)$.

Finally, assuming that $Aut_K(F)$ is a normal subgroup of $Aut_E(F)$, one wants to show that K is a normal extension of E. Let $a \in K$ and let $P_a \in E[x]$ be its monic irreducible polynomial, which splits in F as $\prod_i (x - a_i)$, where the a_i run through the orbit of a by action of $Aut_E(F)$ (by the proof of Lemma 33.8), and one wants to show that each a_i belongs to K: one starts by choosing $\sigma \in Aut_E(F)$ such that $\sigma(a) = a_i$, and then for $\tau \in Aut_K(F)$ one has $\sigma^{-1}\tau\,\sigma \in Aut_K(F)$ since $Aut_K(F)$ is a normal subgroup of $Aut_E(F)$, so that $\sigma^{-1}\tau\,\sigma(a) = a$ because $a \in K$, i.e. $\tau(a_i) = a_i$; since this holds for all $\tau \in Aut_K(F)$, it means that $a_i \in Fix\big(Aut_K(F)\big)$, which is K, because F is a Galois extension of K by b), and it proves c).

Lemma 34.2: Let $f \in E[x]$ be separable over E, and let F be a splitting field extension for f over E. Every $\sigma \in Aut_E(F)$ determines a permutation π of the roots of f, and the knowledge of π characterizes σ.

Moreover, if f is irreducible and $a, b \in F$ are two roots of f, there exists $\sigma \in Aut_E(F)$ with $\sigma(a) = b$, i.e. $Aut_E(F)$ acts *transitively* on the roots of f.[2]
Proof: For any polynomial $P \in E[x]$, any root $r \in F$ of P, and any $\sigma \in Aut_E(F)$, $\sigma(r)$ is a root of P (in F), and since $\sigma^{-1} \in Aut_E(F)$ one deduces that σ induces a permutation π of the roots of P. Since F is a splitting field extension for f over E, and $r_1, \ldots, r_n \in F$ are the roots of f, then $F = E(r_1, \ldots, r_n) = E[r_1, \ldots, r_n]$,[3] so that every $c \in F$ can be written $c = Q(r_1, \ldots, r_n)$ for a polynomial $Q \in E[x_1, \ldots, x_n]$, and then $\sigma(c) = Q\big(\sigma(r_1), \ldots, \sigma(r_n)\big) = Q\big(\pi(r_1), \ldots, \pi(r_n)\big)$ is determined by π.[4]

---

[1] f splits over F and F is generated by E and the roots of f, hence generated by K and the roots.
[2] A group G acts *transitively* on a set X if for every $x_1, x_2 \in X$ there exists $g \in G$ with $g\,x_1 = x_2$.
[3] Since $K(r) = K[r]$ if r is algebraic over K, one deduces by induction that $E(r_1, \ldots, r_n) = K(r_n)$ with $K = E(r_1, \ldots, r_{n-1}) = E[r_1, \ldots, r_{n-1}]$ and then $K(r_n) = K[r_n] = E[r_1, \ldots, r_n]$.
[4] Not every permutation on the roots defines an element $\sigma \in Aut_E(F)$, of course.

The case $b=a$ is obvious (with $\sigma=id$), and one assumes $b\neq a$, so that $deg(f)\geq 2$, and neither a nor b belong to E. Because f is irreducible, $E(a)$ is isomorphic to $E(b)$, and there exists a unique isomorphism σ_0 from $E(a)$ onto $E(b)$ extending id_E and such that $\sigma_0(a)=b$.[5] Then, F is a splitting field extension for f over $E(a)$, and also over $E(b)$, and by the uniqueness of the splitting field extension up to isomorphism, one can extend σ_0 (not in a unique way) into an isomorphism σ of F, which then belongs to $Aut_E(F)$.

Lemma 34.3: The splitting field extension for x^4-2 over $\mathbb{Q}$ is $\mathbb{Q}(\alpha,i)$ with $\alpha=\sqrt[4]{2}$; it is a Galois extension of $\mathbb{Q}$ with $\big|Aut_{\mathbb{Q}}\big(\mathbb{Q}(\alpha,i)\big)\big|=[\mathbb{Q}(\alpha,i):\mathbb{Q}]=8$.
Proof: The polynomial $f=x^4-2$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein criterion, and its roots in $\mathbb{C}$ are $\alpha,\alpha\,i,-\alpha,-\alpha\,i$, so that $\mathbb{Q}(\alpha,\alpha\,i,-\alpha,-\alpha\,i)=\mathbb{Q}(\alpha,\alpha\,i)$ is the desired splitting field extension, but since $\frac{1}{\alpha}\in\mathbb{Q}[\alpha]$, it is $\mathbb{Q}(\alpha,i)$. Since $\mathbb{Q}(\alpha)\subset\mathbb{R}$, x^2+1 is irreducible in $\mathbb{Q}(\alpha)$ (because $\pm i\notin\mathbb{Q}(\alpha)$), so that $Q(\alpha,i)=\big(\mathbb{Q}(\alpha)\big)(i)$, and $[\mathbb{Q}(\alpha,i):\mathbb{Q}(\alpha)]=2$, which with $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$ gives $[\mathbb{Q}(\alpha,i):\mathbb{Q}]=8$. Since f is irreducible in $\mathbb{Q}[x]$ and $f'\neq 0$, f is separable by Lemma 33.4, so that $\mathbb{Q}(\alpha,i)$ is a Galois extension of $\mathbb{Q}$ by Lemma 33.8, which gives $\big|Aut_{\mathbb{Q}}\big(\mathbb{Q}(\alpha,i)\big)\big|=[\mathbb{Q}(\alpha,i):\mathbb{Q}]=8$.

Remark 34.4: Up to isomorphism, the Abelian groups of order 8 are $\mathbb{Z}_8$, $\mathbb{Z}_2\times\mathbb{Z}_4$, and $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$, and the non-Abelian groups of order 8 are the dihedral group D_4, and the quaternion group Q_8.

Lemma 34.5: For $\alpha=\sqrt[4]{2}$, $Aut_{\mathbb{Q}}\big(\mathbb{Q}(\alpha,i)\big)$ is isomorphic to the dihedral group D_4.
Proof: For $\sigma'\in Aut_{\mathbb{Q}}\big(\mathbb{Q}(\alpha,i)\big)$, $\sigma'(\alpha)$ must be one of the 4 roots of $x^4-2=0$, i.e. $\alpha,\alpha\,i,-\alpha,-\alpha\,i$, which one denotes 1, 2, 3, 4, and $\sigma'(i)$ should be one of the 2 roots of $x^2+1=0$, i.e. $i,-i$, and this gives 8 possibilities, but $\mathbb{Q}(\alpha,i)$ being a Galois extension, the group $Aut_{\mathbb{Q}}\big(\mathbb{Q}(\alpha,i)\big)$ has order 8, and all these possibilities are allowed.

Let σ denote the element satisfying $\sigma(\alpha)=\alpha\,i$ and $\sigma(i)=i$, which when restricted to being a permutation of $\{1,2,3,4\}$ corresponds to the circular permutation $(1,2,3,4)$; let τ denote the element satisfying $\tau(\alpha)=\alpha$ and $\tau(i)=-i$, which when restricted to being a permutation of $\{1,2,3,4\}$ corresponds to the transposition $(2,4)$;[6] then $\tau^{-1}\sigma\,\tau(i)=i=\sigma^{-1}(i)$ and $\tau^{-1}\sigma\,\tau(\alpha)=-\alpha\,i=\sigma^{-1}(\alpha)$, so that $\tau^{-1}\sigma\,\tau=\sigma^{-1}$ (or equivalently $\tau\,\sigma\,\tau=\sigma^3$), and such a relation between two generators characterizes the dihedral group D_4.

Lemma 34.6: For $\alpha=\sqrt[4]{2}$, besides $\mathbb{Q}$ itself, and $\mathbb{Q}(\alpha,i)$, which is an extension of $\mathbb{Q}$ of order 8, the intermediate fields (strictly) between $\mathbb{Q}$ and $\mathbb{Q}(\alpha,i)$ are:

$\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, and $\mathbb{Q}(\sqrt{2}\,i)$, which are extensions of $\mathbb{Q}$ of order 2,

$\mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha\,i)$, $\mathbb{Q}\big(\alpha\,(1-i)\big)$, $\mathbb{Q}\big(\alpha\,(1+i)\big)$, and $\mathbb{Q}(\sqrt{2},i)$, which are extensions of $\mathbb{Q}$ of order 4.

Proof: Because $\mathbb{Q}(\alpha,i)$ is a Galois extension of $\mathbb{Q}$, one must make the list of all subgroups of the dihedral group D_4, and identify the corresponding intermediate fields fixed by the subgroups. The group is made of e, $\sigma=(1234)$, $\sigma^2=(13)\,(24)$, $\sigma^3=(1432)$, $\tau=(24)$, $\tau\,\sigma=(14)\,(23)$, $\tau\,\sigma^2=(13)$, and $\tau\,\sigma^3=(12)\,(34)$.

The subgroups of order 2, corresponding to field extensions of $\mathbb{Q}$ of order 4, are

$\{e,(24)\}$: fixes α, so the fixed field contains $\mathbb{Q}(\alpha)$, but $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$, so that the fixed field is $\mathbb{Q}(\alpha)$;

$\{e,(13)\}$: fixes $\alpha\,i$, and similarly the fixed field is $\mathbb{Q}(\alpha\,i)$,

$\{e,(13)\,(24)\}$: maps α to $-\alpha$, so it fixes $\alpha^2=\sqrt{2}$, and it fixes i, so that the fixed field is $\mathbb{Q}(\sqrt{2},i)$;

$\{e,(14)\,(23)\}$: maps α to $-\alpha\,i$, and $\alpha\,i$ to $-\alpha$, so it fixes $\beta=\alpha\,(1-i)$, and the fixed field contains $\mathbb{Q}(\beta)$; one has $\beta^2=-2\alpha^2 i$, $\beta^3=2\alpha^3(1-i)$, $\beta^4=-8$, and Eisenstein criterion does not apply to x^4+8, but 1, β, β^2 and β^3 are $\mathbb{Q}$-linearly independent, so that $[\mathbb{Q}(\beta):\mathbb{Q}]=4$, and the fixed field is $\mathbb{Q}(\beta)$;[7]

$\{e,(12)\,(34)\}$: maps α to $\alpha\,i$, and $\alpha\,i$ to α, so it fixes $\gamma=\alpha\,(1+i)$, and similarly the fixed field is $\mathbb{Q}(\gamma)$.

The subgroups of order 4, corresponding to field extensions of $\mathbb{Q}$ of order 2, are

$\{e,\sigma,\sigma^2,\sigma^3\}$: fixes i, so that the fixed field is $\mathbb{Q}(i)$;

$\{e,(24),(13),(13)\,(24)\}$: fixes α^2, so that the fixed field is $\mathbb{Q}(\sqrt{2})$;

$\{e,(12)\,(34),(13)\,(24),(14)\,(23)\}$: fixes $\alpha^2 i$, so that the fixed field is $\mathbb{Q}(\sqrt{2}\,i)$.

---

[5] It is defined by $\sigma_0\big(R(a)\big)=R(b)$ for all $R\in E[x]$.

[6] τ is the restriction of complex conjugation to $\mathbb{Q}(\alpha,i)$.

[7] It suffices to show that $\mathbb{Q}(\beta)$ is not an extension of $\mathbb{Q}$ of order 2, i.e. that 1, β, and β^2 are $\mathbb{Q}$-linearly independent.