On Dedekind-Kronecker-Kneser's Reciprocity Theorem

August 15, 2006

Introduction

Dedekind, around 1855 gave lecture on Galois theory and proved the following result. Let p and q be two irreducible polynomials of $K[X]$, where K is any commutative field, and let m and n be their respective degrees. Assume we have an extension of K which contains a root a of p and a root b of q, and suppose $p = \phi_1 \cdots \phi_s$ is the decomposition of p in irreducible factors in $K(b)[X]$, $q = \psi_1\psi_2 \cdots \psi_t$ the decomposition of q in irreducible factors in $K(a)[X]$; then $s = t$, and for a convenient ordering, the degrees m_i and n_i of ϕ_i and ψ_i are such that $m_i/n_i = m/n$. As explained in [3], this result was discovered independently by Kronecker and published first by Kneser. This result appears also as an exercice in [2], as an application of Galois theory and in [3], this result is proved directly, and plays then a key role in one possible development of Galois theory.

We give a possible analysis of this theorem.

If $u_1, \ldots, u_n$ are elements of a commutative ring we write $[u_1, \ldots, u_n]$ the ideal ("module" in Kronecker's terminology [3]) generated by $u_1, \ldots, u_n$.

1 Adjoint pairs and Dedekind-Kronecker-Kneser's Theorem

Let K be a commutative field. We assume to have two irreducible monic polynomials f and g of respective degrees m and n. Let L be $K[X]/[f]$ and M be $K[X]/[g]$. Since f and g are irreducible, L and M are two field extensions of K. In L the polynomial f has a root x, which is X mod. f, and in M the polynomial g has a root y, which is X mod. g.

The point of this note is to present an algorithm which, given any decomposition

$$f(X) = \phi_1(X, y) \ldots \phi_n(X, y)$$

in pairwise relatively prime polynomials, *not necessarily irreducible*, build another decomposition

$$g(Y) = \psi_1(x, Y) \ldots \psi_n(x, Y)$$

such that, furthermore, we have $nm_i = mn_i$ if m_i is the degree of $\phi_i(X, y)$ and n_i is the degree of $\psi_i(x, Y)$.

The algorithm is simply to take for $\psi_i(x, Y)$ the monic g.c.d. of $g(Y)$ and $\phi_i(x, Y)$. The rest of this note justifies this algorithm.

Given two polynomials $\phi_1(X, Y)$ and $\psi_1(X, Y)$ in $K[X, Y]$ we say that ϕ_1, ψ_1 are *adjoint* or that ϕ_1, ψ_1 is an *adjoint pair* w.r.t. $f(X), g(Y)$ if and only if we have, in the ring $K[X, Y]$

$$[\psi_1, f(X)] = [\psi_1, g(Y), f(X)] = [\phi_1, g(Y), f(X)] = [\phi_1, g(Y)]$$

Notice that if $\phi_1(X,Y), \psi_1(X,Y)$ is an adjoint pair then $\phi_1(X,y)$ is a g.c.d. of $f(X)$ and $\psi_1(X,y)$ in $M[X]$. This follows from the fact that we have $[f(X), \psi_1(X,Y)] = [\phi_1(X,Y)]$ mod. $g(Y)$. Similarly, $\psi_1(x,Y)$ is a g.c.d. of $g(Y)$ and $\phi_1(x,Y)$ in $L[X]$.

But these conditions are sufficient: if $\phi_1(X,y)$ is a g.c.d. of $f(X)$ and $\psi_1(X,y)$ in $M[X]$ *and* $\psi_1(x,Y)$ divides $g(Y)$ in $L[Y]$ we have

$$[\phi_1(X,Y), g(Y)] = [\psi_1(X,Y), f(X), g(Y)] = [\psi_1(X,Y), f(X)]$$

and so $\phi_1(X,Y), \psi_1(X,Y)$ is an adjoint pair.

Lemma 1.1 *If $\phi_1(X,Y) \in K[X,Y]$ is such that $\phi_1(X,y)$ divides $f(X)$ in $M[X]$ then there exists $\psi_1(X,Y)$ such that ϕ_1, ψ_1 are adjoint w.r.t. $f(X), g(Y)$.*

Proof. Since $\phi_1(X,y)$ divides $f(X)$ in $M[X]$ we have $[\phi_1, f(X), g(Y)] = [\phi_1, g(Y)]$ in $K[X,Y]$. Let $\psi_1(X,Y)$ in $K[X,Y]$ be such that $\psi_1(x,Y)$ is a g.c.d. of $\phi_1(x,Y)$ and $g(Y)$ in $L[Y]$. This means that we have $[\psi_1, f(X)] = [\phi_1, f(X), g(Y)]$. Since $\psi_1(x,Y)$ divides $g(Y)$ in $L[Y]$ we have also $[\psi_1, f(X)] = [\psi_1, g(Y), f(X)]$ and ϕ_1, ψ_1 is an adjoint pair w.r.t. $f(X), g(Y)$. $\square$

We can always chose $\psi_1(X,Y)$ of the form $Y^{m_1} + p_1(X)Y^{m_1-1} + \ldots + p_{m_1}(X)$ and, if it is on this form, the polynomial $\psi_1(x,Y)$ is then uniquely determined.

Lemma 1.2 *Assume that ϕ_i, ψ_i and ϕ_j, ψ_j are two adjoint pairs. If $\phi_i(X,y)$ and $\phi_j(X,y)$ are relatively prime in $L[X]$ then $\psi_i(x,Y)$ and $\psi_j(x,Y)$ are relatively prime in $M[Y]$.*

Proof. If $\phi_i(X,y)$ and $\phi_j(X,y)$ are relatively prime in $L[X]$ we have $1 \in [\phi_i, \phi_j, g(Y)]$. Also

$$[\phi_i, \phi_j, g(Y)] = [\phi_i, \phi_j, f(X), g(Y)] = [\phi_i, \psi_j, f(X), g(Y)] = [\psi_i, \psi_j, f(X), g(Y)] = [\psi_i, \psi_j, f(X)]$$

and hence $1 \in [\psi_i, \psi_j, f(X)]$ which shows that $\psi_i(x,Y)$ and $\psi_j(x,Y)$ are relatively prime in $M[Y]$. $\square$

Lemma 1.3 *Assume that we have a family $\phi_i, \psi_i,\ i = 1, \ldots, s$ of adjoint pairs. If $f(X)$ divides $\phi_1(X,y) \ldots \phi_s(X,y)$ in $L[X]$ then $g(Y)$ divides $\psi_1(x,Y) \ldots \psi_s(x,Y)$ in $M[Y]$.*

Proof. By assumption we have $[f(X), g(Y)] = [\phi_1 \ldots \phi_s, f(X), g(Y)]$. But since $[\phi_i, f(X), g(Y)] = [\psi_i, f(X), g(Y)]$ we get $[\phi_1 \ldots \phi_s, f(X), g(Y)] = [\psi_1 \ldots \psi_s, f(X), g(Y)]$ and so $[f(X), g(Y)] = [\psi_1 \ldots \psi_s, f(X), g(Y)]$. This means that $g(Y)$ divides $\psi_1(x,Y) \ldots \psi_s(x,Y)$ in $M[Y]$. $\square$

We can then deduce the following variation on Dedekind-Kronecker-Kneser's Theorem which does not require a complete decomposition in irreducible polynomials. It results directly from the previous Lemmas.

Proposition 1.4 *Assume $f(X) = \phi_1(X,y) \ldots \phi_s(X,y)$ is a decomposition of $f(X)$ in pairwise prime polynomials in $M[X]$. Let $\psi_i(X,Y)$ be the adjoint of $\phi_i(X,Y)$, monic as a polynomial in Y. Then we have $g(X) = \psi_1(x,Y) \ldots \psi_s(x,Y)$ and this is a decomposition of $g(Y)$ in pairwise relatively prime polynomials in $L[Y]$.*

Proof. Lemma 1.3 shows that $g(Y)$ divides $\psi_1(x,Y) \ldots \psi_s(x,Y)$. Lemma 1.2 shows that $\psi_i(x,Y)$ and $\psi_j(x,Y)$ are relatively prime and, by construction, each $\phi_i(x,Y)$ divides $g(Y)$. $\square$

Lemma 1.5 *Assume that ϕ_1, ψ_1 are adjoint. If n_1 is the degree of $\phi_1(X,y)$ in $M[X]$ and m_1 the degree of $\psi_1(x,Y)$ in $L[Y]$ then $nm_1 = mn_1$.*

Proof. $K[X,Y]/[\psi_1, f(X)] = L[Y]/[\psi_1(x,Y)]$ is of dimension m_1 over L and L is of dimension n over K, so $K[X,Y]/[\psi_1, f(X)]$ is of dimension nm_1 over K. Similarly the algebra $K[X,Y]/[\phi_1, g(Y)] = M[X]/[\phi_1(X,y)]$ is of dimension mn_1 over K. Since ϕ_1, ψ_1 are adjoint we have $K[X,Y]/[\psi_1, f(X)] = K[X,Y]/[\phi_1, g(Y)]$ and hence $nm_1 = mn_1$. □

Corollary 1.6 *(Dedekind-Kronecker-Kneser's Theorem) If $f(X) = \phi_1(X,y)\dots\phi_s(X,y)$ is a decomposition of $f(X)$ in irreducible polynomials in $M[X]$ and $g(Y) = \psi_1(x,Y)\dots\psi_t(x,Y)$ is a decomposition of $g(Y)$ in irreducible polynomials in $L[Y]$ then $s = t$ and for a convenient ordering $\phi_i(X,Y), \psi_i(X,Y)$ are adjoint.*

References

[1] Scharlau, W. Unveröffentlichte algebraische Arbeiten Richard Dedekinds aus seiner Göttinger Zeit 1855–1858. Arch. Hist. Exact Sci. 27 (1982), no. 4, 335–367.

Dedekind, R. Über einen arithmetischen Satz von Gauss. *Werke*, Vol.2, 28-38, 1892.

[2] Edwards, H. *Galois Theory.* Birkhäuser Boston, Inc., Boston, MA, 1990.

[3] Edwards, H. *Essays on Constructive Mathematics.* Springer-Verlag, New York, 2005.