# Solutions Exercise sheet 11

**1.** The *Sylvester matrix* of two polynomials $f(X) := \sum_{i=0}^{m} a_i X^i$ and $g(X) := \sum_{j=0}^{n} a_j X^j$ over a ring $R$ is given by the $(m+n) \times (m+n)$ matrix

$$\mathrm{Sylv}_{f,g} := \begin{pmatrix} a_m & \dots & \dots & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & a_m & \dots & \dots & \dots & a_1 & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & 0 \\ 0 & \dots & 0 & a_m & \dots & \dots & \dots & a_1 & a_0 \\ b_n & \dots & \dots & b_1 & b_0 & 0 & \dots & \dots & 0 \\ 0 & b_n & \dots & \dots & b_1 & b_0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & b_n & \dots & \dots & b_1 & b_0 \end{pmatrix}.$$

The determinant of the Sylvester matrix is called the *resultant of $f$ and $g$* and is denoted by $\mathrm{Res}_{f,g} \in R$.

(a) Compute the resultant of the polynomials $X^3 - X + 1$ and $X^2 + X + 3$.

(b) For two arbitrary polynomials $f, g$ over a ring $R$ prove that

$$\mathrm{Res}_{g,f} = (-1)^{mn}\,\mathrm{Res}_{f,g}$$

(c) For $K$ a field, let $f, g \in K[X]$ be two polynomials. Prove: the resultant of $f$ and $g$ is equal to zero if and only if the two polynomials have a common root.

(d) For polynomials $f(X) = a_m \prod_{i=1}^{m}(X - \alpha_i)$ and $g(X) = b_n \prod_{j=1}^{n}(X - \beta_j)$ prove:

$$\mathrm{Res}_{f,g} = a_m^n \cdot b_n^m \cdot \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i - \beta_j).$$

(e) Let $f(X) = a_0 + a_1 X + \dots + a_{m-1}X^{m-1} + X^m$ be a polynomial over a ring $R$. Let $\Delta(f)$ denote its discriminant (see exercise sheet 10). Show that

$$\Delta(f) = (-1)^{\frac{m(m-1)}{2}}\,\mathrm{Res}_{f,f'},$$

where $f'$ denotes the derivative of $f$.

(f) Determine a general formula for the discriminant of an arbitrary polynomial of degree $2, 3$ and $4$.

*Solution*:

(a) By definition of the resultant, we get

$$\mathrm{Res}_{X^3-X+1,X^2+X+3} = \det \begin{pmatrix} 1 & 0 & -1 & 1 & 0 \\ 0 & 1 & 0 & -1 & 1 \\ 1 & 1 & 3 & 0 & 0 \\ 0 & 1 & 1 & 3 & 0 \\ 0 & 0 & 1 & 1 & 3 \end{pmatrix} = 55.$$

(b) Let $f, g$ be arbitrary polynomials over a ring $R$. Then we obtain $\mathrm{Sylv}_{g,f}$ from $\mathrm{Sylv}_{f,g}$ by swapping two rows $m \cdot n$ times. Every time we swap two rows, the determinant of $\mathrm{Sylv}_{f,g}$ changes sign, so we obtain

$$\det(\mathrm{Sylv}_{g,f}) = (-1)^{mn} \det(\mathrm{Sylv}_{f,g}).$$

(c) Write $f(X) = \sum^m a_i X^i$, $g = \sum^n b_j X^j$ and denote by $\mathrm{Sylv}_{f,g}$ the Sylvester matrix. For $i > m$ and $i < 0$ set $a_i := 0$ and for $j > n$ and $j < 0$ set $b_j := 0$.

Then $\mathrm{Res}_{f,g} = 0$ if and only if the rows of $\mathrm{Sylv}_{g,f}$ are linearly dependent. This is equivalent to the following: there exist an element $(c_1, \ldots, c_n, d_1, \ldots, d_m) \in K^{m+n} \backslash \{\underline{0}\}$ such that for every $1 \leqslant j \leqslant m+n$ we have

$$\sum_{i=1}^{n} c_i a_{m+j-i} = \sum_{i=1}^{m} d_i b_{n+i-j}.$$

This is equivalent to

$$\sum_{j=1}^{m+n} \left( \sum_{i=1}^{n} c_i a_{m+j-i} \right) X^{m+n-j} = \sum_{j=1}^{m+n} \left( \sum_{i=1}^{m} d_i b_{n+i-j} \right) X^{m+n-j}. \tag{1}$$

Writing $m - j + i = k$, we can rewrite the left hand side of (1) as

$$\sum_{i,k} c_i a_k X^{k+n-i} = \left( \sum_{i=1}^{n} c_i X^{n-i} \right) \cdot \left( \sum_{k} a_k X^k \right) =: u \cdot f.$$

Similarly, writing $n + i - j = k$, the right hand side of (1) is equal to

$$\sum_{i,k} d_i b_k X^{k+m-i} = \left( \sum_{i=1}^{m} d_i X^{m-i} \right) \cdot \left( \sum_{k} b_k X^k \right) =: v \cdot g.$$

Hence (1) holds if and only if there exist $u, v \in K[X]$ not both zero, with $\deg(u) < n, \deg(v) < m$ and

$$u \cdot f = v \cdot g. \tag{2}$$

Then $\deg(u) = \deg(v) + \deg(g) - \deg(f) < m + n - n = m$, and similarly $\deg(v) < n$. Thus, comparing the degrees of the polynomials in equation (2) we obtain that this is equivalent to $f$ and $g$ having a common root.

(d) Write $f(X) = \sum^m a_i X^i$, $g = \sum^n b_j X^j$. Then we can express $\det(\mathrm{Sylv}_{f,g})$ in terms of $a_m, b_n, \{\alpha_i\}_i, \{\beta_j\}_j$. The polynomials $f$ and $g$ have a common zero if and only if there

exist $i, j$ with $\alpha_i = \beta_j$, i.e. $\alpha_i - \beta_j = 0$. Since $\mathrm{Res}_{f,g} = 0$ if and only if $\alpha_i - \beta_j = 0$ by part (c), we have that $\alpha_i - \beta_j$ divides $\mathrm{Res}_{f,g}$ for all $1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n$.
By looking at the definition of the Sylvester matrix for $f$ and $g$, we see that $a_m$ divides the first $n$ rows, and $b_n$ divides the rows $n+1$ to $n+m$. Thus $a_m^n \cdot b_n^m \cdot \prod_{i=1}^m \prod_{j=1}^n (\alpha_i - \beta_j)$ divides $\mathrm{Res}_{f,g}$.
Now, note that

$$\det(\mathrm{Sylv}_{f,g}) = a_m^n \cdot b_n^m \begin{pmatrix} 1 & \dots & \dots & \dots & \dots & \prod_{i=1}^m \alpha_i & 0 & \dots & 0 \\ 0 & 1 & \dots & \dots & \dots & \dots & \prod_{i=1}^m \alpha_i & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & & & \ddots & 0 \\ 0 & \dots & 0 & 1 & \dots & \dots & \dots & \prod_{i=1}^m \alpha_i & \\ 1 & \dots & \dots & \dots & \prod_{j=1}^n \beta_j & 0 & \dots & \dots & 0 \\ 0 & 1 & \dots & \dots & \dots & \prod_{j=1}^n \beta_j & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & & & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & & & & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 & \dots & \dots & \dots & \prod_{j=1}^n \beta_j \end{pmatrix},$$

so by looking at the upper- and lower-triangular submatrices of $\mathrm{Sylv}_{f,g}$ which have ones on the diagonal, we obtain that

$$\mathrm{Res}_{f,g} = a_m^n \cdot b_n^m \prod_{i=1}^m \alpha_i^n + \dots + a_m^n \cdot b_n^m \prod_{j=1}^n \beta_j^m.$$

Hence we obtain part (d).

(e) Write $f(X) = \prod_{i=1}^m (X - \alpha_i)$. From Exercise sheet 10, question 5 recall the definition of the discriminant of $f$:

$$\Delta(f) = \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2.$$

Taking the derivative of $f$, we get

$$f'(X) = \sum_{k=1}^m \prod_{i \neq k} (X - \alpha_i),$$

which implies

$$f'(\alpha_j) = \sum_{k=1}^m \prod_{i \neq k} (\alpha_j - \alpha_i) = \prod_{i \neq j} (\alpha_j - \alpha_i).$$

If we write $f'(X) = b \cdot \prod_{j=1}^{m-1} (X - \beta_j)$ then by part (d),

$$\mathrm{Res}_{f,f'} = \prod_{i=1}^m b \cdot \prod_{j=1}^{m-1} (\alpha_i - \beta_j) = \prod_{i=1}^m f'(\alpha_i),$$

and hence

$$\begin{aligned}
(-1)^{\frac{m(m-1)}{2}} \cdot \operatorname{Res}_{f,f'} &= (-1)^{\frac{m(m-1)}{2}} \cdot \prod_{i=1}^{m} f'(\alpha_i) \\
&= (-1)^{\frac{m(m-1)}{2}} \cdot \prod_{i=1}^{m} \prod_{i \neq j} (\alpha_j - \alpha_i) \\
&= \prod_{i<j} (\alpha_i - \alpha_j)^2.
\end{aligned}$$

(f) Consider $f(X) := X^2 + bX + c$. Then

$$\operatorname{Sylv}_{f,f'} = \begin{pmatrix} 1 & b & c \\ 2 & b & 0 \\ 0 & 2 & b \end{pmatrix},$$

so that $\det(\operatorname{Sylv}_{f,f'}) = b^2 + 4c - 2b^2 = 4c - b^2$, and thus $\Delta(f) = b^2 - 4c$.
Similarly for a polynomial of degree 3 and 4, say $f(X) := X^3 + bX^2 + cX + d$ and $g(X) := X^4 + bX^3 + cX^2 + dX + e$, one can compute the determinant of the Sylvester matrix to get

$$\Delta(f) = b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd,$$

and

$$\begin{aligned}
\Delta(g) =& 256e^3 - 192bde^2 - 128c^2e^2 + 144cd^2e - 27d^4 + 144b^2ce^2 - 6b^2d^2e - 80bc^2de \\
&+ 18bcd^3 + 16c^4e - 4c^3d^2 - 27b^4e^2 + 18b^3cde - 4b^3d^3 - 4b^2c^3e + b^2c^2d^2 \,.
\end{aligned}$$

**2.** Let $n$ be a positive integer, and $P \in \mathbb{Z}[X]$ a monic irreducible factor of $X^n - 1 \in \mathbb{Q}[X]$. Suppose that $\zeta$ is a root of $P$.

(a) Show that for each $k \in \mathbb{Z}_{\geqslant 0}$ there exists a unique polynomial $R_k \in \mathbb{Z}[X]$ such that $\deg(R_k) < \deg(P)$ and $P(\zeta^k) = R_k(\zeta)$. Prove that $\{R_k | k \in \mathbb{Z}_{\geqslant 0}\}$ is a finite set. We define

$$a := \sup\{|u| : u \text{ is a coefficient of some } R_k\}$$

(b) Show that for $k = p$ a prime, $p$ divides all coefficients of $R_p$, and that when $p > a$ one has $R_p = 0$ (*Hint:* $P(\zeta^p) = P(\zeta^p) - P(\zeta)^p$).

(c) Deduce that if all primes dividing some positive integer $m$ are strictly greater then $a$, then $P(\zeta^m) = 0$.

(d) Prove that if $r$ and $n$ are coprime, then $P(\zeta^r) = 0$ (*Hint:* Consider the quantity $m = r + n \prod_{p \leqslant a, p \nmid r} p$).

(e) Recall the definition of $n$-th cyclotomic polynomial $\Phi_n$ for $n \in \mathbb{Z}_{>0}$: we take $W_n \subseteq \mathbb{C}$ to be the set of primitive $n$-th roots of unity, and define

$$\Phi_n(X) := \prod_{x \in W_n} (X - x).$$

Prove the following equality for $n \in \mathbb{Z}_{>0}$:

$$\prod_{0<d|n} \Phi_d(X) = X^n - 1,$$

and deduce that $\Phi_n \in \mathbb{Z}[X]$ for every $n$.

(f) Prove that the $n$-th cyclotomic polynomial is irreducible. (*Hint:* Take $\zeta := \exp(2\pi i/n)$ and $P$ its minimal polynomial over $\mathbb{Q}$. Check that $P$ satisfies the required hypothesis to deduce that $\Phi_n(X)|P$ (using parts (a)-(d)). Then irreducibility of $P$ together with part (e) allow you to conclude.)

*Solution:* Recall that for a monic polynomial $f \in \mathbb{Z}[X]$ we know that $f$ is irreducible in $\mathbb{Z}[X]$ if and only if it is irreducible in $\mathbb{Q}[X]$.

(a) Since $P$ is monic and irreducible in $\mathbb{Z}[X]$, it is also irreducible in $\mathbb{Q}[X]$, so that $\mathbb{Q}(\zeta) \cong \mathbb{Q}[X]/(P(X))$ is an algebraic extension of $\mathbb{Q}$ of degree $\deg(P)$, and the elements $1, \zeta, \ldots, \zeta^{\deg(P)}$ are linearly independent. Then $P(\zeta^k) \in \mathbb{Q}(\zeta)$ cannot be expressed in more then one way as $P(\zeta^k) = R_k(\zeta)$ with $R_k \in \mathbb{Z}[X]$ of degree $< \deg(P)$, and we only have to check existence. This is a special case of proving that for each $f \in \mathbb{Z}[X]$ we have $f(\zeta) = b_0 + b_1\zeta + \cdots + b_{\deg(P)-1}\zeta^{\deg(P)-1}$ for some $b_i \in \mathbb{Z}$, which is easily proven by induction on $\deg(f)$: the statement is trivial for all $\deg(f) < \deg(P)$; for bigger degree, we see that the degree of $f$ can be lowered (up to equivalence modulo $P$) by substituting the maximal power $X^{\deg(P)+a}$ of $X$ in $f$ with $X^a(X^{\deg(P)} - P(X))$, which has degree strictly smaller then $\deg(P) + a$ as $P$ is monic, so that the inductive hypothesis can be applied.

(More simply, one can notice that $\mathbb{Z}[X]$ is a unique factorization domain, and that Euclidean division of $f$ by $P$ can be performed (as in $\mathbb{Q}[X]$), so that $R_k(X)$ is nothing but the residue of the division of $R(X^k)$ by $P(X)$.)

Since $\zeta^k = \zeta^h$ for $n|k-h$, the set $\{\zeta^k : k \in \mathbb{Z}_{\geqslant 0}\}$ is finite, and so is the set of the $R_k$'s.

(b) Notice that for $f \in \mathbb{Z}[X]$ one has that $f(X^p) - f(X)^p$ is divisible by $p$. Indeed, we write $f = \sum_{j=0}^{s} \lambda_j X^j$ and consider the multinomial coefficient for a partition into positive integers $t = \sum_i t_i$:

$$(*)\ \binom{t}{t_1, \ldots, t_s} = \frac{t!}{t_1! \cdots t_s!} = \binom{t}{t_1}\binom{t-t_1}{t_2}\binom{t-t_1-t_2}{t_3}\cdots\binom{t_{s-1}+t_s}{t_{s-1}} \in \mathbb{Z},$$

which counts the number of partitions of a set of $t$ elements into subsets of $t_1, t_2, \ldots, t_s$ elements, and we have

$$\begin{aligned} f(X^p) - f(X)^p &= \sum_{j=0}^{s} \lambda_j X^{jp} - \sum_{\substack{e_0+\cdots+e_j=p \\ 0\leqslant e_j \leqslant p}} \binom{p}{e_0, \ldots, e_s} \prod_j^{s} (\lambda_j)^{e_j} X^{je_j} \\ &= \sum_{j=0}^{s} (\lambda_j - \lambda_j^p) X^{jp} - \sum_{\substack{e_0+\cdots+e_j=p \\ 0\leqslant e_j < p}} \binom{p}{e_0, \ldots, e_s} \prod_{j=0}^{s} (\lambda_j)^{e_j} X^{je_j}. \end{aligned}$$

By Fermat's little theorem we have $p|\lambda_j - \lambda_j^p$ for each $j$. Moreover, each multinomial coefficient appearing in the second sum is divisible by $p$, because the definition in terms of factorials in $(*)$ makes it clear that none of the $e_j$ has $p$ as a factor, so that $p$ does not cancel out while simplifying the fraction, which belongs to $\mathbb{Z}$. Hence $p|f(X^p)-f(X)^p$. We can then write $P(\zeta^p) = P(\zeta^p) - P(\zeta)^p = pQ(\zeta)$ for some $Q(X) \in \mathbb{Z}[X]$, and by what we proved in the previous point we can write $Q(\zeta) = R_Q(\zeta)$ for some polynomial $R_Q \in \mathbb{Z}[X]$ of degree strictly smaller than $\deg(P)$. This gives $R_p(\zeta) = P(\zeta^p) = pR_Q(\zeta)$, and by uniqueness of $R_p$ we can conclude that $R_p = pR_Q \in p\mathbb{Z}[X]$.

If $p > a$, then the absolute values of the coefficients of $R_p$ are non-negative multiples of $p$, and by definition of $a$ they need to be zero, so that $R_p = 0$ in this case.

(c) This is an easy induction on the number $s$ of primes (counted with multiplicity) dividing $m$. One can indeed write $m = \prod_{i=1}^{s} p_i$ for some primes $p_i > a$. For $s = 1$ this is just the previous point, because $R_{p_1} = 0$ means $P(\zeta^{p_1}) = 0$. More in general, by inductive hypothesis we can assume that $P(\zeta^{p_1 \cdots p_{s-1}}) = 0$, and apply the previous point with $\zeta^{p_1 \cdots p_{s-1}}$ (which is a root of $P$) instead of $\zeta$ to get $P((\zeta^{p_1 \cdots p_{s-1}})^{p_s}) = 0$.

(d) Let $m = r + n\prod_{p \leqslant a, p\nmid r} p$. For $q \leqslant a$ a prime, we see that $q$ either divides $r$ or $n\prod_{p \leqslant a, p\nmid r} p$, so that $q$ does not divide $m$ and by previous point we get $P(\zeta^m) = 0$. But $\zeta^n = 1$ by hypothesis (because $P|X^n - 1$), so that $\zeta^m = \zeta^r$ and we get $P(\zeta^r) = 0$.

(e) Let $\gamma_n = \prod_{0<d|n} \Phi_d$. Since a complex number belongs to $W_k$ if and only if it has multiplicative order $k$, all the $W_k$'s are disjoint. Then $\gamma_n$ has distinct roots, and its set of roots is $\bigcup_{0<d|n} W_d$. On the other hand, the roots of $X^n - 1$ are also all distinct: they are indeed the $n$ distinct complex numbers $\exp(2\pi ik/n)$ for $a = 0, \ldots, n-1$. It is then easy to see that the two polynomials have indeed the same roots, since a $n$-th root of unity has order $d$ dividing $n$, and primitive $d$-th roots of unity are $n$-th roots of unity for $d|n$. As both $\gamma_n$ and $\Phi_n$ are monic, unique factorization in $\mathbb{Q}[X]$ gives $\gamma_n = \Phi_n$ as desired.

We then prove that the coefficients of the $\Phi_n$ are integer by induction on $n$. For $n = 1$ we have $\Phi_n = X - 1 \in \mathbb{Z}[X]$. For $n > 1$, suppose that $\Phi_k \in \mathbb{Z}[X]$ for all $k < n$. Then

$$\Phi_n = \frac{X^n - 1}{\prod\limits_{\substack{0<d|n \\ d\neq n}} \Phi_d(X)},$$

and since the denominator lies in $\mathbb{Z}[X]$ by inductive hypothesis, we can conclude that $\Phi_n \in \mathbb{Z}[X]$. Indeed, $\Phi_n$ needs necessarily to lie in $\mathbb{Q}[X]$ (else, for $l$ the minimal degree of a coefficient of $\Phi_n$ not lying in $\mathbb{Q}$ and $m$ the minimal degree of a non-zero coefficients of the denominator, one would get that the coefficient of degree $l+m$ in $X^n - 1$ would not lie in $\mathbb{Q}$, contradiction). We can then write the monic polynomial $\Phi_n$ as $\frac{1}{\mu}\Theta_n$ for some primitive polynomial $\Theta_n \in \mathbb{Z}[X]$, but then Gauss's lemma tells us that $X^n - 1$ equals $\frac{1}{d}$ times a primitive polynomial, and the only possibility is $d = \pm 1$, which implies that $\Phi_n \in \mathbb{Z}[X]$.

(f) $\zeta = \exp(2\pi i/n)$ satisfies both its minimal polynomial $P$ and $X^n - 1$, so that $P|X^n - 1$. Being $X^n - 1$ and $P$ monic we necessarily have $P \in \mathbb{Z}[X]$ by Gauss's lemma. Then $W_n = \{\zeta^r : 0 < r < n, (r,n) = 1\}$, so that by part (d) we get $P(x) = 0$ for each $x \in W_n$ and by definition of $\Phi_n$ we obtain $\Phi_n|P$. This is a divisibility relation between two polynomials in $\mathbb{Q}[X]$, hence an equality as $P$ is irreducible in $\mathbb{Q}[X]$. In particular, the cyclotomic polynomial $\Phi_n$ is itself irreducible.

**3**. Let $L$ be a splitting field of the polynomial $X^6 - 5$ over $\mathbb{Q}$. Determine all intermediate fields of $L : \mathbb{Q}$ together with their inclusions.

*Solution*: Since $\mathbb{C}$ is algebraically closed, we can assume $L$ to be embedded in $\mathbb{C}$. Let $a$ be the positive real sixth root of 5. Let $\zeta$ be a primitive third root of unity in $\mathbb{C}$. For $1 \leqslant i \leqslant 6$ let $a_i := a \cdot (-\zeta)^{i-1}$. Then $a_i^6 - 5 = a^6 \cdot (-\zeta)^{6i-6} - 5 = 0$, so $a_1, \ldots, a_6$ are the six different zeros of $X^6 - 5$. Thus $L = \mathbb{Q}(a_1, \ldots, a_6) \subset \mathbb{Q}(a, \zeta)$, and because $a_1 = a$ and $-\frac{a_2}{a_1} = -\frac{a \cdot (-\zeta)}{a} = \zeta$, even $L = \mathbb{Q}(a, \zeta)$.

For $1 \leqslant i \leqslant 6$ we have $[\mathbb{Q}(a_i) : \mathbb{Q}] = 6$, since $X^6 - 5$ is irreducible according to the Eisenstein criterion. Because $\zeta \notin \mathbb{Q}(a) \subset \mathbb{R}$ is also $[L : \mathbb{Q}(a)] = 2$, and thus $[L : \mathbb{Q}] = [L : \mathbb{Q}(a)] \cdot [\mathbb{Q}(a) : \mathbb{Q}] = 12$. In particular, $\operatorname{Gal}(L : \mathbb{Q})$ also has order 12.

In the following, we consider $\operatorname{Gal}(L : \mathbb{Q})$ as a subgroup of $S_6$ given by the embedding induced by $a_i \mapsto i$.

Since $L : \mathbb{Q}$ is normal, the restriction $\sigma$ of the complex conjugation to $L$ is an element of $\operatorname{Gal}(L : \mathbb{Q})$. Specifically, $\sigma$ corresponds to the permutation $(2\,6)(3\,5)$.

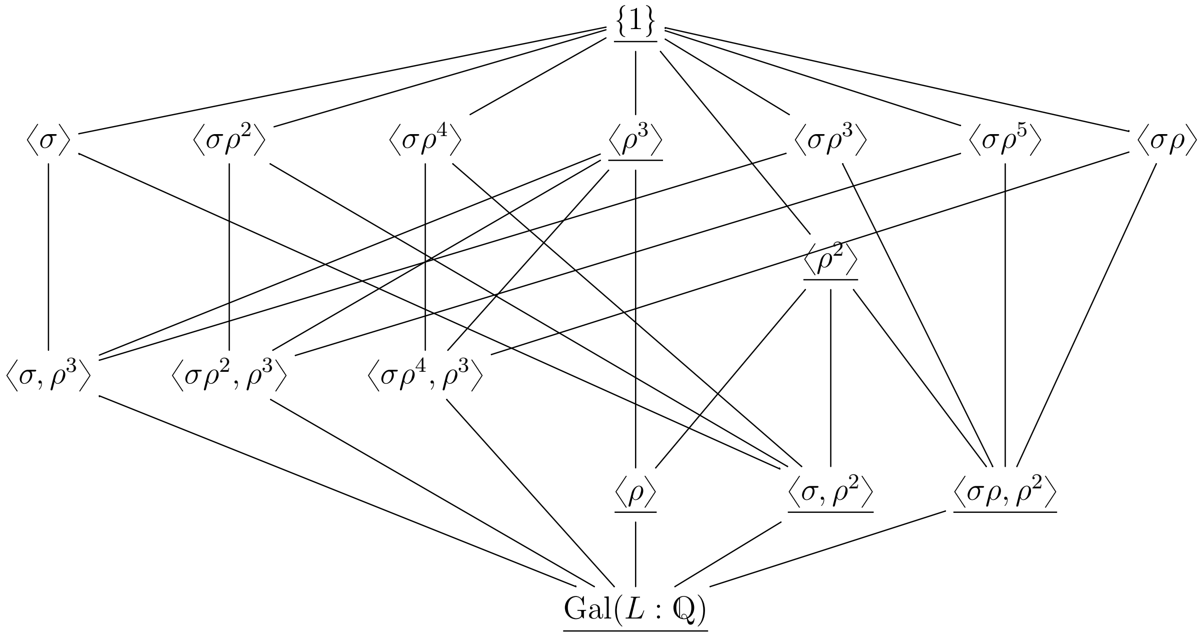
Since $X^6 - 5$ is irreducible, $\operatorname{Gal}(L : \mathbb{Q})$ operates transitively on its zeros; hence there exists $\rho \in \operatorname{Gal}(L : \mathbb{Q})$ with $\rho(a_1) = a_2$. Because $\sigma(a_1) = a_1$, we have $(\rho\sigma)(a_1) = a_2$. Since $\sigma$ swaps the two zeros $\zeta$ and $\zeta^2$ of the irreducible polynomial $X^2 + X + 1$ and $\rho$ swaps or fixes them as $\mathbb{Q}$-homomorphisms, we can therefore assume (by replacing $\rho$ by $\rho\sigma$ if necessary) without loss of generality, that $\rho(\zeta) = \zeta$. Then $\rho(a_i) = \rho\big(a \cdot (-\zeta)^{i-1}\big) = a \cdot (-\zeta)^i$, so $\rho$ has the representation $(1\,2\,3\,4\,5\,6)$.

The calculation $\sigma\rho\sigma^{-1} = (2\,6)(3\,5)(1\,2\,3\,4\,5\,6)(2\,6)(3\,5) = (6\,5\,4\,3\,2\,1) = \rho^{-1}$ now shows that

$$\langle \rho, \sigma \rangle = \langle \rho, \sigma \mid \sigma^2 = \rho^6 = 1, \sigma\rho\sigma^{-1} = \rho^{-1} \rangle \cong D_6,$$

so the subgroup generated by $\rho$ and $\sigma$ has at least order 12, and since $|\operatorname{Gal}(L : \mathbb{Q})| = 12$, we obtain $\operatorname{Gal}(L : \mathbb{Q}) = \langle \rho, \sigma \rangle \cong D_6$.

We now make a list of all subgroups of $\operatorname{Gal}(L : \mathbb{Q}) \cong D_6$ (we leave the detailed verification to the reader); normal subgroups are underlined:

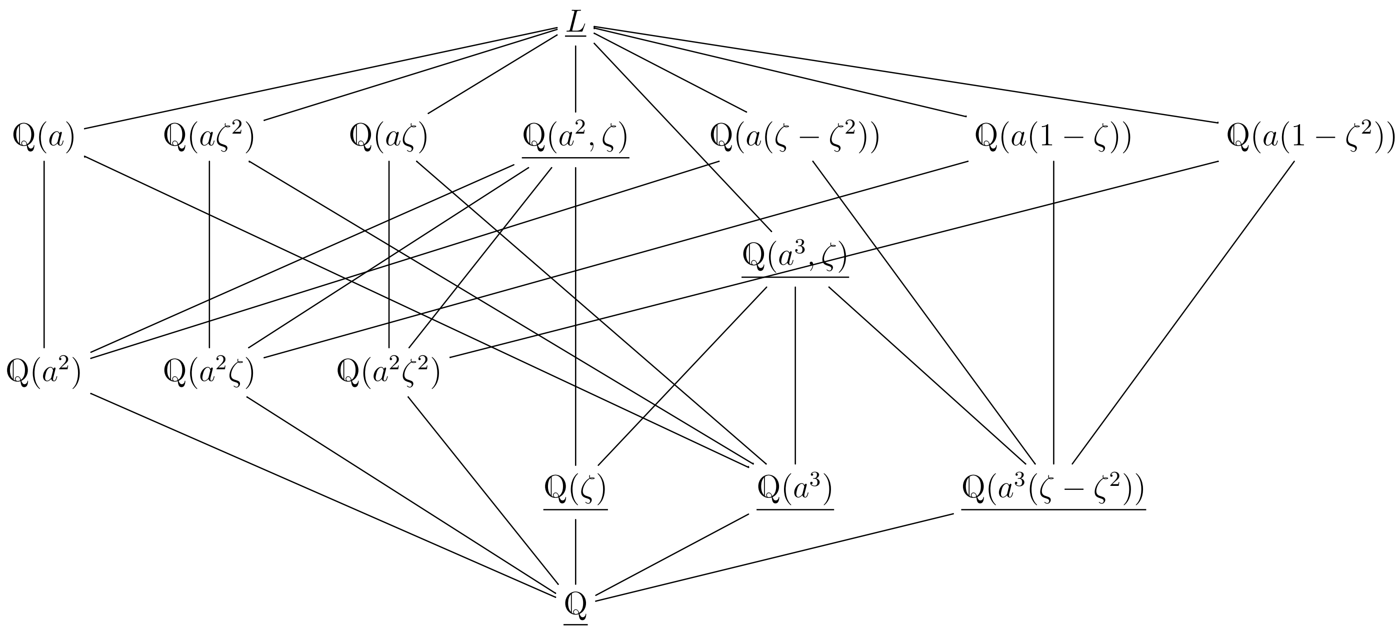



From this we now deduce the set-up of the intermediate fields; the Galois correspondence assigns to a subgroup $H < \mathrm{Gal}(L:\mathbb{Q})$ the fixed field $L^H$ with the extension degree $[L^H : \mathbb{Q}] = \frac{|\mathrm{Gal}(L:\mathbb{Q})|}{|H|} = \frac{12}{|H|}$:

- $L^{\{1\}} = L$.
- $L^{\mathrm{Gal}(L:\mathbb{Q})} = \mathbb{Q}$.
- It is $\sigma(a) = a$, thus $\mathbb{Q}(a) \subset L^{\langle\sigma\rangle}$. In addition, $[\mathbb{Q}(a) : \mathbb{Q}] = 6 = \frac{12}{|\langle\sigma\rangle|}$, i.e. $L^{\langle\sigma\rangle} = \mathbb{Q}(a)$.
- Analogously, $(\sigma\rho^2)(a\zeta^2) = a\zeta^2$, i.e. $\mathbb{Q}(a\zeta^2) \subset L^{\langle\sigma\rho^2\rangle}$. In addition, $[\mathbb{Q}(a\zeta^2) : \mathbb{Q}] = 6 = \frac{12}{|\langle\sigma\rho^2\rangle|}$, i.e. $L^{\langle\sigma\rho^2\rangle} = \mathbb{Q}(a\zeta^2)$.
- Analogously, $(\sigma\rho^4)(a\zeta) = a\zeta$, i.e. $\mathbb{Q}(a\zeta) \subset L^{\langle\sigma\rho^4\rangle}$. Furthermore, $[\mathbb{Q}(a\zeta) : \mathbb{Q}] = 6 = \frac{12}{|\langle\sigma\rho^4\rangle|}$, i.e. $L^{\langle\sigma\rho^4\rangle} = \mathbb{Q}(a\zeta)$.
- It is $\sigma(a^2) = \rho^3(a^2) = a^2$, so $\mathbb{Q}(a^2) \subset L^{\langle\sigma,\rho^3\rangle}$. In addition, $a^2$ is a zero of the polynomial $X^3 - 5$ which is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(a^2) : \mathbb{Q}] = 3 = \frac{12}{|\langle\sigma,\rho^3\rangle|}$ and thus $L^{\langle\sigma,\rho^3\rangle} = \mathbb{Q}(a^2)$.
- Analogously, $(\sigma\rho^2)(a^2\zeta) = \rho^3(a^2\zeta) = a^2\zeta$, thus $\mathbb{Q}(a^2\zeta) \subset L^{\langle\sigma\rho^2,\rho^3\rangle}$. Moreover, $a^2\zeta$ is a zero of the polynomial $X^3 - 5$ irreducible over $\mathbb{Q}$, so $[\mathbb{Q}(a^2\zeta) : \mathbb{Q}] = 3 = \frac{12}{|\langle\sigma\rho^2,\rho^3\rangle|}$ and thus $L^{\langle\sigma\rho^2,\rho^3\rangle} = \mathbb{Q}(a^2\zeta)$.
- Analogously, $(\sigma\rho^4)(a^2\zeta^2) = \rho^3(a^2\zeta^2) = a^2\zeta^2$, i.e. $\mathbb{Q}(a^2\zeta^2) \subset L^{\langle\sigma\rho^4,\rho^3\rangle}$. Furthermore, $a^2\zeta^2$ is a zero of the polynomial $X^3 - 5$ irreducible over $\mathbb{Q}$, thus $[\mathbb{Q}(a^2\zeta^2) : \mathbb{Q}] = 3 = \frac{12}{|\langle\sigma\rho^4,\rho^3\rangle|}$ and thus $L^{\langle\sigma\rho^4,\rho^3\rangle} = \mathbb{Q}(a^2\zeta^2)$.
- It is $\rho(\zeta) = \zeta$, thus $\mathbb{Q}(\zeta) \subset L^{\langle\rho\rangle}$. Furthermore, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2 = \frac{12}{|\langle\rho\rangle|}$, thus $\mathbb{Q}(\zeta) = L^{\langle\rho\rangle}$.
- It is $\sigma(a^3) = \rho^2(a^3) = a^3$, so $\mathbb{Q}(a^3) \subset L^{\langle\sigma,\rho^2\rangle}$. Moreover, $a^3$ is a zero of the irreducible polynomial $X^2 - 5$ over $\mathbb{Q}$, so $[\mathbb{Q}(a^3) : \mathbb{Q}] = 2 = \frac{12}{|\langle\sigma,\rho^2\rangle|}$ and thus $\mathbb{Q}(a^3) = L^{\langle\sigma,\rho^2\rangle}$.

- It is $\rho^2(a^3) = a^3$ and $\rho^2(\zeta) = \zeta$, thus $\mathbb{Q}(a^3, \zeta) \subset L^{\langle \rho^2 \rangle}$. Because $\zeta \notin \mathbb{Q}(a^3) \subset \mathbb{R}$ is $[\mathbb{Q}(a^3, \zeta) : \mathbb{Q}] = [\mathbb{Q}(a^3, \zeta) : \mathbb{Q}(a^3)][\mathbb{Q}(a^3) : \mathbb{Q}] = 4$, thus $[\mathbb{Q}(a^3, \zeta) : \mathbb{Q}] = \frac{12}{|\langle \rho^2 \rangle|}$ and therefore $L^{\langle \rho^2 \rangle} = \mathbb{Q}(a^3, \zeta)$.
- Analogously, $\rho^3(a^2) = a^2$ and $\rho^3(\zeta) = \zeta$, thus $\mathbb{Q}(a^2, \zeta) \subset L^{\langle \rho^3 \rangle}$. Because $\zeta \notin \mathbb{Q}(a^2) \subset \mathbb{R}$ is $[\mathbb{Q}(a^2, \zeta) : \mathbb{Q}] = [\mathbb{Q}(a^2, \zeta) : \mathbb{Q}(a^2)][\mathbb{Q}(a^2) : \mathbb{Q}] = 6$, thus $[\mathbb{Q}(a^2, \zeta) : \mathbb{Q}] = \frac{12}{|\langle \rho^3 \rangle|}$ and therefore $L^{\langle \rho^3 \rangle} = \mathbb{Q}(a^2, \zeta)$.
- $(\sigma\rho^3)(a\zeta) = -a\zeta^2$ and therefore $(\sigma\rho^3)(a(\zeta - \zeta^2)) = a(\zeta - \zeta^2)$ because $(\sigma\rho^3)^2 = 1_L$; so $\mathbb{Q}(a(\zeta - \zeta^2)) is \subset L^{\langle \sigma\rho^3 \rangle}$. In addition, $a(\zeta - \zeta^2)$ is a zero of the polynomial $X^6 + 135$, and this is irreducible over $\mathbb{Q}$ according to the Eisenstein criterion with respect to the prime number $5$. Therefore, $[\mathbb{Q}(a(\zeta - \zeta^2)) : \mathbb{Q}] = 6 = \frac{12}{|\langle \sigma\rho^3 \rangle|}$ and thus $L^{\langle \sigma\rho^3 \rangle} = \mathbb{Q}(a(\zeta - \zeta^2))$.
- Analogously, $(\sigma\rho^5)(a) = -a\zeta$ and thus $(\sigma\rho^5)(a(1 - \zeta)) = a(1 - \zeta)$ because $(\sigma\rho^5)^2 = 1_L$; therefore $\mathbb{Q}(a(1 - \zeta)) \subset L^{\langle \sigma\rho^5 \rangle}$. In addition, $a(1 - \zeta)$ is a zero of the polynomial $X^6 + 135$. Therefore, $[\mathbb{Q}(a(1 - \zeta)) : \mathbb{Q}] = 6 = \frac{12}{|\langle \sigma\rho^5 \rangle|}$ and thus $L^{\langle \sigma\rho^5 \rangle} = \mathbb{Q}(a(1 - \zeta))$.
- Analogously, $(\sigma\rho)(a) = -a\zeta^2$ and therefore $(\sigma\rho)(a(1 - \zeta^2)) = a(1 - \zeta^2)$ because $(\sigma\rho)^2 = 1_L$; thus $\mathbb{Q}(a(1 - \zeta^2)) is \subset L^{\langle \sigma\rho \rangle}$. In addition, $a(1 - \zeta^2)$ is a zero of the polynomial $X^6 + 135$. Therefore, $[\mathbb{Q}(a(1 - \zeta^2)) : \mathbb{Q}] = 6 = \frac{12}{|\langle \sigma\rho \rangle|}$ and thus $L^{\langle \sigma\rho \rangle} = \mathbb{Q}(a(1 - \zeta^2))$.
- It is $L^{\langle \sigma\rho, \rho^2 \rangle} = L^{\langle \sigma\rho \rangle} \cap L^{\langle \rho^2 \rangle} = \mathbb{Q}(a^3, \zeta) \cap \mathbb{Q}(a(1 - \zeta^2)) \ni (a(1 - \zeta^2))^3 = 3a^3(\zeta - \zeta^2)$. Because $[L^{\langle \sigma\rho, \rho^2 \rangle} : \mathbb{Q}] = \frac{12}{|\langle \sigma\rho, \rho^2 \rangle|} = 2$ and $a^3(\zeta - \zeta^2) \notin \mathbb{Q} \subset \mathbb{R}$ therefore $L^{\langle \sigma\rho, \rho^2 \rangle} = \mathbb{Q}(a^3(\zeta - \zeta^2))$.

In total, we obtain the following towers of fields:




*Remark.* An intermediate field above is underlined if the corresponding subgroup of $\mathrm{Gal}(L : \mathbb{Q})$ is normal.