Let $K$ be a field and let $f, g \in K[X]$. Suppose that

$$f = a\prod_{i=1}^{n}(X-\alpha_i), \qquad \text{and} \qquad g = b\prod_{j=1}^{m}(X-\beta_j),$$

for certain $\alpha_i$, $\beta_j$ and non-zero $a, b$ in a splitting field of $fg$.

**Definition.** The *resultant* $\mathrm{Res}(f,g)$ of $f$ and $g$ is defined by

$$\mathrm{Res}(f,g) = a^m b^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j).$$

Since the resultant is invariant under permutations of the $\alpha_i$ and of the $\beta_j$, it is contained in $K$. It vanishes if and only if $f$ and $g$ have a common zero. The resultant is not symmetric in $f$ and $g$, but almost. This is the content of part (a) of following proposition.

**Proposition.** *Let $f$ and $g$ be as above. Then*
*(a)* $\mathrm{Res}(f,g) = (-1)^{nm}\mathrm{Res}(g,f)$;
*(b)* $\mathrm{Res}(f,g) = a^m \prod_{i=1}^{n} g(\alpha_i)$;
*(c) If $g \equiv g_1 \pmod{f}$ in $K[X]$ for some $g_1 \in K[X]$ of degree $m_1$, we have*

$$\mathrm{Res}(f,g) = a^{m-m_1}\mathrm{Res}(f,g_1).$$

**Proof.** Parts (a) and (b) are trivial. If $g \equiv g_1 \pmod{f}$, we have

$$\prod_{i=1}^{n} g(\alpha_i) = \prod_{i=1}^{n} g_1(\alpha_i).$$

Part (c) therefore follows from part (b). This proves the proposition.

For a monic polynomial $f \in K[X]$ we define its *discriminant* $\mathrm{Disc}(f)$ as follows. Suppose that $f = \prod_{i=1}^{n}(X-\alpha_i)$ for some $\alpha_i$ in a splitting field of $f$. Then

$$\mathrm{Disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2.$$

The discriminant of $f$ is contained in $K$. It vanishes if and only if $\alpha_i = \alpha_j$ for some $i \neq j$. The following proposition expresses the discriminant in terms of a resultant.

**Proposition.** *Let $f \in K[X]$ be a monic polynomial. Then*

$$\mathrm{Disc}(f) = (-1)^{\frac{n(n-1)}{2}}\mathrm{Res}(f,f').$$

*Here $f'$ denotes the derivative of $f$.*

**Proof.** The formula for the discriminant of $f$ can also be written as

$$\mathrm{Disc}(f) \;=\; (-1)^{\frac{n(n-1)}{2}} \prod_{i\neq j}(\alpha_i - \alpha_j).$$

Since $f = \prod_{i=1}^{n}(X-\alpha_i)$, Leibniz's rule implies that

$$f'(X) \;=\; \prod_{i=1}^{n}\prod_{j\neq i}(X-\alpha_j),$$

and therefore $f'(\alpha_i) = \prod_{j\neq i}(\alpha_i - \alpha_j)$ for $i = 1,\ldots,n$. The result now follows from part (b) of the previous proposition.

**Exampe 1.** $f = X^2 + bX + c$. Since $n = 2$, the proposition implies that

$$\mathrm{Disc}(f) \;=\; -\mathrm{Res}(X^2 + bX + c, 2X + b)$$

By part (a) of Proposition 1 we can switch the two polynomials and by part (b) we find

$$\mathrm{Disc}(f) = -\mathrm{Res}(2X + b, X^2 + bX + c) = -2^2((-\tfrac{1}{2}b)^2 + b(-\tfrac{1}{2}b) + c) = b^2 - 4c.$$

**Exampe 2.** $f = X^3 + pX + q$. Since $n = 3$, the proposition implies that

$$\mathrm{Disc}(f) \;=\; -\mathrm{Res}(X^3 + pX + q, 3X^2 + p)$$

By part (a) of Proposition 1 we can switch the two polynomials and then we use the fact that $X^3 + pX + q - \frac{X}{3}(3X^2 + p) = \frac{2p}{3}X + q$. This means that

$$X^3 + pX + q \equiv \frac{2p}{3}X + q \pmod{3X^2 + p}$$

It follows that

$$\mathrm{Disc}(f) = -\mathrm{Res}(3X^2 + p, X^3 + pX + q) = -3^2\mathrm{Res}(3x^2 + p, \tfrac{2p}{3}X + q).$$

Switching the polynomials once again and then using (b) finally gives

$$\mathrm{Disc}(f) = 3^2\mathrm{Res}(\tfrac{2p}{3}X + q, 3x^2 + p) = -9(\tfrac{2p}{3})^2(3(\tfrac{3q}{2p})^2 + p) = -4p^3 - 27q^2$$

**Exampe 3.** $f = X^5 + X + 1$, and $f' = 5x^4 + 1$. Since $n = 5$, the proposition implies that

$$\mathrm{Disc}(f) \;=\; \mathrm{Res}(f, f')$$
$$= \mathrm{Res}(f', f) = \mathrm{Res}(5X^4 + 1, X^5 + X + 1),$$

by part (a) of Proposition 1. Next write $f = qf' + r$

$$X^5 + X + 1 = \frac{X}{5}(5X^4 + 1) + \frac{4}{5}X + 1$$

which is equivalent to $f \equiv r \bmod f'$, and use part (c) of Proposition 1, to obtain

$$\mathrm{Disc}(f) = \mathrm{Res}(5X^4 + 1, X^5 + X + 1) = 5^{5-1}\mathrm{Res}(5X^4 + 1, \tfrac{4}{5}X + 1).$$

Switching the polynomials again and using (b) then gives

$$\mathrm{Disc}(f) = 5^4\mathrm{Res}(\tfrac{4}{5}X + 1, 5X^4 + 1) = 5^4(\tfrac{4}{5})^4(5(-\tfrac{5}{4})^4 + 1) = 5^5 + 4^4 = 3381.$$