$\mathbb{C}$ is algebraically closed. Paul Taylor

1. This examples sheet is based directly on Gauss' 1815 paper, DEMONSTRATIO NOVA ALTERA THEOREMATIS OMNEM FUNCTIONEM ALGEBRAICAM RATIONALEM INTEGRAM UNIUS VARIABILIS IN FACTORES REALES PRIMI VEL SECUNDI GRADUS RESOLVI POSSE which will be found as pp. 33-56 of vol. III of his collected works. It assumes only that in $\mathbb{R}$ we have (i) square roots of positive numbers and (ii) roots of odd-degree polynomials. Since in 1815 the definition of $\mathbb{R}$ had yet to be (re)discovered, Gauss was of course unable to prove these but assumed them obvious. You, however, <u>can</u> prove them from Analysis I.

2. Let $Y(x), Y'(x)$ be two polyns. with $\deg Y \geq \deg Y'$; by considering

$$\begin{aligned} Y &= q.Y' + Y'' && \text{with } \deg Y'' < \deg Y' \\ Y' &= q'.Y'' + Y''' && \text{"} \quad \deg Y''' < \deg Y'' \end{aligned}$$

etc. up to
$$Y^{(\mu-1)} = q^{(\mu-1)} Y^{(\mu)}$$

show that (i) $Y^{(\mu)}$ is a divisor of each $Y^{(i)}$, $0 \leq i \leq \mu$; (ii) any common divisor of $Y, Y'$ also divides $Y^{(\mu)}$ which is thus the highest common divisor; (iii) if $\deg Y^{(\mu)} = 0$ then $Y, Y'$ have no common factor; (iv) there are polyns $Z(x), Z'(x)$ st. $Y^{(\mu)} = ZY + Z'Y'$; (v) $Y, Y'$ have no common factor iff there are $Z, Z'$ with $1 = ZY + Z'Y'$.

3. If $(x-a)(x-b)(x-c)\ldots = x^m - \lambda' x^{m-1} + \lambda'' x^{m-2} - \ldots$, explain precisely what $\lambda', \lambda'', \ldots$ are and show that they are symmetric polyns. in $a, b, c, \ldots$, as is any polyn. fn. of them

4. Prove the converse, that if $p(a,b,c,\ldots)$ is a symmetric polyn. in $a,b,c,\ldots$ then there's a polyn. $p(l', l'', \ldots, l^{(m)})$ which becomes $p(a,b,c,\ldots)$ by the substitution $l' = \lambda'(a,b,c,\ldots)$, $l'' = \lambda''(a,b,c,\ldots), \ldots$ ~~Moreover show that this is unique.~~
~~Hence if $p_1(l',l'',l''',\ldots)$ and $p_2(l',l'',l''',\ldots)$ are two polyns.~~
~~s.t. for all $A,B,C,\ldots \in \mathbb{R}$,~~
~~$p_1(\lambda'(A,B,C,\ldots), \lambda''(A,B,C,\ldots),\ldots) = p_2(\lambda'(A,B,C,\ldots),\lambda''(A,B,C),\ldots)$~~
~~then for all $l',l'',l''',\ldots \in \mathbb{R}$ $p_1(l',l'',\ldots) = p_2(l',l'',\ldots)$~~
[<u>Hint</u>: Let a typical term of $p(a,b,c,\ldots)$ be $Ma^\alpha b^\beta c^\gamma\ldots$; arrange the terms in order s.t. if $M'a^{\alpha'}b^{\beta'}c^{\gamma'}\ldots$ is another then

$$\begin{aligned} & \alpha > \alpha' \\ \text{or } & \alpha = \alpha' \ \& \ \beta > \beta' \\ \text{or } & \alpha = \alpha' \ \& \ \beta = \beta' \ \& \ \gamma > \gamma' \\ \text{or } & \ldots \end{aligned}$$

Then if $Ma^\alpha b^\beta c^\gamma\ldots$ is the first term we have $\alpha \geq \beta \geq \gamma \geq \ldots$ and $M\lambda'^{\alpha-\beta}\lambda''^{\beta-\gamma}\lambda'''^{\gamma-\delta}\ldots$ may be subtracted]

5. Show that $p$ is uniquely determined by $\rho$. Hence if $\rho_1, \rho_2$ are symm. polyns. in $a,b,c,\ldots$ s.t. for all $A,B,C,\ldots \in \mathbb{R}$ we have $\rho_1(A,B,C,\ldots) = \rho_2(A,B,C,\ldots)$ then for all $L', L'', \ldots \in \mathbb{R}$ we have $p_1(L', L'', L''', \ldots) = p_2(L', L'', L''', \ldots)$ where $p_1, p_2$ are the corr. polyns. in $l', l'', l''', \ldots$

6. Consider $\pi(a,b,c,\ldots) = \prod_{i \neq j}(a_i - b_j)$, a product of $m(m-1)$ factors; this is a symm. fn. and so corr. to a polyn. $p(l', l'', \ldots)$ called the <u>discriminant</u> [Gauss calls it *determinans*] of the polyn. $y = x^m - l'x^{m-1} + l''x^{m-2} - \ldots$.
Show that for $m=2$ we have

$$p = -l'^2 + 4l''$$

and for $m=3$ $\quad p = -l'^2 l'' + 4l'^3 l''' + 4l''^3 - 18 l'l''l''' + 27 l'''^2$.
For $m=1$, put $p=1$.
For a particular polynomial $Y = x^m - L'x^{m-1} + L''x^{m-2} - \ldots$ with $L', L'', \ldots \in \mathbb{R}$ the discriminant takes a definite value $P$. If $Y$ factorises as $(x-A)(x-B)\ldots$ then $P=0$ iff two of the roots coincide.
Now consider the [formal] derivative

$$Y' = mx^{m-1} - (m-1)L'x^{m-2} + (m-2)L''x^{m-3} - \ldots$$

which, in the case where $Y$ factorises, becomes

$$\begin{aligned} Y' = \; & (x-B)(x-C)\ldots \\ & + (x-A)(x-C)\ldots \\ & + \ldots \end{aligned}$$

Then $Y, Y'$ have a common factor iff $P=0$

7. We have assumed above that $Y$ can be factorised, which is begging the question [*petitio principii*]. Show that in modern terms there is no difficulty by constructing a splitting field for $Y$ over $\mathbb{Q}$. Gauss, of course, suffered from the handicap of *actually believing* that he was dealing with concrete real/complex nos.

8. Put $v = (x-a)(x-b)\ldots$ and

$$\rho = \frac{\pi.(x-b)(x-c)\ldots}{(a-b)^2(a-c)^2\ldots} + \frac{\pi.(x-a)(x-c)\ldots}{(b-a)^2(b-c)^2\ldots} + \ldots$$

Show that $v$ divides $\pi - \rho v'$ and, with $\sigma = (\pi - \rho v')/v$, that $\rho, \sigma$ are symm. in $a,b,c,\ldots$, corr. to polyns. $r, s$ in $[x,]a,b,c,\ldots$ Let $R = r(L', L'', \ldots)$, $S = s(L', L'', \ldots)$; show that $R, S$ are polyns. in $x$ s.t.

$$P = SY + RY'$$

so that, since $P \in \mathbb{R}$, $Y, Y'$ can only have a common factor if $P=0$.

9. Prove the converse. [*Hint*: Let $Y$ be the polyn with $Y = x^m - L'x^{m-1} + L''x^{m-2} - \dots$; let $y = x^m - l'x^{m-1} + \dots$, $v = (x-a)(x-b)\dots$ Choose polyns. $f, \varphi$ st. $f(x)Y(x) + \varphi(x)Y'(x) = 1$ and consider $f(x).v(x,a,b,\dots) + \varphi(x).v'(x,a,b,\dots)$, putting $F(x,l',l'',\dots) = f(x)(y-Y) + \varphi(x).(y'-Y')$. Let $\psi(\lambda',\lambda'',\dots,l',l'',\dots) = [1+F(a,l',l'',\dots)][1+F(b,l',l'',\dots)]\dots$ and show that $\exists\ t(l',l'',\dots)$ st $p(l',l'',\dots)t(l',l'',\dots) = \psi(l',l'',\dots,l',l'',\dots)$. Show that $\psi(L',L'',\dots,L',L'',\dots)$ and deduce $P \neq 0$]

10. Show that any polyn $Y(x)$ can be split into factors none of whose discriminants vanish. During this process polyns. will be each split into two factors: why must one of these necessarily have nonzero discriminant even without further resolution? If $\deg Y = 2^\mu . k$, show that it has a factor with nonzero discriminant and degree $2^\nu . k'$ with $\nu \leq \mu$ ($k, k'$ being odd).

11. §11 of Gauss' paper discusses the meaning of phrases like "product of all $u-(a+b)x+ab$ excluding repetitions". Make an intelligent guess as to what this short paragraph says and improve on it with the benefit of hindsight and later mathematics.

12. Let $\zeta$ be the product of $\frac{1}{2}m(m-1)$ factors of the form $u-(a+b)x+ab$, and let $z, Z$ be the corr. polyns. in $u, x, l', l'', \dots$ and just $u, x$ resp. Consider these as polyns. in $u$ whose coeffs depend on $x, l', l'', \dots$ and $x$ resp. Then if $P \neq 0$, $Z$ does not vanish identically in $u, x$.

13. Prove this claim under the assumption that $Y = (x-A)(x-B)\dots$

14. What are the degrees of the discriminants of $\zeta, z, Z$ considered as polyns in $x$? Show that these discriminants are respectively $\pi^{m-2}, v^{(m-1)(m-2)}.\rho$, $p^{m-2}.y^{(m-1)(m-2)}.r$ and $P^{m-2}Y^{(m-1)(m-2)}R$ where $\rho = \rho(x,a,b,\dots)$, $r = r(x,l',l'',\dots)$ and $R = R(x)$ are polyns. to be determined. Thus we require $P \neq 0 \Rightarrow R$ is not identically zero.

15 Let $f(w,\lambda',\lambda'',\dots)$ be the product of all $(a+b-c-d)w + (a-c)(a-d)$ excluding repetitions. Determine $f(0,L',L'',\dots)$ and hence show that if $P \neq 0$ then $f(w,L',L'',\dots)$ does not vanish identically. Putting $Nx^\nu$ for the highest nonvanishing term of $f(x-a,L',L'',\dots)$ as a polyn. in $x$, find the degree of the product $f(x-a,L',L'',\dots)f(x-b,L',L'',\dots)\dots$ Let $\varphi(x,\lambda',\lambda'',\dots,l',l'',\dots) = f(x-a,l',l'',\dots)f(x-b,l',l'',\dots)\dots$ and show that $\rho$ divides the product of all $f(x-a,\lambda',\lambda'',\dots)$. Hence prove the claim of §12.

16. Let $\varphi(u,x)$ be a product of factors of the form $\alpha+\beta u+\gamma x$ for some $\alpha, \beta, \gamma, \alpha', \beta', \gamma', \ldots \in \mathbb{R}$. Denote by $\varphi_x$ and $\varphi_u$ the [formal] derivatives of $\varphi$ wrt $x, u$, resp. Show that $\varphi(u,x)$ divides $\Omega(u,x,w) = \varphi(u+w.\varphi_x(u,x), x-w.\varphi_u(u,x))$.

17. Applying §16 to $\zeta$, let the quotient be $\psi(u,x,w,\lambda',\lambda'',\ldots)$. Show that $Z(u+w.\,Z_x(u,x), x-w.\,Z_u(u,x)) = Z(u,x).\psi(u,x,w,L',L'',\ldots)$.

18 Let $U, X \in \mathbb{R}$ and put $X' = Z_x(U,X)$, $U' = Z_u(U,X)$. Then if $U' \neq 0$, put $w = (X-x)/U'$. Show that

$$Z(U + XX'/U' - X'x/U', x) = Z(U,X).\psi(U,X,(X-x)/U,L',L'',\ldots)$$

19. Now suppose $P \neq 0$. Show that $\exists X \in \mathbb{R}$ st. the discriminant of $Z(u,X)$ is nonzero. Hence $Z(u,X)$ and $Z_u(u,X)$ have no common factor. Now suppose we have $U \in \mathbb{I}$ st. $Z(U,X)=0$, so $(u-U)$ divides $Z(u,X)$ but not $Z_u(u,X)$. Let $U' = Z_u(U,X)$, $X' = Z_x(U,X)$. Show that $Z(U+XX'/U'-X'x/U', x)=0$ identically so that $u+(X'/U')x - (U+XX'/U')$ is a factor of $Z(u,x)$. Hence if $x$ is a sol$^n$ of $x^2+(X'/U')x - (U+XX'/U') = 0$ then $Z(x^2,x)=0$. Show that then also $Y(x)=0$ since $\zeta(x^2,x,\lambda',\lambda'',\ldots)$ is the product of all $(x-a)(x-b)$ excluding repetitions and is hence equal to $U^{m-1}$ so that $Z(x^2,x) = Y^{m-1}$.

20. Let $Y = x^m - L'x^{m-1} + L''x^{m-2} - \ldots$ be any polyn. of degree $m = 2^\mu.k$ (with $k$ odd) with real coeff.s Show that there is a polyn. of degree $2^\nu.k'$ (with $\nu<\mu$ and $k'$ odd) with real coeffs. any root of which is also a root of $Y$. ~~Hence and whose discriminant is~~ Hence show that, since $\mathbb{R}$ has square roots and roots of odd degree polyns, $Y$ may be resolved into real factors of degree 1 or 2, ie that $\mathbb{C}$ is algebraically closed.

*21. [Modern proof] Let $K$ be any field (not nec. char. 0) which has roots of all quadratic & odd-degree polyns. Let $Y$ be an [irred] polyn. and $L:K$ its splitting field; show that this is finite normal & separable, with Galois group $G$ of order $2^\mu.k$. Let $H \leq G$ with $|H| = 2^\mu$ by Sylow's thm: show that $H=G$, so $k=1$. Let $J \trianglelefteq H$ with $|J| = 2^{\mu-1}$ (if $\mu \neq 0$) and derive a contradiction. Hence $K$ is algebraically closed.

...***22. Find the relationship between the two proofs