Homework problems given by Prof. J. Tate in a course on Algebra 250(a) at Harvard in the Fall of 1985.

October 22, 1985

(1) Suppose $f(X)$ is irreducible and G_f is abelian. Prove that the order of G_f is the degree of f.

(2) Suppose K/F is a finite Galois extension. Let $G = \mathrm{Gal}(K/F)$.

(a) Suppose G acts transitively on a set I. Show that there exists a family $(\alpha_i)_{i\in I}$ of elements of K such that $\sigma(\alpha_i) = \alpha_{\sigma i}$ for all $\sigma \in G$.

(b) Let n be an integer ≥ 0 and suppose $h : G \hookrightarrow \mathcal{S}_n$ is an injective group homomorphism. Show that if F has at least n elements, then there is a polynomial $f(X) \in F[X]$ with distinct roots such that K is a splitting field for f over F and such that $G_f = h(G) \subset \mathcal{S}_n$.

(3) Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be "variables" and

$$f(X) = \prod_{i=1}^{n}(X - \alpha_i) = X^n - a_1 X^{n-1} + \dots$$

Put :

$$\beta = \sum_{\pi\in\mathcal{A}_n} \alpha_{\pi(2)}\alpha^2_{\pi(3)}\dots\alpha^{n-1}_{\pi(n)}, \text{ and } \gamma = \sum_{\pi\in\mathcal{S}_n\setminus\mathcal{A}_n} \alpha_{\pi(2)}\alpha^2_{\pi(3)}\dots\alpha^{n-1}_{\pi(n)}.$$

(a) Show that $(\beta - \gamma)^2 = d_f$ (the discriminant of f).

(b) Let $b = \beta + \gamma$ and $c = \beta\gamma$. How do you know b and c are in $\mathbb{Z}[a_1, a_2, \dots]$.

(c) For $n = 2$ and 3, give b and c explicitly as elements of $\mathbb{Z}[a_1, a_2]$, and of $\mathbb{Z}[a_1, a_2, a_3]$ (Recall : $f(X) = X^n - a_1X^{n-1} + a_2X^{n-2} - \dots$).

(d) Now drop the assumption that the α_i are "variables". Let F be a field, $a_i \in F$, $1 \leq i \leq n$, and suppose $d_f \neq 0$. Let K be a splitting field for f over F, i.e., $K = F(\alpha_1, \dots, \alpha_n)$ and $G = \mathrm{Gal}(K/F)$. Show that the fixed field of $G_f \cap \mathcal{A}_n$ is the splitting field of the quadratic polynomial $X^2 - bX + c$, regardless of the characteristic.

(e) Let $F = \mathbb{F}_2(t)$, t transcendental. Find G_f in the following cases :

(i) $f(X) = X^3 + tX + 1$;

(ii) $f(X) = X^3 + t^3X + t^2$;

(iii) $f(X) = X^3 + t^2X + (t + 1)$;

(f) Show that if the $a_i \in \mathbb{Z}$, then $d_f \equiv 0$ or $1 \pmod 4$ (just express d_f in terms of b and c).

(4) Let

$$f(X) = X^4 - a_1X^3 + a_2X^2 - a_3X + a_4 = \prod_{i=1}^{4}(X - \alpha_i)$$

with $a_i \in F$, F a field, $\alpha_i \in K = F(\alpha_1, \ldots, \alpha_4)$, the splitting field. Put

$$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3,$$

and let :

$$\begin{aligned} g(X) &= (X - \beta_1)(X - \beta_2)(X - \beta_3) \\ &= X^3 - a_2X^2 + (a_1a_3 - 4a_4)X + (a_1^2a_4 + a_3^2 - 4a_2a_4) \end{aligned}$$

be the "cubic resolvent" of f. Prove that $d_f = d_g$ (discriminants). Suppose $d_f \neq 0$, and char$F \neq 2$ when necessary. Assume also that $f(X)$ *has no root in* F.

(a) Show that f has a quadratic factor in $F[X]$ if and only if, for some i,

$$\beta_i \in F \text{ and both } a_1^2 - 4a_2 + 4\beta_i \text{ and } \beta_i^2 - 4a_4 \text{ are squares in } F.$$

(b) $G_f = \mathcal{S}_4 \iff g$ has no root in F and d_f not a square in F; $G_f = \mathcal{A}_4 \iff g$ has no root in F and d_f is a square in F.

Suppose from now on, that f *is irreducible in* $F[X]$ *and* g *has a root, say* β_1*, in* F.

(c) Show that G_f is a group of order a power of 2, so is contained in a 2-Sylow subgroup of $\mathcal{S}_4$.

(d) Show $G_f = V \overset{\text{defn}}{=} \{(1), (12)(34), (13)(24), (14)(23)\}$ if and only if g has three roots in f, if and only if d_f is a square in F.

(e) Suppose G_f has exactly one root in F. Show that G_f is cyclic of order 4, or is dihedral of order 8, and give a criterion to decide which.

(f) Find G_f's for the following five quartic f's :

(i) $x^4 + x^3 + x^2 + x + 1$;
(ii) $x^4 + x + 1$;
(iii) $x^4 + 2$;
(iv) $x^4 + 8x + 12$;
(v) $x^4 - 2x^2 + 9$.

October 29, 1985

(1) Let $f(X) \in \mathbb{Z}[X]$ be an irreducible quintic. We have seen in class that its group, G_f, has order $120, 60, 20, 10$ or 5, being isomorphic to $\mathcal{S}_5$, $\mathcal{A}_5$, or to the group of permutations of $\mathbb{F}_5$ of the form $x \mapsto ax + b$ for $b \in \mathbb{F}_5$ and for $a \in \mathbb{F}_5^\times$, or $a = \pm 1$, or $a = 1$. For $i = 0, 1, 2, 3, 5$, let $\mathcal{P}_i$ denote the set of prime numbers p such that the congruence $f(X) \equiv 0 \bmod p$ has exactly i incongruent solutions mod p. Assuming the Tschebotaroff density theorem, make a table giving, for each of the five possible G_f's, the density of $\mathcal{P}_i$ in that case. For example, the density of $\mathcal{P}_5$ is $\frac{1}{120}, \frac{1}{60}, \frac{1}{20}, \frac{1}{10}$ or $\frac{1}{5}$, i.e., is $|G_f|^{-1}$ in each case.

(2) Consider the polynomials $A(X) = X^5 - X^3 - 2X^2 - 2X - 1$, $B(X) = X^5 - X + 3$, $C(X) = X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$, $D(X) = X^5 - 5$, $E(X) = X^5 + 10X^3 - 10X^2 + 35X - 18$. Each of these five is irreducible. Their discriminants are : $d_A = 47^2$, $d_B = 252869$ (prime), $d_C = 11^4, d_D = 5^9$, $d_E = 2^6 5^8 11^{12}$. The following is a table, produced in about 25 hours of running time by my Macintosh, giving for each polynomial the number of primes in $\mathcal{P}_i$ (cf. Problem 1) among the first 360 primes. (Thus, the sum of each row is 360).

	0 roots	1 root	2 roots	3 roots	5 roots
A	147	180	0	$1 \leftarrow p = 47$	32
B	143	131	58	27	1
C	288	1 $(p = 11)$	0	0	71
D	78	272	0	0	0
E	142	88	128	0	2

The primes among the first 360 which are in $\mathcal{P}_5$, i.e., for which $f(X)$ splits in $\mathbb{F}_p$ are in each case as follows :

$A : p = 83, 191, 197, 269, 439, 487, 523, 619, 761, 823, 907, 947,$
$977, 1193, 1277, 1319, 1447, 1481, 1499, 1579, 1693, 1709, 1741,$
$1811, 1861, 1867, 2053, 2213, 2221, 2273, 2339, 2351.$
$B :$ just $p = 1609$.
$C :$ all primes $p \equiv \pm 1 (\bmod 11)$, i.e., $p = 23, 43, 67, 89, \ldots,$
$2287, 2309, 2311, 2333, 2377, 2399.$
$D : p = 31, 191, 251, 271, 601, 641, 761, 1091, 1861, 2381.$
$E :$ just $p = 2063$ and 2213.

Armed with all this information (you don't really need much of it), and using the simple form of $D(X)$, determine the groups G_B, G_E and G_D. What are the only possibilities for G_A and G_C? Which of these possibilities do you guess is the correct one?

(3) Guess what the splitting field of G_C is. Try to prove your guess by guessing the element α in that field whose minimal polynomial is $C(X)$.

(4) To prove your guess for G_A is not so easy without a clue. To show it by brute force, let α be a root of $A(X)$ and check that in $\mathbb{Z}[\alpha][X]$, we have :

$$A(X) = (X - \alpha)(X^2 - c_1 X + c_2)(X^2 - d_1 X + d_2),$$

where

$$c_1 = 2\alpha^4 - \alpha^3 - 2\alpha^2 - 3\alpha - 2, d_1 = -2\alpha^4 + \alpha^3 + 2\alpha^2 + 2\alpha + 2,$$
$$c_2 = -\alpha^4 + \alpha^3 + \alpha^2 + \alpha, d_2 = -\alpha^4 + \alpha^3 + 2\alpha + 1.$$

Please don't hand in your verification of this. But answer the following : What is the quadratic field contained in the splitting field of $A(X)$?

November 5, 1985

(1) Let $F \subset K$ be finite fields. Prove that $N_{K/F} : K^\times \to F^\times$ is surjective.

(2) Let F be the fraction field of an integral domain A. Prove that A is integrally closed (in F) $\iff$ A has the following property : if $f(X)$ and $g(X) \in F[X]$ are monic and $f(X) \cdot g(X) \in A[X]$, then $f(X)$ and $g(X) \in A[X]$.

(3) Let $F = \mathbb{Q}(i)$ and $K = F(2^{\frac{1}{4}}, i^{\frac{1}{4}})$, where $2^{\frac{1}{4}}$ is the positive fourth root of 2 and $i^{\frac{1}{4}} = e^{\frac{2\pi i}{16}}$. Determine $\mathrm{Gal}(K/F)$. Is $K/\mathbb{Q}$ Galois, and if so, what is its Galois group?

(4) (a) A ring of the form $\mathbb{Z}[\alpha]$ has at most two homomorphisms into $\mathbb{F}_2$. Why?

(b) Let A be the integral closure of $\mathbb{Z}$ in the field $\mathbb{Q}(\sqrt{-7}, \sqrt{17})$. Find a $\mathbb{Z}$-base for A (cf. class discussion on October 31).

(c) Show that A has four distinct homomorphisms into $\mathbb{F}_2$ (and consequently there does not exist $\alpha \in A$ such that $A = \mathbb{Z}[\alpha]$).

(5) Find three integers a, b, c such that $\mathbb{Q}(e^{\frac{2\pi i}{4}}) = \mathbb{Q}(\sqrt{a}, \sqrt{b}, \sqrt{c})$.

(6) (a) Prove that $\mathbb{R}$ has no non-trivial automorphism (hint : show that an automorphism of $\mathbb{R}$ is order-preserving automatically).

(b) Show that the only automorphisms of $\mathbb{C}$ which commute with complex conjugation are the identity and complex conjugation.

(7) Let $\alpha = (2+\sqrt{2})(3+\sqrt{3}) = -\sqrt{6}(1+\sqrt{2})(1+\sqrt{3})$ and let $\theta = \sqrt{-\alpha} = i\sqrt{\alpha}$. Show $\mathbb{Q}(\theta)/\mathbb{Q}$ is Galois of degree 8. Determine the structure of $G = \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$, and explain why $\mathbb{Q}(\theta)$ is not the splitting field of any polynomial of degree < 8.

(8) Suppose $[F : \mathbb{Q}]$ is odd. Prove that -1 is not a sum of squares of elements of F.

(9) Suppose F is a field of characteristic $p > 0$. The map $x \mapsto x^p - x$ is a homomorphism of the additive group of F into itself with kernel $\mathbb{F}_p$. Suppose $a \in F$ is not in the image, i.e., suppose the polynomial $f(X) = X^p - X - a$ has no root in F. Show that the splitting field of $f(X)$ is cyclic of degree p over F.

November 12, 1985

(1) Let e be an idempotent ($e^2 = e$) in a local ring A (a ring with a unique maximal ideal). Show that $e = 0$ or 1.

(2) Suppose A is integrally closed in its fraction field F. Prove that the same is true for $A[X]$ (polynomial ring). (Suggestion : $F[X]$ *is* integrally closed, being a PID).

(3) (a) Show that an order B in a quadratic extension of $\mathbb{Q}$ is of the form $B = \mathbb{Z}[\alpha] = \mathbb{Z}+\mathbb{Z}\alpha$, where α is a root of an irreducible monic quadratic polynomial $f(X) = X^2 + rX + s \in \mathbb{Z}[X]$.

(b) For each such polynomial f, let $d_f = r^2 - 4s$ and $B_f = \mathbb{Z}[\alpha] = \mathbb{Z}[\alpha, \beta]$ where α and β are the complex (or real) roots of f. Let g be another irreducible monic quadratic polynomial in $\mathbb{Z}[X]$. Show

$$B_g \subset B_f \iff d_f \boxbar d_g,$$

where $a \boxbar b$ means by definition that $b = m^2 a$, for some $m \in \mathbb{Z}$, and when that is the case, show that the additive group B_f/B_g is *cyclic* of order m, where $d_g = m^2 d_f$.

(c) Thus, $B_g = B_f \iff d_f = d_g$. Show that the integers d which occur as discriminants of quadaratic orders, i.e., the integers d of the form d_f for some f as above, are those $d \equiv 0$ or 1 (mod 4) such that d is not a perfect square.

(d) Show that B_f is integrally closed if and only if

$$d \boxbar d_f, d \equiv 0 \text{ or } 1 \bmod 4 \Rightarrow d = d_f,$$

and then the other orders in $\mathbb{Q}(B_f)$ are the B_g's such that $d_f \boxbar d_g$.

(e) Suppose f and g are as in (d), say $d_g = m^2 d_f$. Show for each prime number p such that $p \mid d_g$ that there is a unique prime ideal P of B_g such that $p \in P$, and that $B_g = P + \mathbb{Z}$, i.e., $B_g/P \cong \mathbb{F}_p$. Show $P^2 = pB_g$ if $p \nmid m$, $P^2 = pP$ if $p \mid m$.

November 19, 1985

(1) Let k be a field, $\mathbb{M}_2(k)$ the ring of 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $a, b, c, d \in k$, and let A be the subring of all such matrices with $c = 0$. The maps $\varphi_1 : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto a$ and $\varphi_2 : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto d$ are homomorphisms of A onto k. Let $P_j = \operatorname{Ker} \varphi_j$ for $j = 1, 2$. Since $\dim_k A = 3 < \infty$, A is of finite length as a left A-module.

(a) Show that A/P_1 and A/P_2 are the only simple A-modules (up to isomorphism).
(b) Compute $P_1^2, P_1P_2, P_2P_1, P_2^2$ and $P_1 \cap P_2$. Are these the only two sided ideals of A (besides (0) and A)? What are the left ideals?
(c) What are the multiplicities of A/P_1 and A/P_2 in the left A-module A?
(d) Show that A is not isomorphic to the direct product of two non-zero rings.

(2) Consider the cubic polynomials :

$f_1(X) = X^3 + X^2 + 7X - 8$, $\equiv (X-6)(X+5)(X+2) \pmod{13}$ and is irreducible mod 17, 19 and 29	$f_2(X) = X^3 - 8X + 15$ $\equiv (X+4)(X+6)(X+7) \pmod{17}$ irred. mod 13, 29, 29
$f_3(X) = X^3 + X^2 - 7X + 12$ $\equiv (X-8)(X+8)(X+1) \pmod{19}$ irred. mod 13, 17, 29	$f_4(X) = X^3 + 10X + 1$ $\equiv (X-2)(X-3)(X-5) \pmod{29}$ irred. mod 13, 17, 19

Each of the four polynomials has discriminant -4027, a prime. Nevertheless, the fields $\mathbb{Q}(\alpha_i)$, α_i a root of $f_i(X)$, are pairwise non-isomorphic. Why?

(3) Suppose $f(X)$ is a monic cubic with coefficients in a finite field k, and suppose the discriminant of f is not a square in k. Prove that $f(X)$ is the product of a linear polynomial and an irreducible quadratic polynomial in $k[X]$. Now explain why we didn't give congruences mod $p = 2, 3, 5, 7, 11$ and 23 in problem 2 (there is an arrow to the 'Why?' question of problem 2).

(4) Let k be a field ($\mathbb{C}$ or $\mathbb{R}$ if you wish) and let $f(X, Y)$ be an irreducible polynomial in two variables over k, i.e., a prime element in the U. F. D. $k[X, Y]$. Let $A = k[X, Y]/(f)$. Then A is Noetherian (Tate writes 'noetherian'), and the nonzero prime ideals of A are maximal. Can you show this? Anyway, taking that for granted, let $(x_0, y_0) \in k \times k$ be a point on the curve $f(X, Y) = 0$, i.e., be such that $f(x_0, y_0) = 0$, and let P be the corresponding maximal ideal of A, consisting of the polynomials $p(X, Y)$ such that $p(x_0, y_0) = 0$, modulo (f). Prove that P is an invertible ideal in A if and only if the point (x_0, y_0) is a "non-singular" point of the curve, in the sense that *not* both partial derivatives $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ vanish at (x_0, y_0). (Suggestion : Note that the translation $(X, Y) \mapsto (X - x_0, Y - y_0)$, which

is an automorphism of $k[X,Y]$, allows you to assume $(x_0, y_0) = (0,0)$ without loss of generality).

(5) Let a and b be positive integers such that ab is square free > 1, and let $E = \mathbb{Q}(\sqrt[3]{ab^2})$. Let $\alpha = \sqrt[3]{ab^2}$, and $\beta = \sqrt[3]{a^2b} = ab/\alpha$. Show that if $a^2 \not\equiv b^2 \pmod 9$, then the integral closure of $\mathbb{Z}$ in E is $\mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta$, and the discriminant of the field E is $-27a^2b^2$. What if $a^2 \equiv b^2 (\mathrm{mod}\ 9)$?

$\boxed{X^7 - 7X + 3}$

(I) Suppose $f(X) \in \mathbb{Z}[X]$ is monic irreducible of degree 7, has a square discriminant, and has exactly three real roots. Prove that G_f is isomorphic either to $\mathcal{A}_7$ or to the group $G_{168} = \mathrm{GL}(3, \mathbb{F}_2) \approx \mathrm{PSL}(2, \mathbb{F}_7)$. Note that G_{168} is isomorphic to a subgroup of $\mathcal{S}_7$, in fact of $\mathcal{A}_7$, via the action of $G_{168} = \mathrm{GL}_3(\mathbb{F}_2)$ on the 7 non-zero vectors in $\mathbb{F}_2^3$.
(By considering Sylow subgroups, especially the ones for 7, this can be done from scratch without too much trouble. But it is even easier if you know that the only non-abelian simple groups of order < 1000 are $\mathcal{A}_5$ of order $60 = 2^2 \cdot 3 \cdot 5$, G_{168} of order $168 = 2^3 \cdot 3 \cdot 7$, $\mathcal{A}_6$ of order $360 = 2^3 \cdot 3^2 \cdot 5$, $\mathrm{PSL}(2, \mathbb{F}_8)$ of order $504 = 2^3 \cdot 3^2 \cdot 7$, $\mathrm{PSL}(2, \mathbb{F}_{11})$ of order $660 = 2^2 \cdot 3 \cdot 5 \cdot 11$).

(II) Let $f(X) = X^7 - 7X + 3$ (shown me by Mr. Elkies). It is easy to check that $f(X)$ satisfies the conditions of (I). For example, $d_f = 3^8 \cdot 7^8$. Moreover, out of the first 360 primes :

$$p = 2, 3, 5, 7, \ldots, 2423 \ :$$

- $f(X)$ has no root (mod p) for 104 p's;
- $f(X)$ has 1 root (mod p) for 214 p's;
- $f(X)$ has 3 roots (mod p) for 41 p's;
- $f(X)$ has 7 roots (mod p) for 1 p (namely $p = 1879$);

Is $G_f = G_{168}$, or $\mathcal{A}_7$?

Newton Formulas, Discriminant

$$f(X) = X^n - a_1X^{n-1} + a_2X^{n-2} - \dots + (-1)^n a_n = (X-\alpha_1)(X-\alpha_2)\dots(X-\alpha_n).$$

Here $a_\nu = \sum_{i_1<i_2<\dots<i_\nu} \alpha_{i_1}\alpha_{i_2}\dots\alpha_{i_\nu}$. Put $S_\nu = \sum_i \alpha_i^\nu$.
Then :

$S_1 - a_1 = 0.$
$S_2 - a_1S_1 + 2a_2 = 0.$
$S_3 - a_1S_2 + a_2S_1 - 3a_3 = 0.$
$\dots$
$S_n - a_1S_{n-1} + \dots \pm a_nS_0 = 0.$
$\dots$
$S_m - a_1S_{m-1} + \dots \pm a_nS_{m-n} = 0, m \geq n.$

Proof. Write :

$$\prod_{i=1}^{n}(1-\alpha_i t) = 1 - a_1t + a_2t^2 - \dots = \sum_{\nu\geq 0}(-1)^\nu a_\nu t^\nu.$$

Take the logarithmic derivative formally :

$$\sum_i \frac{-\alpha_i}{1-\alpha_i t} = -\sum_{i,\nu}\alpha_i^{\nu+1}t^\nu = -\sum_\nu S_{\nu+1}t^\nu = \frac{-a_1 + 2a_2t - 3a_3t^2 + \dots}{1 - a_1t + a_2t^2 - a_3t^3 + \dots},$$

cross-multiply and compare coefficients of t^ν. □

Solving for S_n we get for $n \leq 4$:

$$S_4 = a_1^4 - 4a_1^2a_2 + 2a_2^2 + 4a_1a_3 - 4a_4.$$
$$S_3 = a_1^3 - 3a_1a_2 + 3a_3.$$
$$S_2 = a_1^2 - 2a_2.$$
$$S_1 = a_1.$$
$$S_0 = n.$$

Further, the discriminant d_f of $f(X)$ is

$$= d_f = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i\neq j}(\alpha_i - \alpha_j) = (-1)^{\frac{n(n-1)}{2}} \prod_j f'(\alpha_j)$$

$$= \det{}^2 \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1}. \end{bmatrix}$$

$$= \det \left(\begin{bmatrix} 1 & 1 & 1 & \dots & \alpha_1^{n-1} \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \dots & \alpha_n^2 \\ \dots & \dots & \dots & \dots & \dots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \alpha_3^{n-1} & \dots & \alpha_n^{n-1}. \end{bmatrix} \cdot \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \dots & \alpha_3^{n-1} \\ \vdots & \vdots & & & \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1}. \end{bmatrix} \right)$$

$$= \det \begin{bmatrix} S_0 & S_1 & S_2 & \dots & S_{n-1} \\ S_1 & S_2 & S_3 & \dots & S_n \\ \vdots & \vdots & \vdots & & \vdots \\ S_{n-1} & S_n & S_{n+1} & \dots & S_{2n-2}. \end{bmatrix}.$$

This last can also be written :

$$d_f = (-1)^{\frac{n(n-1)}{2}} R(f, f'),$$

where R is the *resultant*; cf. Lang page 211 (Ch V, §10).

Example : For $f(X) = X^n + pX + q$, we have $(-1)^{\frac{n(n-1)}{2}} d_f = n^n q^{n-1} + (1-n)^{n-1} p^n$, as can be seen by writing $-\alpha_j f'(\alpha_j) = nq - (1-n)p\alpha_j$ and multiplying over j.

Examples of prime ideals

(1) Let A be a u.f.d. (unique factorization domain, e.g., $A = \mathbb{Z}[x_1, \ldots, x_n]$ or $A = K[x_1, \ldots, x_n]$, K a field) and let π be a prime element in A. Show :
  (a) The principal ideal πA is a prime ideal.
  (b) Every nonzero prime ideal contains one of the form πA.
  (c) The ideals of the form πA are the minimal elements in the set of nonzero prime ideals, ordered by inclusion, and they are the only nonzero principal prime ideals.

(2) Let A be a p.i.d. (principal ideal domain, e.g., $A = \mathbb{Z}$ or $A = K[X]$, K a field). Then the ideals of the form πA are maximal, and are the only non-zero prime ideals of A.

(3) Let B be an integral domain with field of fractions K. Let $A = B[X]$ and let P be a prime ideal of A; then $P \cap B$ is a prime ideal in B.

$$\begin{array}{ccc} A = B[X] & \hookrightarrow & K[X] \\ \uparrow & & \uparrow \\ B & \hookrightarrow & K \end{array}$$

  (a) If $P \cap B = (0)$, show :
    (i) $PK = P(K[X])$ is a prime ideal in $AK = K[X]$.
    (ii) $P = PK \cap A$.
    (iii) If B is a u.f.d., then either $P = (0)$, or $P = f(X)A$, where $f(X)$ is a polynomial with coefficients in B, these coefficients having "no" common divisor (i.e., none except units in B), and $f(X)$ being irreducible in $K[X]$. Moreover f is determined by P up to a unit (invertible element) of B.
  (b) If $P \cap B = M$, a maximal ideal of B, then, making the identification $A/MA = B[X]/MB[X] \approx (B/M)[X] = k[X]$, where $k = B/M$, we see that P/MA is a prime ideal in $k[X]$. Hence show : either $P = MA$, or $P = MA + g(x)A$, where $g(X)$ is a polynomial with coefficients in B such that the polynomial $\overline{g}(X)$ which we obtain by reducing the coefficients of g (mod M) is an irreducible polynomial in $k[X]$. Moreover g is determined by P up to multiplication by an element of B not in M and addition of a polynomial whose coefficients are in M.

(4) Apply (3) to the case where B is a p.i.d., and show that the prime ideals P of A are of the following distinct types :
  (I) $P = (0)$.
  (II) $P = f(X)A$, where f is as in 3.a.iii.
  (III) $P = \pi A$, π a prime element of B.
  (IV) $P = \pi^* A + g(X)$, π^* a prime element of B, and g as in 3b, with $M = \pi B$.

The ideals of type IV are maximal and are not principal. The ideals of type IV which contain a given πA of type III are those for which $\pi^* \sim \pi$, i.e., $\pi^* B = \pi B$.

The ideals of type IV which contain a given $f(X)A$ of type II are those for which $\overline{g}(X)$ divides $\overline{f}(X)$ in $k[X]$, where $k = B/\pi^* B$ and where $\overline{g}$ and $\overline{f}$ denote the polynomials obtained from g and f by reducing their coeffients (mod π^*); hence no ideal of type II is maximal *unless* B has only a finite number of maximal ideals, say $\pi_1 B, \pi_2 B, \ldots, \pi_m B$, in which case, the ideals of type II generated by $f(X)$ of the form $f(X) = 1 + \pi_1 \pi_2 \ldots \pi_m X h(X)$, with $h(X) \in B(X)$ *are* maximal (because for every π_i we have $\bar{f} = f(\text{mod } \pi_i) - 1$!

(5) If $\mathbb{C}$ is the field of complex numbers (or any algebraically closed field), apply (4) to $B = \mathbb{C}[Y]$ to show that the prime ideals P in the ring $A = \mathbb{C}[X, Y]$ are of three distinct types :

(I) $P = (0)$.

(II) and (III) $P = f(X, Y)A$ where $f(X, Y)$ is an irreducible polynomial in two variables with complex coefficients, uniquely determined by P up to a nonzero constant factor.

(IV) $P = (X - x_0)A + (Y - y_0)A$, where x_0 and y_0 are complex numbers uniquely determined by P.

The only maximal ideals are those of type IV, and the ideals of type IV containing a given $f(X, Y)A$ are those for which $f(x_0, y_0) = 0$.

(6) Let $A = \mathbb{C}[X, Y, Z]$. What are the minimal non-zero prime ideals of A? Try to prove that the only maximal ideals of A are those of the form $(X - x_0, Y - y_0, Z - z_0)$ (special case of Hilbert's Nullstellensatz). The prime ideals of A which are neither maximal nor minimal nonzero are harder to describe. One such is $P = (X, Y)$. But not all of them can be generated by two elements. For example, let $\varphi : A \to \mathbb{C}[T]$ be the homomorphism defined by $\varphi(f(X, Y, Z)) = f(T^3, T^4, T^5)$, and let P be the kernel of φ. Try to show that P is generated by the three elements $Y^2 - XZ, X^3 - YZ, Z^2 - X^2 Y$, but on the other hand, P cannot be generated by two elements.

(7) Let M be a maximal ideal in a ring B and let $A = B/M^n$ for some integer $n > 0$. Show that the only prime ideal of A is M/M^n.
Examples: $A = \mathbb{Z}/1024\mathbb{Z}$, $A = \mathbb{C}[X]/X^n\mathbb{C}[X]$.

(8) Let A be the ring of power series $c_0 + c_1 z + c_2 z^2 + \ldots$ with complex coefficients c_i which have a nonzero radius of convergence (ring of germs of analytic functions at the origin $z = 0$ in the complex z-plane). Discuss the prime ideals in A. Do the same for the ring of formal power series $A = K[[z]]$ in one variable z over any field.

(9) Let E be a compact Hausdorff topological space. Let A be the ring of all continuous real valued functions on E. For each $x \in E$, let $M(x)$ be the maximal ideal of A consisting of the functions $f \in A$ such that $f(x) = 0$ (i.e., $M(x) =$ Kernel of the homomorphism $f \rightsquigarrow f(x)$). Prove that the map $x \rightsquigarrow M(x)$ is a *homeomorphism* of E *onto* the maximal ideal spectrum of A. (You may use the well-known lemma which states that, given two disjoint closed subsets of E (in particular two distinct points of E), there exists a continuous real valued function on E taking the value 0 on one of the sets and the value 1 on the other - if you

don't like too much abstraction, take E to be the closed interval $[0, 1]$ on the real line.) (Hint : the only hard part is to show that every maximal ideal $\mathcal{M}$ of A is of the form $M(x)$ for some $x \in E$. To do this, suppose the contrary. Then for every $x \in E$ there exists a function $f_x \in \mathcal{M}$, but with $f_x(x) \neq 0$. Show that if you replace f_x by $g_x f_x$ with a suitable g_x, you can assume $f_x \in \mathcal{M}$, and $f_x(y) = 1$ for all y in some neighborhood U_x of x. Now these U_x cover E, so already a finite number $U_{x_1}, U_{x_2}, \ldots, U_{x_n}$ cover E etc.).