2ND FRENCH-GERMAN SUMMER SCHOOL
GALOIS THEORY AND NUMBER THEORY
–
PROBLEMS

Problem 1 — Show that every finite abelian group G is the Galois group of some field extension of $\mathbb{Q}$.

Comments: Consider first the special case that G is cyclic: use cyclotomic extensions and the lemma that for each integer $m \neq 0$, there are infinitely many integers that are congruent to 1 modulo m.
(see [Dèb09, §2.1.2]).

Problem 2 — (Hensel's lemma)

a) Show that $X^2 + 1$ has a root in $\mathbb{Z}_5 = \varprojlim_n \mathbb{Z}/5^n\mathbb{Z}$.
b) Let (A, v) be a complete discrete valuation ring with residue field κ. Let $f \in A[X]$ be a polynomial such that the polynomial $\overline{f} \in \kappa[X]$ obtained by reducing the coefficients of f modulo the valuation ideal has a simple root $\lambda \in \kappa$. Show that f has a root $x \in A$.

Comments: see [Dèb09, §1.2.2.7].

Problem 3 — (Krasner's lemma) Let (k, v) be a complete field for a discrete valuation v, of characteristic 0. Let $P, Q \in k[Y]$ be two monic polynomials with the same degree $d \geq 1$. Assume that P is irreducible. Denote the roots of P (resp. of Q) counted with multiplicities by $(a_1, \dots, a_d)$ (resp. by $(b_1, \dots, b_d)$).
Set $D = \prod_{i=1}^d Q(a_i) = \prod_{i,j}(a_i - b_j)$ and $\rho = \min_{i \neq j} |a_i - a_j|$.

a) show that if $|D| < \rho^{d^2}$, then there exist $i, j \in \{1, \dots, d\}$ such that $|a_i - b_j| < \rho$. Deduce that $|a_i - b_j| < |a_k - b_j|$ for every $k \neq i$, and then that $a_i \in k(b_j)$.
b) Show that if P and Q are sufficiently close (coefficient by coefficient, for the valuation v), then Q is irreducible and has a root in the fields $k(a_i)$ $(i = 1, \dots, d)$.
c) Show that if in addition, $k(a_1)/k$ is Galois, then $k(a_1) = k(b_1)$.

Problem 4 — Let G be a finite group and H be a subgroup of G. Denote by U the union of all conjugate subgroups gHg^{-1} of H by elements $g \in G$.

a) Show that if $\{g_1, \dots, g_n\}$ are representatives of the left cosets of G modulo H, then $U \setminus \{1\} = \bigcup_{i=1}^n \left(g_i H g_i^{-1} \setminus \{1\}\right)$.
b) Deduce that $\mathrm{card}(U) \leq |G| - [G : H] + 1$
c) (*Jordan's lemma*) Let H be a subgroup of G that contains at least one element from each conjugacy class of G. Show that $H = G$.
d) Let G be a transitive subgroup of S_n with $n > 1$. Show that there exists an element of G with no fixed point.

Problem 5 — Let $P \in \mathbb{Z}[Y]$ be a polynomial, irreducible in $\mathbb{Q}[Y]$. Show that there exist infinitely many primes p such that the polynomial P reduced modulo p has no roots in $\mathbb{F}_p$.

Comments: Use the classical density Tchebotarev theorem.

Problem 6 — Show that a Henselian field (k, v) for a discrete valuation v is not Hilbertian.

Comments: For m in the valuation ideal of v, consider the polynomials $P_1 = Y^2 - mT - 1$ and $P_2 = Y^2 - (mT/T + 1) - 1$ (with Y^2 replaced by Y^3 if k is of characteristic 2) and show that the Hilbert set $H_k(P_1, P_2)$ is empty. (see [Dèb09, Example 5.0.1]).

Problem 7 — Let $d \geq 1$ be an integer, $\underline{U} = U_1, \ldots, U_d$ be d indeterminates and $T_1(\underline{U}), \ldots, T_d(\underline{U})$ be the d elementary symmetric functions in $\underline{U}$. Let k be a field.

a) Show that $T_1(\underline{U}), \ldots, T_d(\underline{U})$ are algebraically independent over $\overline{k}$.
b) Show that the field extension $k(\underline{U})/k(\underline{T}(\underline{U}))$ is Galois with Galois group the symmetric group S_d.

Comments: see [Dèb09, §2.5.1.1]).

Problem 8 — Given a field k and a finite separable extension $F/k(T)$, show that the following assertions are equivalent:
(i) $F \cap \overline{k} = k$,
(ii) for every finite extension E/k, $[FE : E(T)] = [F : k(T)]$,
(iii) $[F\overline{k} : \overline{k}(T)] = [F : k(T)]$.
Comments: see [Dèb09, §2.3.1].

Problem 9 — Let $F/k(T)$ be a degree n extension with F/k regular. Assume that the Galois closure of $F\overline{k}/\overline{k}(T)$ is of group S_n. Show that the Galois closure of F/k is regular. Give an example for which the conclusion fails if the assumption if removed.

Problem 10 — Let $n \geq 1$ be an integer and

$$f(Y) = Y^n + a_1 Y^{n-1} + \cdots + a_n$$

be a polynomial with coefficients $a_i \in \mathbb{Q}$. Set

$$P(T, Y) = f(Y) - T$$

and denote by $\mathcal{Y} \in \overline{\mathbb{Q}(T)}$ a root of the polynomial $P(T, Y)$ (in Y).

a) Show that $P(T, Y)$ is irreducible in $\overline{\mathbb{Q}}(T)[Y]$.

Set $E = \overline{\mathbb{Q}}(T)(\mathcal{Y})$, denote the Galois closure of the extension $E/\overline{\mathbb{Q}}(T)$ by $\widehat{E}/\overline{\mathbb{Q}}(T)$ and its Galois group by G.

b) Recall how G can be viewed as a transitive subgroup of S_n.

From now on, assume that f satisfies the following conditions:
(i) The roots $\beta_1, \ldots, \beta_{n-1} \in \overline{\mathbb{Q}}$ of the derivative $f'(Y)$ are simple.
(ii) $f(\beta_i) \neq f(\beta_j)$ for $i \neq j$.

c) Show that the branch points of the extension $E/\overline{\mathbb{Q}}(T)$ are in the set $\{f(\beta_1), \ldots, f(\beta_{n-1}), \infty\}$.

d) Show that for $i = 1, \ldots, n-1$ we have $f(Y) - f(\beta_i) = (Y - \beta_i)^2 g_i(Y)$ with $g_i(Y) \in \overline{\mathbb{Q}}[Y]$ separable and such that $g_i(\beta_i) \neq 0$.

e) Show that, for $i = 1, \ldots, n-1$, there are $n-2$ unramified points and one ramified point in the extension $E/\overline{\mathbb{Q}}(T)$ above $f(\beta_i)$, and that every inertia group is generated by a 2-cycle.

f) Show that if $v_{1/T}$ is the unique prolongation of the $1/T$-adic valuation from $\overline{\mathbb{Q}}((1/T))$ to the algebraic closure $\overline{\overline{\mathbb{Q}}((1/T))}$, then we have $v_{1/T}(\mathcal{Y}) = -1/n$.

g) Show that, above ∞, there is a totally ramified point in the extension $E/\overline{\mathbb{Q}}(T)$, and that every inertia group is generated by a n-cycle.

h) Denote by R the sum of all integers $e(\mathcal{P}) - 1$ where $\mathcal{P}$ ranges over all the points/places of E and $e(\mathcal{P})$ is the corresponding ramification index. Check that

$$-2[E : \overline{\mathbb{Q}}(T)] + R = -2$$

(that is, *via* the Riemann-Hurwitz formula, the function field E is of genus 0) and that

$$E = \overline{\mathbb{Q}}(\mathcal{Y})$$

(that is, E a pure transcendental extension of $\overline{\mathbb{Q}}$).

i) Show that the group G is generated by the inertia groups above the points $f(\beta_1), \ldots, f(\beta_{n-1})$. Conclude that $G = S_n$ (by using that a transitive subgroup of S_n that is generated by 2-cycles (or, more generally by cycles of prime length) is equal to S_n).

Problem 11 —

a) Deduce from problem 8 and problem 10 that S_n is a regular Galois group over $\mathbb{Q}$.

b) Show that for every finite group G, there exist a number field K such that G is a Galois group over K.

Problem 12 — Given $n \geq 3$, let E be the splitting field of $P(T, X) = X^n - X^{n-1} - T$ over $\mathbb{Q}(T)$.

a) Show that $P(T, X)$ is irreducible over $\overline{\mathbb{Q}}(T)$.

b) Show that the branch points of $E/\mathbb{Q}(T)$ are $0, \infty, Q(1 - (1/n))$ with $Q(Y) = Y^n - Y^{n-1}$, with inertia groups generated by an n-cycle at ∞, an $(n-1)$-cycle at 0, and a transposition at $Q(1 - (1/n))$. Conclude that $E/\mathbb{Q}(T)$ has Galois group S_n.

c) Show that $E^{A_n} = \mathbb{Q}(U)$ for some transcendental U. Conclude that A_n is a regular Galois group over $\mathbb{Q}$ (in particular, a Galois group over $\mathbb{Q}$).

Comments: More details and more general statements can be found in [Ser92, §4.4-5] and in [FJ08, §16.7]. Compared with Problem 11, one can do things with A_n. Of course, the statement of the above exercise should be more detailed.

Problem 13 — Let $n \geq 3$.

a) Show that there exist infinitely monic polynomials $f \in \mathbb{Z}[X]$ of degree n such that f mod 2 is irreducible, f mod 3 is separable with an irreducible factor of degree $n-1$, and (for some further prime p) f mod p is separable with exactly one quadratic factor and linear factors otherwise.

Hint: Chinese Remainder.

b) Use Dedekind's criterion and Jordan's theorem to conclude that infinitely many polynomials have Galois group S_n over $\mathbb{Q}$.

Problem 14 — Let $P(T) \in \mathbb{Z}[T]$ be a separable polynomial of degree n. Set $P(T) = a_0 + a_1 T + \cdots + a_{n-1}T^{n-1} + a_n T^n$ and $E = \mathbb{Q}(T)(\sqrt{P(T)})$. Denote the roots of $P(T)$ by $t_1, \dots, t_n$.

a) Show that the integral closure of $\overline{\mathbb{Q}}[T]$ in $E\overline{\mathbb{Q}}$ is $\overline{\mathbb{Q}}[T] + \overline{\mathbb{Q}}[T]\sqrt{P(T)}$. Conclude that the set $\mathbf{t}$ of branch points of $E/\mathbb{Q}(T)$ is $\{t_1, \dots, t_n\}$ (resp., $\{t_1, \dots, t_n\} \cup \{\infty\}$) if n is even (resp., if n is odd).

b) Let $t_0 \in \mathbb{P}^1(\mathbb{Q}) \setminus \mathbf{t}$. Show that $E_{t_0} = \mathbb{Q}(\sqrt{P(t_0)})$ if $t_0 \in \mathbb{Q}$ and $E_\infty = \mathbb{Q}(\sqrt{a_n})$ (if n is even).

c) Let d be a non-zero integer. Show that d is a square in $\mathbb{Z}$ if and only if d is a square in $\mathbb{F}_p$ for all but finitely many prime numbers p.

d) Suppose $n = 2$. Show that $E/\mathbb{Q}(T)$ is $\mathbb{Q}$-parametric iff $a_1^2 - 4a_0a_2$ is a square in $\mathbb{Z}$.

Comments: For (a), use, e.g., [Leg13, Lemma 2.3.5] (and its proof) and the Riemann-Hurwitz formula. For (b), see, e.g., [KL18, Lemma 8.3]. (c) is a classical consequence of the Chebotarev density theorem (more elementary proofs exist in the quadratic case, of course). (d) is [Leg15, Proposition 3.1].

Problem 15 —

a) Let k be an arbitrary field and L/k a finite Galois extension of group S_3. Show that there exists $t_0 \in k$ such that L is the splitting field over k of the polynomial $X^3 + t_0 X + t_0$ (that is, $X^3 + TX + T$ is generic).

b) Let F be the splitting field over $\mathbb{Q}$ of the polynomial $P(X) = X^3 + 3X^2 - 6X - 4$. Show that $F/\mathbb{Q}$ has Galois group S_3 and $F \subseteq \mathbb{R}$.

c) Let E be the splitting field over $\mathbb{Q}(T)$ of the polynomial $X^3 + T^2 X + T^2$. Show that $E/\mathbb{Q}(T)$ is a regular Galois extension of group S_3 and no specialization of it is contained in $\mathbb{R}$. Conclude that $E/\mathbb{Q}(T)$ cannot be $\mathbb{Q}$-parametric.

Comments: For (1), see [JLY02, page 30]. For (2), $P(X)$ is irreducible modulo $p = 5$. Moreover, setting $Y = X + 1$, one sees that F is the splitting field over $\mathbb{Q}$ of $Y^3 - 9Y + 4$ whose discriminant is a positive non-square. One can also study the derivative of $P(X)$ to show that F is contained in $\mathbb{R}$. For (3), see [Leg15, Proposition 3.5].

Problem 16 — Let $f(T, X) \in \mathbb{Q}(T)[X]$ be an irreducible degree-n polynomial with Galois group $G \leq S_n$. Assume that $f(0, X)$ is separable of degree-n and splits completely over $\mathbb{Q}$. Let p be a prime number.

a) Show that for all $t_0 \in \mathbb{Q}$ which are divisible by p sufficiently often, the polynomial $f(t_0, X)$ splits completely over $\mathbb{Q}_p$.

b) Now let S be a finite set of prime numbers. Conclude the existence of infinitely many G-extensions which are unramified at all primes $p \in S$.

Problem 17 — Let $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n$ and T be independent transcendentals, and let

$$f(X) = \prod_{i=1}^{n}(X - \alpha_i) - T\prod_{j=1}^{n}(X - \beta_j)$$

a) Show that $Gal(f \mid \mathbb{Q}(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n, T)) = S_n$.
b) Show that f' is separable as a polynomial in T.
c) Conclude that all inertia subgroups (with respect to T) of the splitting field of f are generated by transpositions.
d) Use Hilbert's irreducibility theorem, the specialization inertia theorem and problem 14 to show that there are infinitely many S_n-extensions of $\mathbb{Q}$ all of whose inertia groups are generated by transpositions.

Problem 18 — Let $\mathbb{C}(X)/\mathbb{C}(T)$ be a Galois extension of rational function fields, let $n := [\mathbb{C}(X) : \mathbb{C}(T)]$, and let $(e_1, \dots, e_r)$ be the tuple of ramification indices at the branch points of $\mathbb{C}(X)/\mathbb{C}(T)$ (sorted with $e_1 \leq \dots \leq e_r$).

a) Use the Riemann-Hurwitz formula to show that $(n, (e_1, \dots, e_r))$ is one of the following types:

$$(n, (n, n)), (n, (2, 2, n/2)), (12, (2, 3, 3)), (24, (2, 3, 4)), (60, (2, 3, 5)).$$

b) What conclusions can you obtain from this about the finite subgroups of $PGL_2(\mathbb{C})$?

Problem 19 — Let $E/\mathbb{C}(T)$ be a finite Galois extension ramified at $r \geq 2$ points. Let $d \in \mathbb{N}$. Show that there exists a degree-d rational function field extension $\mathbb{C}(S)/\mathbb{C}(T)$ such that the rational pullback $E(S)/\mathbb{Q}(S)$ has exactly rd branch points, and another one such that the pullback has at most $(r-2)d + 2$ branch points.

Problem 20 —

a) Let X_1, X_2 be compact connected Riemann surfaces of genus ≥ 2, and $f_i : X_i \to \mathbb{P}^1_{\mathbb{C}}$ be Galois covers ($i = 1, 2$) such that f_1 is isomorphic to a rational pullback of f_2 and vice versa. Show that the pullback maps must have been "trivial", i.e., fractional linear transformations.
b) Now drop the assumption of genus ≥ 2. Can you construct genus-0 Galois covers f_1, f_2 which are mutual pullbacks of each other in a non-trivial way? How about genus 1?

Problem 21 — (Invariants and resolvents): Let $F = X_1X_3 + X_2X_4$.

a) Show that F has stabilizer isomorphic to D_4 (under the action of S_4).
b) One can calculate that this yields the following resolvent for $G = D_4$:

$$\theta_G(f, F) = X^3 - a_2X^2 + (a_3a_1 - 4a_0)X + 4a_2a_0 - a_3^2a_0 - a_1^2,$$

where f is given as $f = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$.
Use this to find irreducible polynomials f of the form $f = X^4 + aX + a \in \mathbb{Q}[X]$ whose Galois group is contained in D_4.
Can you show that there are infinitely many such polynomials?

Problem 22 — (Some truncated series)
Let p be an odd prime and let $f = 1 + 2X + 3X^2 + \cdots + pX^{p-1}$.

a) Show that $f \equiv -(X-1)^{p-2} \bmod p$.
b) Using Newton polygons, show that f factors over $\mathbb{Q}_p$ into irreducible polynomials of degree 1 and $p-2$.
(It might be convenient to argue with $f(X+1)$.)
c) Show that the Galois group of f is a doubly transitive subgroup of S_{p-1}.
d) Under the assumption that $q := \frac{p+1}{2}$ is also a prime, use Newton polygons again to show $Gal(f)$ contains a q-cycle, and conclude that $Gal(f) = S_n$ or A_n.

Problem 23 — (A polynomial with group D_5)
Let $f(X) = X^5 - 2X^4 + 2X^3 - X^2 + 1$, $g(X) = X(X-1)^2$, and $F(t,X) = f(X) - tg(X)$.

a) Show that $G = Gal(F/\mathbb{Q}(t))$ is a transitive subgroup of S_5 of even order.
b) Use (without proof) the following fact to show that $G \cong D_5$:

$$f(X)g(Y) - g(X)f(Y) = (X-Y)(X^2Y - X^2 + XY^2 - 2XY + 2X - Y^2 + 2Y - 1)(X^2Y^2 - X^2Y - XY^2 + 1).$$

(Hint: Show that the point stabilizer in G must have order 2.)

Problem 24 — Let

$$R_2(B) = \#\{a, b \in \mathbb{Z} : |a|, |b| \le B,\ X^2 + aX + b \text{ is reducible}\}.$$

Prove that there exists positive constants $0 < c < C$ such that for every $B > 0$

$$c\frac{B}{\log B} \le R_2(B) \le C\frac{B}{\log B}.$$

Problem 25 —

a) Prove that if $G \le S_d$ is 2-transitive (i.e. acts transitively on the set of pairs (a,b) with $a \ne b$, or equivalently, G is transitive and the stabilizer of a point G_a is transitive on $\{1, \ldots, d\} \smallsetminus \{a\}$) and contains a transposition, then $G = S_d$.
b) Deduce that a subgroup of S_d containing a transposition, a d-cycle, and a $(d-1)$-cycle must be S_d.
c) Recall that a subgroup $G \le S_d$ is primitive if it is transitive and it preserves no non-trivial partition of $\{1, \ldots, d\}$ (equivalently G is transitive and a stabilizer G_a is a maximal subgroup). Show that if a primitive group $G \le S_d$ contains a transposition then $G = S_d$.
d) Let $f \in K[X]$ be a separable polynomial of degree d, let N be a splitting field, let $\alpha, \beta \in N$ be two distinct roots of f and let $G = \mathrm{Gal}(N/K) \le S_d$. Show that
   (1) G is primitive if and only if $[K(\alpha) : K] = d$ and $K(\alpha)/K$ is minimal (i.e., there are no proper subextensions)
   (2) G is doubly transitive if and only if $[K(\alpha, \beta) : K] = d(d-1)$.

Problem 26 — Use the large sieve inequality to show that

$$\#\{n \leq x : n, n+2 \text{ are both prime}\} \ll \frac{x}{(\log x)^2}$$

and deduce that

$$B_2 := \sum_{\substack{p \leq x \\ p+2 \text{ prime}}} \frac{1}{p} < \infty.$$

(Computation may show that $B_2 = 1.902160540...$).

Problem 27 — Let $\mathbf{t} = (t_1, \ldots, t_r)$, let $f(\mathbf{t}, X) \in \mathbb{Q}[\mathbf{t}, X]$ be an irreducible polynomial that is monic in X, let L be a splitting field of f over $\mathbb{Q}(\mathbf{t})$, and let R be the integral closure of $\mathbb{Q}[\mathbf{t}]$ in L.

a) Show that the specialization $\mathbf{t} \mapsto \mathbf{a}$ may be extended to an epimorphism $\phi\colon R \to L_{\mathbf{a}}$.
b) Show that if $\operatorname{disc}(f(\mathbf{a}, X)) \neq 0$, then ϕ induces a bijection between the roots of $f(\mathbf{t}, X)$ and of $f(\mathbf{a}, X)$.
c) Show that in the case of the previous question the bijection $x_i \mapsto \phi(x_i)$ between the roots of $f(\mathbf{t}, X)$ in R and the roots of $f(\mathbf{a}, X)$ in $L_{\mathbf{a}}$ induces an embedding of $G_{\mathbf{a}}$ into G.
d) Deduce that if $[L : \mathbb{Q}(\mathbf{t})] = [L_{\mathbf{a}} : \mathbb{Q}]$, then $f(\mathbf{a}, X)$ is irreducible.
e) Give example in which $f(\mathbf{a}, X)$ is irreducible but $[L : \mathbb{Q}(\mathbf{t})] \neq [L_{\mathbf{a}} : \mathbb{Q}]$.

Problem 28 —

a) Prove the LYM inequality: Let A be a family of subsets of $\{1, 2, \ldots, n\}$. If A is an anti-chain (that is, $s \not\subseteq t$ for any $s \neq t \in A$), then

$$\sum_{s \in A} \frac{1}{\binom{n}{|s|}} \leq 1.$$

(Hint: What can be said about permutations π of $\{1, 2, \ldots, n\}$ such that $\{\pi(1), \ldots, \pi(|s|)\} = s$ for some $s \in A$?)
b) Deduce Sperner's inequality: Under the same conditions as before, $|A| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

Problem 29 — Denote by $\mathcal{O}$ the set of algebraic integers. Given $\alpha \in \mathcal{O}$, we denote by $d(\alpha)$ the degree of its minimal polynomial.

Fix $H \geq 2$, and let $A_{n,H}$ be the set of monic integer polynomials with coefficients in $\{1, 2, \ldots, H\}$, endowed with the counting measure. Give an *explicit* upper bound on the cardinality of

$$T(\ell) = \{\alpha \in \mathcal{O} : d(\alpha) \leq \ell, \exists f \in \mathbb{Z}[x] \text{ of height at most } H \text{ s.t. } f(\alpha) = 0\}.$$

Use it to construct an *explicit* function $s(n)$, tending to infinity with n, such that

$$\mathbb{P}_{f \in A_{n,h}}(f \text{ has no divisor of degree } \leq s(n)) \to 1$$

as n tends to infinity.

Problem 30 —

a) Let $f = x^n + \sum_{i=0}^{n-1} a_i x^i \in \mathbb{C}[x]$. Suppose that $a_0 \neq 0$ and that $|a_{n-1}| > 1 + |a_{n-2}| + |a_{n-3}| + \ldots + |a_0|$. Prove that f has $n-1$ roots with absolute value less than 1, and one root with absolute value greater than 1.
(Hint: Rouché's Theorem.)

b) (Perron) Let $f = x^n + \sum_{i=0}^{n-1} a_i x^i \in \mathbb{Z}[x]$ be a polynomial satisfying $a_0 \neq 0$ and $|a_{n-1}| > 1 + |a_{n-2}| + |a_{n-3}| + \ldots + |a_0|$. Prove that f is irreducible over $\mathbb{Q}$.

c) Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$. Suppose that $a_n \geq 1$, $a_{n-1} \geq 0$ and that $|a_i| \leq H$ for $i = 0, 1, \ldots, n-2$, where H is some fixed positive constant. Then any complex zero α of f either has non-positive real part or satisfies

$$|\alpha| < \frac{1 + \sqrt{1 + 4H}}{2}.$$

d) Let $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i \in \mathbb{Z}[x]$ with $a_i \in \{0, 1\}$ for every i. If $|\arg \alpha| \leq \pi/4$, then $|\alpha| < 3/2$. Otherwise $\Re\alpha < (1 + \sqrt{5})/(2\sqrt{2})$.
(Here $\arg(z) \in [-\pi/2, \pi/2)$ is defined via $z/|z| = e^{i\arg(z)}$.)

e) (Cohn) Let $b \geq 2$ be an integer, and let p be a prime with b-adic expansion

$$p = a_n b^n + a_{n-1} b^{n-1} + a_1 b + a_0,$$

i.e. for each i, a_i is an integer with $0 \leq a_i < b$. Then $f(x) = \sum_{i=0}^{n} a_i x^i$ is irreducible over $\mathbb{Q}$.

Problem 31 — The divisor function $d_k(f)$ for a monic polynomial $f \in \mathbb{F}_q[x]$ is the number of k-tuples $(a_1, \cdots, a_n) \in \mathbb{F}_q[x]^k$ of monic polynomials so that $f = a_1 \cdots a_k$. Show that for $\mathrm{Re}(s) > 1$,

$$\sum_{f monic} \frac{d_k(f)}{|f|^s} = \zeta_q(s)^k.$$

Problem 32 — The Möbius function for $\mathbb{F}_q[x]$ is defined as $\mu(f) = (-1)^k$ if $f = cP_1 \cdots P_k$ is a product of k distinct monic irreducibles, $c \in \mathbb{F}_q^*$, and $\mu(f) = 0$ otherwise. Show that for $\mathrm{Re}(s) > 1$,

$$\sum_{f monic} \frac{\mu(f)}{|f|^s} = \frac{1}{\zeta_q(s)}.$$

Problem 33 — Show that

$$\sum_{d|f} \Lambda(d) = \deg f.$$

Problem 34 — Show that for $k \geq 2$, the mean value of $d_k(f)$ over all monic polynomials $f \in \mathbb{F}_q[x]$ of degree n is given by the binomial coefficient

$$\frac{1}{q^n} \sum_{\substack{\deg f = n \\ f monic}} d_k(f) = \binom{n+k-1}{k-1} = \frac{(n+k-1)\cdots(n+1)}{(k-1)!}.$$

Problem 35 — Show that

$$\sum_{\substack{\deg f=n \\ f monic}} \mu(f) = 0,\ n \geq 2.$$

Problem 36 — Show that

$$\sum_{\deg P \leq N} \frac{1}{|P|} \sim \log N,\ N \to \infty.$$

The sum over all prime polynomials (monic irreducibles) and in particular that $\sum_P \frac{1}{|P|} = \infty$.

Problem 37 — The cycle structure of a permutation σ of n letters is $\lambda(\sigma) = (\lambda_1, \cdots, \lambda_n)$ if in the decomposition of σ as a product of disjoint cycle, there are λ_j cycle of length j. In particular $\lambda_1(\sigma)$ is the number of fixed points of σ.

For each partition $\lambda \vdash n$, denote by $p(\lambda)$ the probability that a random permutation on n letters has cycle structure λ:

$$p(\lambda) = \frac{\#\{\sigma \in S_n : \lambda(\sigma) = \lambda\}}{\# S_n}.$$

Show that

$$p(\lambda) = \prod_{j=1}^{n} \frac{1}{j^{\lambda_j}.\lambda_j!}.$$

In particular, this shows that the proportion of n-cycles in the symmetric group S_n is $1/n$.

Problem 38 — For $f \in \mathbb{F}_q[x]$ of positive degree n, we say its cycle structure is $\lambda(f) = (\lambda_1, \cdots, \lambda_n)$ if in the prime decomposition $f = \prod_\alpha P_\alpha$ (we allow repetition), we have $\#\{\alpha : \deg P_\alpha = j\} = \lambda_j$. In particular, $\deg f = \sum_j j\lambda_j$. Thus we get a partition od $\deg f$, which we denote by $\lambda(f)$. For instance, f is prime if and only if $\lambda(f) = (0, 0, \cdots, 0, 1)$.

Given a partition $\lambda \vdash n$, show that the probability that a random monic polynomial f of degree n has cycle structure λ is asymptotic, as $q \to \infty$, to the probability that a random permutation of n letters has that cycle structure:

$$\frac{1}{q}\#\{f \text{ monic},\ \deg f = n : \lambda(f) = \lambda\} = p(\lambda)\left(1 + O_n(\frac{1}{q})\right).$$

Hint: start with primes, where the statement is just the Prime Polynomial Theorem.

Problem 39 — Consider the set Ω of n-tuples $\lambda = (\lambda_1, \ldots, \lambda_n)$ of non-negative integers with $\sum_i i\lambda_i = n$. Define two probability measures on Ω. We pick a uniform random $f \in \mathbb{F}_q[T]$, and we define $P_1(\lambda)$ to be the probably that f has cycle structure λ. For the second measure, we pick uniformly at random $\sigma \in S_n$ and we define $P_2(\lambda)$ to be the probability that σ has cycle structure λ.

a) Show that there exists a constant C_n depending only on n such that
$$|P_1(\lambda) - P_2(\lambda)| \leq C_n q^{-1}.$$
b) Show that there exists an absolute constant $C > 0$ such that
$$|P_1(\lambda) - P_2(\lambda)| \leq C q^{-1}.$$
c) Show that there exists an event $E \subseteq \Omega$ such that $|P_1(E) - P_2(E)| > cq^{-1}$.

d) Let E be event consisting on some λ-s with $\lambda_1 = \cdots = \lambda_k = 0$ for some $1 \leq k < n$ with k tending to infinity with n (e.g. $k = \log\log n$). Show that $|P_1(E) - P_2(E)| \to 0$ as $n \to \infty$.

References

[Dèb09] Pierre Dèbes. Arithmétique des revêtements de la droite. 2009. `http://math.univ-lille1.fr/~pde/pub.html`

[FJ08] Michael D. Fried and Moshe Jarden. *Field arithmetic.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 11. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden. xxiv + 792 pp.

[JLY02] Christian U. Jensen, Arne Ledet, and Noriko Yui. *Generic polynomials. Constructive Aspects of the Inverse Galois Problem.* Mathematical Sciences Research Institute Publications, 45. Cambridge University Press, 2002. x+258 pp.

[KL18] Joachim König and François Legrand. Non-parametric sets of regular realizations over number fields. *J. Algebra*, 497:302–336, 2018.

[Leg13] François Legrand. *Spécialisations de revêtements et théorie inverse de Galois.* PhD thesis, Université Lille 1, France, 2013.

[Leg15] François Legrand. Parametric Galois extensions. *J. Algebra*, 422:187–222, 2015.

[Ser92] Jean-Pierre Serre. *Topics in Galois Theory*, volume 1 of *Research Notes in Mathematics.* Jones and Bartlett Publishers, Boston, MA, 1992. Lecture notes prepared by Henri Darmon [Henri Darmon]. With a foreword by Darmon and the author. xvi+117 pp.