Math 5591H **Some practice problems**

1. *If K/F is a Galois extension of degree $n = mp^r$ where p is prime and $p \nmid m$, prove that K/F has a subextension L/F such that $[L : F] = m$, and that all such subextensions are isomorphic.*

Solution. By Galois's theorem, subextensions L/F of K/F of degree m correspond to subgroups of $\mathrm{Gal}(K/F)$ of order $n/m = p^r$, that is, tp Sylow p-subgroups. Hence, they exist and are all conjugate.

2. *Let p be a prime integer, let F be a field with $\mathrm{char}\, F \neq p$, let $f \in F[x]$ be a separable polynomial, and assume that the splitting field K of f has degree p^r over F for some $r \in \mathbb{N}$. Prove that f is solvable in radicals. If F contains a root of unity of degree p, how many nested radicals and of what degrees would suffice to express a root of f?*

Solution. $\mathrm{Gal}(K/F)$ is a p-group, so K/F is a p-extension, so is a tower of r cyclic extensions of degree p. Since $\mathrm{char}\, F \neq p$, after adjoining to F a primitive p-th root of unity ω, all these extensions are radical of degree p. So, in addition to ω, we will need at most r nested radicals of degree p to express roots of f.

3. (a) *Is it true that a normal extension of a normal extension is normal? (Prove or give a counterexample.)*

Solution. Not true, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ are normal but $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ isn't.

(b) *Is it true that a separable extension of a separable extension is separable?*

Solution. This is true, but not that easy to prove.

4. *Prove that every root of unity of degree n is expressible in radicals of degrees $< n$.*

Solution. In characteristic zero, the Galois group of the n-th cyclotomic polynomial is abelian (isomorphic to $\mathbb{Z}_n^*$) of order $\varphi(n) < n$, so its roots are expressible in radicals of degrees $< n$. In finite characteristic p, if $p \mid n$, then the roots of unity of degree n are also roots of unity of degree n/p. If $p \nmid n$, then the polynomial $x^n - 1$ is separable, and its Galois group is a subgroup of $\mathbb{Z}_n^*$.

5. *Let K/F be a Galois extension with $\mathrm{Gal}(K/F) = G$ and let $\alpha \in K$.*

(a) *Prove that $K = F(\alpha)$ iff the elements $\varphi(\alpha)$, $\varphi \in G$, are all distinct.*

Solution. $K = F(\alpha)$ iff $\deg_F \alpha = [K : F]$ iff α has $[K : F] = |G|$ conjugates iff $\varphi(\alpha)$, $\varphi \in G$, are all distinct.

(b) *In general, prove that $[K : F(\alpha)] = |H|$ where H is the stabilizer of α in G, $H = \{\varphi \in G : \varphi(\alpha) = \alpha\}$.*

Solution. An element of G fixes $F(\alpha)$ iff it fixes α, so the stabilizer H of α in G is just $\mathrm{Gal}(K/F(\alpha))$, so $[K : F(\alpha)] = |H|$.

6. *Let K/F be a Galois extension of degree pq where $p < q$ are primes. How many subextensions and of what degrees can K/F have? (Consider two cases: where p divides $q - 1$ and where it doesn't.)*

Solution. Translating it to the language of groups, the question is: given a group G of order pq, how many subgroups and of what indexes may G have? And the answer is: either G has one subgroup of index p and one of index q, or, in the case $q = 1 \bmod p$ and G is noncommutative, it has one subgroup of index p (that is, of order q) and q subgroups (of order p) of index q.

7. *If $\mathrm{char}\, F \neq 0$, prove that an extension K/F of degree 4 can be generated by the root of an irreducible biquadratic $x^4 + ax^2 + b \in F[x]$ if and only if K contains a quadratic extension of F.*

Solution. If $K = F(\alpha)$ where α is a root of a biquadratic polynomial $x^4 + ax^2 + b$, then $\alpha = \pm\sqrt{a/2 \pm \sqrt{D}/2}$ where $D = a^2 - 4b$. Were $\sqrt{D}$ in F, then α would have degree ≤ 2 over F; so, $\sqrt{D} \notin F$ and K contains the quadratic subextension $F(\sqrt{D})/F$.

Conversely, assume that F contains a quadratic extension L of F. Then $L = F(\sqrt{c})$ for some $c \in F$, and K is a quadratic extension of L, so $K = L(\alpha)$ where $\alpha = \sqrt{\gamma}$ for some $\gamma \in F(\sqrt{c})$. Let $\gamma = a + b\sqrt{c}$, $a, b \in F$, then $\alpha^2 = a + b\sqrt{c}$, so $(\alpha^2 - a)^2 = bc^2$, and α is a root of the biquadratic polynomial $x^4 - 2ax^2 + a^2 - bc^2$.

8. *Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be a squarefree integer and let $a \in \mathbb{Q}$ be a nonzero rational number. Prove that the extension $\mathbb{Q}(\sqrt{a\sqrt{d}})/\mathbb{Q}$ is Galois only if $d = -1$.*

Solution. Let $\alpha = \sqrt{a\sqrt{d}}$ and $K = \mathbb{Q}(\alpha)$; the minimal polynomial of α is $f(x) = x^4 - a^2d$, and the conjugates of α are $\pm\alpha, \pm i\alpha$. Assume that $K/\mathbb{Q}$ is Galois, then $i\alpha \in K$, so $i \in K$. The degree of K over $\mathbb{Q}$ may be 2 or 4. If $[K : \mathbb{Q}] = 2$, then $K = \mathbb{Q}(\sqrt{d})$, and since $i \in K$, $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$. Hence, $-d = d/(-1)$ is a square in $\mathbb{Q}$, and since d is squarefree, $-d = 1$.

If $[K : \mathbb{Q}] = 4$, then the Galois group of $K/\mathbb{Q}$ is either $\mathbb{Z}_4$ of V_4. If it is $\mathbb{Z}_4$, then K has a single quadratic subextension, so $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(i)$, and $d = -1$ as above. If the group is V_4, then the square root of the discriminant of f is in $\mathbb{Q}$. As the discriminant of f is $-4^4(a^2d)^3$, we again have $\sqrt{-d} \in \mathbb{Q}$, so $d = -1$.

9. *Construct a polynomial over $\mathbb{Q}$ whose Galois group is isomorphic to $\mathbb{Z}_4$.*

Solution. There are many ways to do this; I'll use an irreducible biquadratic polynomial $f(x) = x^4 + ax^2 + b$. It has roots $\pm\alpha$, $\pm\beta$ with $\alpha\beta = \sqrt{b}$, and if $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ and $\sqrt{b} \notin \mathbb{Q}$, then the Galois group G of f has order 4 and contains an element φ with $\varphi(\alpha) = \beta$ and $\varphi(\sqrt{b}) = -\sqrt{b}$, so $\varphi^2(\alpha) = \varphi(\beta) = \varphi(\sqrt{b}/\alpha) = -\sqrt{b}/\beta = -\alpha$; thus φ has order 4 and $G = \langle\varphi\rangle$. Ok, take $\alpha = \sqrt{2+\sqrt{2}}$ and $\beta = \sqrt{2-\sqrt{2}}$, then $\alpha\beta = \sqrt{2} \in \mathbb{Q}(\alpha)$, so $\beta \in \mathbb{Q}(\alpha)$ and $\alpha\beta \notin \mathbb{Q}$. The corresponding polynomial is $x^4 - 4x + 2$.

10. *For which n is the number $\sqrt[n]{3}$ constructible?*

Solution. The polynomial $x^n - 3$ is irreducible over $\mathbb{Q}$ by Eisenstein criterion, thus $\deg_{\mathbb{Q}} \sqrt[n]{3} = n$. For this number to be constructible, it must be that $n = 2^k$ for some $k \in \mathbb{N}$. And, since we can "construct" square roots, it is easy to see that this condition is also sufficient.

11. *Find the Galois group of $f = x^3 - 3x + 3 \in \mathbb{Q}[x]$.*

Solution. f is irreducible by Eisenstein&Gauss. The discriminant of f is $-4 \cdot (-3)^3 - 27 \cdot 3^2 < 0$, so the Galois group is S_3.

Alternatively, f is irreducible and has one real and two complex roots, so the group is S_3.

12. *Find the Galois group of $f = x^4 - 2$*

(a) *over $\mathbb{Q}$;*

Solution. f is irreducible. The splitting field of f is $\mathbb{Q}(\alpha, i)$ where $\alpha = \sqrt[4]{2}$, $\mathbb{Q}(\alpha) \cap \mathbb{Q}(i) = \mathbb{Q}$, $\mathbb{Q}(i)/\mathbb{Q}$ is normal, $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}_2$, $\mathrm{Gal}(K/\mathbb{Q}(i)) \cong \mathbb{Z}_4$, so $\mathrm{Gal}(f/\mathbb{Q})$ is the nondirect $\cong \mathbb{Z}_4 \rtimes \mathbb{Z}_2$.

(b) *over $\mathbb{F}_3$;*

Solution. f is reducible, $f = (x^2 + x - 1)(x^2 - x - 1)$, where both $x^2 + x - 1$ and $x^2 - x - 1$ are irreducible, the splitting field of f is $\mathbb{F}_{3^2}$, the Galois group is $\mathbb{Z}_2$.

(c) *over $\mathbb{F}_7$.*

Solution. f has roots ± 2 in $\mathbb{F}_7$, so $x^4 - 2 = (x - 2)(x + 2)(x^2 + 4)$, and $x^2 + 4$ is irreducible. So, the Galois group is $\mathbb{Z}_2$.

13. *Find the Galois group over $\mathbb{Q}$ of the polynomials*

(a) *$f = x^5 - 2$;*

Solution. $\mathbb{Z}_5 \rtimes \mathbb{Z}_5^*$. (For any odd n and positive $a \in \mathbb{Q}$ such that $x^n - a$ is irreducible we have $\mathrm{Gal}(x^n - a/\mathbb{Q}) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^* = \mathrm{Hol}(\mathbb{Z}_n)$.)

(b) *$f = x^9 - 2$.*

Solution. $\mathbb{Z}_9 \rtimes \mathbb{Z}_9^* = \mathrm{Hol}(\mathbb{Z}_9)$.

14. *Find the Galois group of $f = x^4 + x^3 + x^2 + x + 1$*

(a) *over $\mathbb{Q}$;*

Solution. Over $\mathbb{Q}$, f is the cyclotomic polynomial Φ_5, and its Galois group is $\mathbb{Z}_5^* \cong \mathbb{Z}^4$.

(b) *over $\mathbb{F}_2$.*

Solution. f is also irreducible (it has no roots and is not equal to $(x^2 + x + 1)^2$), so its splitting field is $\mathbb{F}_{2^4}$ and the Galois group is $\mathbb{Z}_4$ as well.

15. *Find the Galois group and all subfields of the splitting field of $f = x^4 + 3x^2 + 1 \in \mathbb{Q}[x]$.*

Solution. The theory of the Galois groups of quartics says that the group is V_4, but since we have to describe the subextensions of the splitting field let's compute $G = \mathrm{Gal}(f/\mathbb{Q})$ directly.

f has no rational roots, and (it can be checked that) is not a product of two quadratic polynomials, so is irreducible. Let K be the splitting field of f. Let $\alpha = \sqrt{-3/2 + \sqrt{5}/2}$ and $\beta = \sqrt{-3/2 - \sqrt{5}/2}$ (where $\sqrt{5}$ in both formulas is the same, say, > 0). Then the roots of f are $\pm\alpha, \pm\beta$, and $K = \mathbb{Q}(\alpha, \beta)$. Both α and β have degree 4 over $\mathbb{Q}$, and the fields $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$ contain (and are quadratic extensions of) $\mathbb{Q}(\sqrt{5})$, thus either $[K : \mathbb{Q}] = 8$ (if $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ or $[K : \mathbb{Q}] = 4$ (if $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$). We have $\alpha\beta = 1$ (or -1, which depends on the choice of signs for α and β), so $\beta \in \mathbb{Q}(\alpha)$, $K = \mathbb{Q}(\alpha)$, and $[K : \mathbb{Q}] = 4$. Hence, G is either $\mathbb{Z}_4$ or V_4.

Since $K = \mathbb{Q}(\alpha)$, elements of G are defined by their action on α. Let $\varphi_1, \varphi_2, \varphi_3 \in G$ be such that $\varphi_1(\alpha) = \beta$, $\varphi_2(\alpha) = -\beta$, and $\varphi_3(\alpha) = -\alpha$. Then $\varphi_1(\beta) = \varphi_1(1/\alpha) = 1/\varphi_1(\alpha) = 1/\beta = \alpha$, so $\varphi_1^2(\alpha) = \alpha$ and $\varphi_1^2(\beta) = \beta$, so $\varphi_1^2 = 1$; $\varphi_2(\beta) = \varphi_2(1/\alpha) = 1/\varphi_2(\alpha) = -1/\beta = -\alpha$, so $\varphi_2^2(\alpha) = \varphi_2(-\beta) = \alpha$ and $\varphi_2^2(\beta) = \beta$, so $\varphi_2^2 = 1$; and $\alpha_3(\beta) = -\beta$, so $\alpha_3^2 = 1$ as well. Hence, $G \cong V_4$.

G has 3 nontrivial proper subgroups, thus, in addition to $\mathbb{Q}$ and itself, K has 3 subfields. All these subfields have degree 2 over $\mathbb{Q}$, and so, are generated by any non-rational elements thereof. The subfield fixed by φ_1 is $\mathbb{Q}(\alpha + \beta)$, the sibfield fixed by φ_2 is $\mathbb{Q}(\alpha - \beta)$, and the subfield fixed by φ_3 is $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{5})$.

16. *Find the Galois group and all subfields of the splitting field of $f = x^4 + x^2 + 1 \in \mathbb{Q}[x]$.*

Solution. f is reducible, $f = (x^2 + x + 1)(x^2 - x + 1)$. The first factor is the 3rd cyclotomic polynomial Φ_3, and the second factor is the 6th cyclotomic polynomial Φ_6. So, the roots of the first factor are contained in the field generated by the roots of the second factor, and the splitting field of f is $K = \mathbb{Q}(\omega)$ where $\omega = e^{2\pi i/6}$. Thus, $[K : \mathbb{Q}] = 2$, $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_2$, and K contains no nontrivial proper subfields.

17. *Find the Galois group of $f = x^4 + 2x^2 + x + 3 \in \mathbb{Q}[x]$.*

Solution. First of all, f is irreducible: modulo 2 it is $x^4 + x + 1$, which is irreducible in $\mathbb{F}_2[x]$. Next, the cubic resolvent of f is $R(x) = x^3 - 2 \cdot 2x^2 + (2^2 - 4 \cdot 3)x + 1^2 = x^3 - 4x^2 - 8x + 1$. R has no roots (± 1 don't fit), so, is irreducible. Hence, in accordance with our classification, the Galois group of f is either S_4 or A_4. The discriminant of R (and of f) is $D = (-4)^2(-8)^2 - 4(-8)^3 - 4(-4)^3 \cdot 1 - 27 \cdot 1^2 + 18(-4)(-8) \cdot 1 = 3877$, which is prime and so, is not a square in $\mathbb{Q}$; hence, the group is S_4.

18. *For prime p, prove that the Galois group of $f = x^4 + px + p \in \mathbb{Q}[x]$ is S_4 for $p \neq 3,\ 5$, D_8 for $p = 3$, and $\mathbb{Z}_4$ for $p = 5$.*

Solution. First of all, f is irreducible by Eisenstein's criterion. The cubic resolvent of f is $R(x) = x^3 - 4px + p^2$, and the discriminant is $D = 256p^3 - 27p^4$. D is never a square (since if $256p - 27p^2 = n^2$, then $n = mp$, so $256 - 27p = m^2p$, so $p = 2$; but for $p = 2$, $D = 16 \cdot 101$ is not a square either). For $p = 2$ or $p \geq 7$, R has no roots ($\pm 1, \pm p, \pm p^2$ don't fit), so, is irreducible, and the Galois group is S_4.

For $p = 3$, $R(x) = (x - 3)(x^2 + 3x - 3)$, where the second factor is irreducible by Eisenstein's criterion; so, the group is either D_8 (if f is irreducible over $\mathbb{Q}(\sqrt{D})$) or $\mathbb{Z}_4$ (otherwise). We have $D = 3^2(256 \cdot 3 - 27 \cdot 9) = 3^2 5^2 21$, so $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{21})$. The ring S of integers of this field is a PID; 3 is not prime in S, it factorizes $3 = \pi\overline{\pi}$ where $\pi = \frac{\sqrt{21}+3}{2}$ and $\overline{\pi} = \frac{\sqrt{21}-3}{2}$. But the elements π and $\overline{\pi}$ are already prime (their norms $N(\pi), N(\overline{\pi}) = -3$ are prime) and non-associate ($\frac{\pi}{\overline{\pi}} = \frac{\sqrt{21}+3}{\sqrt{21}-3} = \frac{(\sqrt{21}+3)^2}{18} \notin R$), thus $f(x) = x^4 + \pi\overline{\pi}x + \pi\overline{\pi}$ is irreducible by Eisenstein's criterion. Hence, the Galois group of f is D_8.

For $p = 5$, $R(x) = (x - 5)(x^2 + 5x - 5)$, where, again, the second factor is irreducible by Eisenstein's criterion. Now, $D = 55^2 \cdot 5$, so $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{5})$. This time f splits

$$f(x) = \left(x^2 + \sqrt{5}x + \tfrac{5-\sqrt{5}}{2}\right)\left(x^2 - \sqrt{5}x + \tfrac{5+\sqrt{5}}{2}\right)$$

over $\mathbb{Q}(\sqrt{5})$ (it is a separate question how to find this decomposition), so the group is $\mathbb{Z}_4$.

19. *Find the Galois group of $f = x^5 - x - 1 \in \mathbb{Q}[x]$.*

Solution. Modulo 2, f splits as $(x^3 + x^2 + 1)(x^2 + x + 1)$. So, the Galois group G contains a permutation σ of the cycle type $(3, 2)$. σ^3 is a transposition, so G contains a transposition. Modulo 3, f is irreducible, so $|G|$ is divisible by 5, so G contains a 5-cycle. Hence, $G \cong S_5$.