Algebraic Structures II (80446)

The Hebrew University of Jerusalem Department of Mathematics

Solutions of practical questions of the training exam.

Part b.

1. If L/K is a finite separable extension, then there are finitely many intermediate fields between K and L.

Yes. By the primitive element theorems, L/K is simple, and hence has finitely many intermediate fields.

2. If L, F are finite extensions of a field K, then $[LF : F]$ divides $[L : K]$.

No. The standard bad example works here: $K = \mathbf{Q}$, $L = \mathbf{Q}(2^{1/3})$, $F = \mathbf{Q}(\xi_3 2^{1/3})$. Then $[LF : K] = 6$, $[L : K] = [F : K] = 3$ and $[LF : F] = [LF : L] = 2$.

3. If p, q are prime numbers and K is the splitting field of $x^q - p$ over $\mathbf{Q}$, then $[K : \mathbf{Q}] = p(q-1)$.

No. This is the compositum of $\mathbf{Q}(\xi_q)/\mathbf{Q}$, whose degree is $q-1$, and $\mathbf{Q}(p^{1/q})/\mathbf{Q}$, whose degree is q, since $x^q - p$ is irreducible by Eisenstein. So, $[K : \mathbf{Q}] = q(q-1)$.

4. One can construct the right polygon with 51 edges using compass and straightedge.

Yes, 51 is the product of two distinct Fermat's primes, 3 and 17.

5. If $x, y \in \mathbf{C}$ are such that $\text{tr.deg.}(\mathbf{Q}(x)/\mathbf{Q}) = \text{tr.deg.}(\mathbf{Q}(y)/\mathbf{Q}) = 1$, then $\text{tr.deg.}(\mathbf{Q}(x,y)/\mathbf{Q}) = 2$.

No. Take $x = y$ transcendental over $\mathbf{Q}$, then $\text{tr.deg.}(\mathbf{Q}(x,y)/\mathbf{Q}) = 1$. (If you do not like $x = y$, the choice of $x = y + 1$ or $x = y^2 - y^3$ also will do the job.)

Part c (16 points each problem, total 48 points). Solve three from the following four problems. Explain your solution; any result proved in class can be used, once you state it clearly.

1. Show that the polynomial $f(x) = x^5 - 4x + 2$ can not be solved in radicals over $\mathbf{Q}$.

The Galois group is S_5, by the same solution as studied on recitation. Namely, G_f has an element of order 5 by Cauchy's theorem, and since f has three real roots and two complex, the complex conjugation acts as a transposition. Any two such elements generate S_5. Since S_5 is not solvable, the equation is not solvable by radicals by Galois theorem.

2. Prove that if K is of characteristic $p > 2$ and $K(a)/K$ is an inseparable extension, then the extension $K(a^2)/K$ is inseparable too.

Clearly $a \neq 0$, and hence $f(x) = x^2 - a^2$ has two distinct roots $\pm a$ (as $\text{char}(K) \neq 2$). In particular, $f(x)$ is separable, and hence the extension $K(a)/K(a^2)$ is separable. If $K(a^2)/K$ is separable, then by the transitivity of separable extensions applied to the tower $K(a)/K(a^2)/K$, the extension $K(a)/K$ would be separable. A contradiction.

3. Let $\xi = \xi_7$ be the primitive root of unity of order 7. Assume one is given the complex plane $\mathbf{C}$ with marked points 0 and 1. Show that the point $\xi + \xi^6$

cannot be constructed by compass and straightedge, and the point $\xi + \xi^2 + \xi^4$ can be constructed by compass and straightedge.

If $K = \mathbf{Q}(\xi)$ then by the theorem about cyclotomic extensions of $\mathbf{Q}$, $G = G_{K/\mathbf{Q}} = (\mathbf{Z}/7\mathbf{Z})^\times$ is a cyclic group of order 6 acting by $i(\xi) = \xi^i$ for $1 \le i \le 6$. Subgroups of order 2 and 3 in G are $H_2 = \{\pm 1\}$ and $H_3 = \{1, 2, 4\}$. The field $K_3 = K^{H_3}$ is quadratic over $\mathbf{Q}$ because $[K_3 : \mathbf{Q}] = 6/|H_3| = 6/3 = 2$. Therefore, any its element can be constructed by compass and straightedge, and it remains to note that $\xi + \xi^2 + \xi^4 = \mathrm{Tr}_{K/K_3}(\xi) \in K_3$.

It remains to show that $a = \xi + \xi^6 = \xi + \xi^{-1}$ is not constructible. Since $\xi^2 - a\xi + 1 = 0$ and ξ is of degree 6 over $\mathbf{Q}$, we definitely have that $a \notin \mathbf{Q}$. On the other hand, $a = \mathrm{Tr}_{K/K_2}(\xi)$ where $K_2 = K^{H_2}$, and $[K_2 : \mathbf{Q}] = 6/|H_2| = 3$. So, K_2 contains no intermediate fields and we obtain that a generates K_2 and hence is of degree 3 over $\mathbf{Q}$. Therefore, a cannot be embedded in a Galois extension of $\mathbf{Q}$ of degree 2^n, and hence is not constructible by compass and straightedge.

4. For a prime number $p \neq 3$ let K_p denote the splitting field of $x^9 - 1$ over $\mathbf{F}_p$. Find the list of all possible Galois groups $G_{K_p/\mathbf{F}_p}$, and specify one concrete p for each group in your list.

The splitting field is $K_p = \mathbf{F}_p(\xi_9)$, hence by the theorem on cyclotomic extensions $G \subseteq (\mathbf{Z}/9\mathbf{Z})^\times = \mathbf{Z}/6\mathbf{Z}$. So, $G = \mathbf{Z}/n\mathbf{Z}$ is cyclic of order $n = 1, 2, 3, 6$. Now, the order n of G is precisely the minimal number such that $\mathbf{F}_{p^n}$ contains ξ_9, that is n is minimal such that $9|(p^n - 1)$. A simple search shows that $n = 6$ for $p = 2$ (since $2^2 - 1$ and $2^3 - 1$ are not divisible by 9), $n = 3$ for $p = 7$ (since $\xi_3 \in \mathbf{F}_7$, the extension is of degree 3), $n = 2$ for $p = 17$ (since $9|(p+1)$, we have $9|(p^2 - 1)$), and $n = 1$ for $p = 37$ (since $9|(p - 1)$).

Part d (10 points). Bonus problem.

1. a) (5 points) How many groups G with 81 elements exist so that the following is true: there exists a field K and an irreducible polynomial $f(x) \in K[x]$ of degree 10 such that G is the Galois group G_f of the splitting filed of f over K.

The answer is 0. If L is the splitting field of f and a is a root, then $[K(a) : K]$ divides $[L : K]$. Since f is irreducible, $[K(a) : K] = 10$ and we obtain that 10 divides $[L : K]$. So, $|G_f| = [L : K] \neq 81$.

An alternative solution in venue of (b) would be to say that G should be a Sylow subgroup of S_{10}. Such a subgroup is unique up to conjugation, and also S_9 contains a Sylow subgroup with 81 elements. So, a conjugate of G is contained in $S_9 \subset S_{10}$ and hence does not act transitively on the set of 10 roots. So, it cannot be a Galois group of an irreducible f of degree 10.

b) (5 points) How many groups G with 81 elements exist so that the following is true: there exists a field K and an irreducible polynomial $f(x) \in K[x]$ of degree 9 such that G is the Galois group G_f of the splitting filed of f over K.

The answer is 1. By a theorem on Galois groups, any such G can be embedded into S_9 so that it acts transitively on the 9 elements. The maximal power of 3 dividing $|S_9| = 9!$ is $3 * 3 * 9 = 81$. Hence G must be a Sylow 3-subgroup, which is unique up to a conjugation, hence also up to an isomorphism. Thus, there is at most one such group G – the 3-Sylow subgroup of S_9. Next, note that this $G \subset S_9$ acts transitively because it contains an element of order 9 – any such element lies in a Sylow 3-subgroup, and any element of order 9 is a cycle of length 9 in S_9.

Finally, such a G can indeed be realized as G_f. Indeed, take any L with $S_9 \subseteq \mathrm{Aut}(L)$. For example, $L = \mathbf{Q}(x_1, \ldots, x_9)$ with S_9 acting by permuting the x_i. Then $G \subset S_9$ acts on $x_1, \ldots, x_9$ transitively, hence $f(t) = (t-x_1)\ldots(t-x_9)$ is irreducible in $L^G[t]$, and by Artin's theorem $G = [L : L^G]$ is the Galois group of $f(t)$ over L^G.