

SOLUTIONS FOR THE FINAL EXAM, MATH 535

December 13, 2004

S. Katok

Instructions: Do Problem 1 and any three of Problems 2–6. If you solve more than three, the score will be counted as extra-credit. Each problem is 30 pts.

Problem 1 consists of 10 questions, I will add 3 pts for each correct answer and subtract 1 pt for each incorrect answer. There will be 0 pts if you leave a question not answered.

1. In TRUE/FALSE questions mark your answer; in other questions give an answer. Explanations are optional.

1.1. The equation $x^6 + 2x^3 + 1 = 0$ over \mathbb{Q} is solvable by radicals.

TRUE	FALSE
T	

$x^6 + 2x^3 + 1 = (1 + x^3)^2$, hence the splitting field is $\mathbb{Q}(\omega)$, where ω is a primitive 3^{rd} root of unity, and $\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ is a radical extension.

1.2. Find the Galois group G of the polynomial $x^5 + 6x^3 + 9x \in \mathbb{Q}[x]$.

The polynomial is reducible: $x^5 + 6x^3 + 9x = x(x^2 - 3)^2$. Hence $G \cong \mathbb{I}_2$.

1.3. Galois group of any irreducible cubic equation with three real roots is \mathbb{I}_3 .

TRUE	FALSE
	F

$G \cong A_3 \cong \mathbb{I}_3$ iff the discriminant is a square.

1.4. The zeros in \mathbb{C} of $(x^{28} - 1) \in \mathbb{Q}[x]$ form a cyclic group by multiplication.

TRUE	FALSE
T	

The zeros are 28^{th} roots of unity. The group is generated by $e^{2\pi i/28}$.

1.5. $\mathbb{Q}(\sqrt{5}, i)$ is a normal extension of \mathbb{Q} .

TRUE	FALSE
T	

It is a splitting field of $(x^2 - 5)(x^2 + 1)$, hence, by a Theorem proved in class, a normal extension.

1.6. The group U_n of units modulo n is cyclic.

TRUE	FALSE
	F

U_8 is V while U_{10} is cyclic of order 4.

1.7. For α and β algebraic over a field F , there is always an isomorphism of $F(\alpha)$ onto $F(\beta)$.

TRUE	FALSE
	F

If degrees of minimal polynomials of α and β are not equal such isomorphism does not exist. Even if the degrees coincide, an isomorphism does not have to exist, e.g. $\mathbb{Q}(\sqrt{2})$ is not isomorphic to $\mathbb{Q}(\sqrt{3})$, as has been shown in class.

1.8. Every field is a PID.

TRUE	FALSE
T	

The only ideals in a field F are $\{0\}$ and F itself, which are principal.

1.9. The group of units of any finite field is cyclic.

TRUE	FALSE
T	

Theorem 3.30.

1.10. Every extension of a field of a positive characteristic is separable.

TRUE	FALSE
	F

A classical counter-example: $k = \mathbb{F}_p(t) = \text{Frac}(\mathbb{F}_p[t])$, $E = k(\alpha)$ where α is a root of $f(x) - x^p - t$ irreducible, but $f(x) = (x - \alpha)^p$. This is Example 4.5 from the book.

2. Identify the Galois group of the polynomial $f(x) = x^5 - 6x^4 + 3$ over F , when

- (1) $F = \mathbb{Q}$ and when
- (2) $F = \mathbb{F}_2$.

Solution. (1) The polynomial is irreducible by Eisenstein for $p = 2$ and has exactly 2 non-real roots by consideration of its derivative, hence $G = \text{Gal}(E/F) \cong S_5$ with generators (12) and (12345). (2) If $F = \mathbb{F}_2$, $f(x) = x^5 - 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$, the 5th cyclotomic polynomial. By Prop. 4.11 $G = \text{Gal}(E/F)$ is a subgroup of U_5 , a cyclic group of order 4, so $\text{Gal}(E/F)$ is cyclic and $|G| \leq 4$. We also know that since $2 = \text{char}(F)$ does not divide the degree of the cyclotomic polynomial, 5, $f(x)$ has no repeated roots (Example 4.6). But the second factor $x^4 + x^3 + x^2 + x + 1$ is irreducible since it does not have roots in \mathbb{F}_2 and is not a square of the only irreducible quadratic in $\mathbb{F}_2[x]$, $x^2 + x + 1$. Therefore, E is the splitting field of the separable polynomial $x^4 + x^3 + x^2 + x + 1$, and by Corollary 4.9, $4 \mid |G|$, which implies that $|G| \geq 4$. Thus $G \cong \mathbb{I}_4$, cyclic of order 4. Another way to see that $G \cong \mathbb{I}_4$ is the following. E is a splitting field of an irreducible polynomial $x^4 + x^3 + x^2 + x + 1$ (prove the irreducibility as above), and $E = F(\omega)$, where ω is a 5th roots of unity (since the 5th roots of unity form a multiplicative group). Then

$$E = \mathbb{F}_2[x]/(x^4 + x^3 + x^2 + x + 1) = \mathbb{F}_{2^4},$$

hence $[E : F] = 4$, and by Prop. 4.7(ii) $|G| = 4$. It is cyclic since the \mathbb{F}_{2^4} has only one subfield F' with $[\mathbb{F}_{2^4} : F'] = 2$, $F' = \mathbb{F}_{2^2}$.

3. Let F be a field of 81 elements. For each of the following polynomials $g(x)$ determine the number of roots of $g(x)$ that lie in F : $x^{80} - 1$, $x^{81} - 1$, $x^{88} - 1$.

Solution. Notice that $x = 0$ does not satisfy any of these equations. The group F^\times is cyclic of order 80. Hence $x^{80} - 1 = 0$ for all $x \in F^\times$. Hence $x^{80} - 1$ has 80 roots in F . $x^{81} = x^{80}x = x$, hence $x^{81} - 1$ has only one solution $x = 1$. Similarly, $x^{88} = x^{80}x^8 = x^8$. Hence the set of roots of $x^{88} - 1$ in F coincides with the set of roots of $x^8 - 1$ in F . Let a be a generator of F^\times , then $\langle a^{10} \rangle \leq F^\times$ is a cyclic subgroup of order 8 all elements of which are the roots of $x^8 - 1$. Since $x^8 - 1$ has at most 8 roots in F by Theorem 3.25, we have found all of them, Therefore $x^{88} - 1$ has 8 roots in F .

4. Let G be the Galois group of the polynomial $x^5 - 2$ over \mathbb{Q} .

- (1) Determine the order of G .
- (2) Determine whether G is abelian.
- (3) Determine whether G is solvable.

Solution. Let $\alpha = \sqrt[5]{2}$, and θ be a primitive 5th root of unity, then $E = \mathbb{Q}(\alpha, \theta)$ is a splitting field of $x^5 - 2$ over \mathbb{Q} . (1) By the Tower Theorem we have

$$[\mathbb{Q}(\alpha, \theta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \theta) : \mathbb{Q}(\theta)][\mathbb{Q}(\theta) : \mathbb{Q}] = 5 \times 4 = 20,$$

where $[\mathbb{Q}(\theta) : \mathbb{Q}] = 4 = \varphi(5)$, the degree of the 5th cyclotomic polynomial, and $[\mathbb{Q}(\alpha, \theta) : \mathbb{Q}(\theta)] = 5$ since $x^5 - 2$ is irreducible over $\mathbb{Q}(\theta)$, which follows from Prop. 3.126 since $x^5 - 2$ does not have a root in $\mathbb{Q}(\theta)$. Therefore the order of G is 20 by Prop. 4.7(ii). (2) The generators are $\sigma = (12345)$ and $\tau = (2354)$, where $\sigma(\alpha) = \theta\alpha$ and $\tau(\theta) = \theta^2$. G is non-abelian since the generators do not commute. Another way to see this: since $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not normal, by FTGT it corresponds a subgroup $H < G$ which is not normal, but in an abelian group all subgroups are normal. (3) Solvable. The equation $x^5 - 2 = 0$ is solvable by radicals over \mathbb{Q} since E/\mathbb{Q} is a radical extension with $n = 5$ with

$$\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq \mathbb{Q}(\alpha, \theta) = E.$$

Hence by Galois' Solvability Theorem the Galois group is solvable. Another way to see this is to notice that all groups of order < 60 are solvable, the unsolvable group of order 60 being A_5 , although I did not mentioned this particular statement in class.

5. How many irreducible factors does $x^{255} - 1 \in \mathbb{Q}[x]$ have and what are their degrees?

Solution. We proved that

$$x^{255} - 1 = \prod_{d|255} \Phi_d = \Phi_1 \Phi_3 \Phi_5 \Phi_{15} \Phi_{17} \Phi_{51} \Phi_{85} \Phi_{255}.$$

Their degrees are 1, 2, 4, 8, 16, 32, 64, 128.

6. Show that there is an isomorphism from the ring $R = \mathbb{Q}[x]/(x^3 - 6x - 6)$ onto the field $\mathbb{Q}(\sqrt[3]{2})$ which takes $[x]$ to $\sqrt[3]{2} + \sqrt[3]{4}$.

Solution. First, notice that $x^3 - 6x - 6$ is Eisenstein with $p = 2$ hence irreducible, hence R is a field. Let $a_1 = [x] \in R$, then $R = \mathbb{Q}(a_1)$ and the minimal polynomial for a_1 is $x^3 - 6x - 6$. Second $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ since $x^3 - 2$ is irreducible. Let $a_2 = \sqrt[3]{2} + \sqrt[3]{4}$. Then $a_2 \in \mathbb{Q}(\sqrt[3]{2})$ and $a_2 \notin \mathbb{Q}$ as $1, \sqrt[3]{2}, \sqrt[3]{4}$ are linearly independent. Hence $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(a_2)$ as $[\mathbb{Q}(a_2) : \mathbb{Q}] > 1$ and must divide 3. Third, $a_2^3 = 6 + 6a_2$, hence a_2 satisfies $x^3 - 6x - 6 = 0$. Thus by the First isomorphism theorem for rings, there is an isomorphism from R onto $\mathbb{Q}(a_2)$ which takes a_1 to a_2 .