

MATH 123: ABSTRACT ALGEBRA II
SOLUTION SET # 11

GREGG MUSIKER

1. CHAPTER 14, SECTION 1

Problem 1 Determine the irreducible polynomial for $\alpha = i + \sqrt{2}$ over \mathbb{Q} .

There were several ways to do this problem. The basic idea is to find a linear combination of powers of α that equals zero. Then one needs to explain why the associated polynomial is irreducible.

$\alpha^2 = -1 + 2\sqrt{-2} + 2 = 1 + 2\sqrt{-2}$. Thus $(\alpha^2 - 1)^2 = -8$ hence α satisfies $(x^2 - 1)^2 + 8 = x^4 - 2x^2 + 9 = f(x)$. It is probably easiest to prove that this is irreducible by the theory of field extensions (rather than the tricks from chapter 11). Namely, let K be the splitting field for $f(x)$. $\mathbb{Q}(\sqrt{2}, i)$ contains K . $\mathbb{Q}(\sqrt{2})$ has degree 2 over \mathbb{Q} and since $i \notin \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i, \sqrt{2})$ has degree 2 over $\mathbb{Q}(\sqrt{2})$. Consequently, $K = \mathbb{Q}(\sqrt{2}, i)$, $[K : \mathbb{Q}] = 4$ and $f(x)$ is irreducible.

Problem 6 Determine the degree of the splitting field of the following polynomials over \mathbb{Q} .

a) $x^4 - 1$. One can quickly recognize the roots ± 1 and/or that $x^4 = 1$ means the fourth roots of unity will be the roots of this polynomial. Hence $x^4 - 1 = (x - 1)(x - i)(x + 1)(x + i)$ so the splitting field is $\mathbb{Q}(i)$ which has degree 2 over \mathbb{Q} since i satisfies the irreducible polynomial $x^2 + 1$.

b) $x^3 - 2$. $\alpha = \sqrt[3]{2}$ is clearly a root of $x^3 - 2$. Then after factoring and applying quadratic formula (if needed) one factors $x^3 - 2$ as $x^3 - 2 = (x - \alpha)(x - \alpha\zeta)(x - \alpha\zeta^2)$ where ζ is a complex cube root of unity. $\zeta^2 + \zeta + 1 = 0$ and $\zeta \notin \mathbb{R}$ hence $\zeta \notin \mathbb{Q}(\alpha)$ so the splitting field of $x^3 - 2$ has degree $3 \cdot 2 = 6$. In fact the splitting field is $\mathbb{Q}(\alpha, \zeta)$.

c) $x^4 + 1$. This polynomial has the fourth roots of (-1) as roots thus “ $\pm\sqrt{\pm i}$ “, better known as $\frac{\pm\sqrt{2} \pm i\sqrt{2}}{2}$ are the four roots of $x^4 + 1$. The splitting field will contain both i and $\sqrt{2}$ and similar to the reasoning in problem 1, we can claim that the degree of the splitting field is 4.

Problem 8 Let $\zeta = e^{2\pi i/5}$.

a) Prove that $K = \mathbb{Q}(\zeta)$ is a splitting field for the polynomial $x^5 - 1$ over \mathbb{Q} , and determine the degree $[K : \mathbb{Q}]$.

$\zeta^5 - 1 = 0$ by inspection, and in fact $x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1) = (x - 1)(x - \zeta)(x - \zeta^2)(x - \zeta^3)(x - \zeta^4)$. Thus K is $x^5 - 1$'s splitting field, and since $\zeta \neq 1$, ζ is the root of an irreducible (cyclotomic polynomial) polynomial of degree 4. Hence $[K : \mathbb{Q}] = 4$.

b) Without using Theorem (1.11), prove that K is a Galois extension of \mathbb{Q} , and determine its Galois group.

Let σ_i send ζ to ζ^i . Then $\sigma_1, \dots, \sigma_4$ are all automorphisms of K . Since $|\text{Aut}(K/\mathbb{Q})| = 4 = [K : \mathbb{Q}]$, K/\mathbb{Q} is Galois, and the Galois group is $\mathbb{Z}/4\mathbb{Z}$. Notice $\sigma_2^4 = \sigma_1(16) = \sigma_3(8)\sigma_2 = \sigma_4^2$ thus $\text{Gal}(K/\mathbb{Q})$ is of order 4 and has an element of order 4 thus it cannot be V_4 and must be $\mathbb{Z}/4\mathbb{Z}$.

Problem 12 Determine all automorphisms of the field $\mathbb{Q}(\sqrt[3]{2})$.

From class we saw that if $f(\alpha) = 0$, then the automorphisms of $\mathbb{Q}(\alpha)$ send α to another root of $f(x)$. This is true if we let $\alpha = \sqrt[3]{2}$. But the other roots are $\beta = \alpha\zeta$ and $\gamma = \alpha\zeta^2$, both which are not real. Thus an automorphism of $\mathbb{Q}(\alpha)$ cannot send α to β nor γ , thus the only possible automorphism is the identity map.

This highlights the importance of an extension being Galois. $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not Galois because $\mathbb{Q}(\alpha)$ is not a splitting field for any polynomial in \mathbb{Q} . As we saw in problem 6, α is a root of $x^3 - 2$ whose splitting field has degree 6 over \mathbb{Q} .

Problem 13 Let K/F be a finite extension. Prove that the Galois group $\text{Gal}(K/F)$ is a finite group.

To make this easiest to explain, we will assume that F has characteristic zero, and apply theorem 14.4.1, the primitive element theorem. Thus $\exists \alpha \in K$ such that $K = F(\alpha)$ since $[K : F]$ finite (without char zero and the primitive element theorem, $K = F(\alpha_1, \dots, \alpha_n)$ we just pick $\alpha \in K$ which is a root of $f(x) \in F[x]$) and thus α is a root of polynomial $f(x)$ in $F[x]$ of degree $[K : F]$. Using the fact that an automorphism of K (that fixes field F) must send α to another root of $f(x) \in K$. But since the number of roots of $f(x)$ which lie in $K \leq [K : F]$, the automorphism group must also be finite. In fact the group will be a subgroup of the symmetric group $S_{[K:F]}$ since the automorphisms will permute the roots.

Problem 14 Determine all the quadratic number fields $\mathbb{Q}(\sqrt{d})$ which contain a primitive p th root of unity, for some prime $p \neq 2$.

Let $\zeta \neq 1$ satisfy $x^p - 1 = 0$. $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ since this is a cyclotomic extension. If $\zeta \in \mathbb{Q}(\sqrt{d})$, this implies we can create a tower:

$$\begin{array}{c} \mathbb{Q}(\sqrt{d}) \\ | \\ \mathbb{Q}(\zeta) \\ | \\ \mathbb{Q} \end{array}$$

$[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ so the only way this tower can occur is if $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\zeta)$, $p = 3$. In fact $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ but this is the only time that a quadratic number field contains a p th root of unity for $p > 2$.

Problem 15 Prove that every Galois extension K/F whose Galois group is the Klein four group is biquadratic.

By the main theorem, if the Galois group has three subgroups of index 2 (as the Klein 4 group does) then K contains three subfields containing F which have degree 2 over F . Let two of these subfields be $F(\beta)$ and $F(\gamma)$. Since these subfields are distinct and both have degree 2 over F , $\beta \notin F(\gamma)$ and $\gamma \notin F(\beta)$ but $\beta, \gamma \in K$. Thus $F(\beta, \gamma)$ has degree 2 over $F(\beta)$, $F(\beta, \gamma)$ has degree 4 over F and $K \supset F(\beta, \gamma)$ implies $K = F(\beta, \gamma)$. Thus K is the splitting field for $(x - \beta)(x + \beta)(x - \gamma)(x + \gamma)$ where $(x - \beta)(x + \beta)$ splits in $F(\beta)$ and $(x - \gamma)(x + \gamma)$ splits in $F(\gamma)$. Thus K/F is a biquadratic extension. *Note: the third subfield of degree 2 over F is $F(\beta\gamma)$.*

2. CHAPTER 14, SECTION 4

Problem 1 Let G be a group of automorphisms of a field K . Prove that the fixed elements K^G form a subfield of K .

K^G is defined as the set $\{x \in K : g(x) = x \text{ for all } g \in G\}$. Since K^G is a subset of a field, associativity, commutativity, and distribution will follow as long as K^G is closed under addition, subtraction, multiplication, and division. Note that being closed under subtraction implies the additive identity is in K^G and likewise for the multiplicative identity. Since $g \in G$ is an automorphism of K , $g(x+y) = g(x)+g(y)$, $g(0) = 0$, $g(1) = 1$, and $g(xy) = g(x)g(y)$. Assume $x, y \in K^G$. Then $g(x+y) = g(x) + g(y) = x + y$ and $g(xy) = g(x)g(y) = xy$. $g(-x) + x = g(-x) + g(x) = g(-x+x) = g(0) = 0$ implies $g(-x) = -x$. $g(1/x)g(x) = g(1) = 1$ implies $g(1/x) = 1/x$. Thus K^G is a subfield of K .

Problem 2 Let $\alpha = \sqrt[3]{2}$, $\zeta = \frac{-1+\sqrt{-3}}{2}$, $\beta = \alpha\zeta$.

a) Prove that for all $c \in \mathbb{Q}$, $\gamma = \alpha + c\beta$ is the root of a sixth-degree polynomial of the form $x^6 + ax^3 + b$.

Note that $\gamma = \alpha(1 + c\zeta)$. Thus $\gamma^3 = 2(1 + c\zeta)^3 \in \mathbb{Q}(\zeta)$. $\gamma^3 \notin \mathbb{Q}$ unless $c = 0$. Assume $c \neq 0$. Since $\mathbb{Q}(\zeta)$ has degree 2 over \mathbb{Q} (satisfies $x^2 + x + 1$), γ^3 must satisfy an equation of the form $y^2 + ay + b$. Consequently, γ satisfies $x^6 + ax^3 + b$. If $c = 0$ then $\alpha^6 = 4$ and α satisfies $x^6 - 4$.

Alternate proof². The field $K = \mathbb{Q}(\alpha, \beta)$ is the splitting field for $x^3 - 2$ over \mathbb{Q} . This extension has degree 6, its Galois group is S_3 , and the three roots of $x^3 - 2$ are α, β , and $\beta\zeta = \delta$. Thus the orbit of $\gamma = \alpha + c\beta$ under the group action of $\text{Gal}(K/\mathbb{Q})$ is the set $\{\alpha + c\beta, \beta + c\alpha, \alpha + c\delta, \delta + c\alpha, \beta + c\delta, \delta + c\beta\}$. Thus the irreducible polynomial for γ will divide

$$g(x) = [x - \alpha(1 + c\zeta)][x - \alpha(\zeta + c)][x - \alpha(1 + c\zeta^2)][x - \alpha(\zeta^2 + c)][x - \alpha(\zeta + c\zeta^2)][x - \alpha(\zeta^2 + c\zeta)].$$

We expand this expression to get $x^6 + ax^3 + b$ where $a = -4c^3 + 6c^2 + 6c - 4$ and $b = 4(c^2 - c + 1)^3$.

¹Thanks to Philip Zeyliger.

²Thanks to Noam Zeilberger.

To see this expansion, we note that $\zeta + \zeta^2 = -1$ and the constant term is the product of

$$\alpha^6[(1+c\zeta)(1+c\zeta^2)][(\zeta+c\zeta^2)(\zeta^2+c\zeta)][(\zeta^2+c)(\zeta+c)] = \\ \alpha^6[(1+c\zeta)(1+c\zeta^2)][\zeta(1+c\zeta)\zeta^2(1+c\zeta^2)][\zeta^2(1+c\zeta)\zeta(1+c\zeta^2)]$$

where each bracketed expression is equal to $1 - c + c^2$. One can show using the fact that $(\zeta^2 + \zeta + 1)x = 0$ that the degree five, four, two, and one terms are zero and the degree three term of the expansion is as above.

Yet another proof. Many people solved this problem using the following method:

$\gamma^6 = c_1 + c_2\zeta + c_3\zeta$. Some people noticed that one can rewrite this as $\gamma^6 = d_1 + d_2\zeta$ or $d_1 + d_3\zeta^2$ since $\zeta + \zeta^2 = -1$. (Here the coefficients are all rational.) Using this and the fact that $\gamma^3 = e_1 + e_3\zeta^2$, one finds that $\gamma^6 - d_3/e_3\gamma^3$ is rational. $e_3 \neq 0$ unless $c = 0$ a case which implies $\gamma^6 = 4$.

b) *Prove that the irreducible polynomial for $\alpha + \beta$ is a cubic.*

Here, I will use Noam's observation that $\alpha + c\beta$ satisfies $x^6 + ax^3 + b$ where $a = -4c^3 + 6c^2 + 6c - 4$ and $b = 4(c^2 - c + 1)^3$. (Alternatively, one can just show through explicit computation that $\alpha + \beta$ satisfies the cubic $x^3 - 2$.) Since $c = 1$, $\alpha + \beta$ satisfies $x^6 + 4x^3 + 4$ which factors as $(x^3 - 2)^2$.

c) *Prove that $\alpha - \beta$ has degree 6 over \mathbb{Q} .*

Proving this amounts to proving that $\alpha - \beta$ is a primitive element for the splitting field of $x^3 - 2$. Thus letting $a_i, b_i \in \{\alpha, \alpha\zeta, \alpha\zeta^2\}$, we form the quotients $\frac{a_i + \alpha}{b_j - \beta}$ for $i \neq j$ like on page 553. None of these equal -1 so $\alpha - \beta$ is the primitive element.