MATH 201, Algebra II, Final (March 12, 1999)

(Winter 1999, R. Boltje)

1. Find an element $\alpha \in \mathbb{C}$ such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension of degree 3.

2. Find an element $\alpha \in \mathbb{C}$ such that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$. Is $\mathbb{Q}(\alpha)/\mathbb{Q}$ a Galois extension? Compute all subfields of $\mathbb{Q}(\alpha)$.

3. Let $\bar{\mathbb{Q}}$ be the set of all complex numbers which are algebraic over $\mathbb{Q}$.
(a) Show that $\bar{\mathbb{Q}}$ is a subfield of $\mathbb{C}$ containing $\mathbb{Q}$.
(b) Show that $\bar{\mathbb{Q}}$ is algebraically closed.
($\bar{\mathbb{Q}}$ is called the *field of algebraic numbers.*)

4. Construct a finite field with 27 elements and find a nonzero element of maximal multiplicative order.

5. Let p be a prime and let F be a field with p^{25} elements. Does F contain a subfield with p^{10} elements?

6. Is the Galois group of $f(X) = X^4 - 2$ over $\mathbb{Q}$ abelian?

7. Let $\zeta := e^{2\pi i/7} \in \mathbb{C}$. Is $\sqrt{7}i \in \mathbb{Q}(\zeta)$?

Solutions

1. and **7.** It is not easy to write down a Galois extension of degree 3 over $\mathbb{Q}$ directly. But we can easily find a Galois extension $E/\mathbb{Q}$ with abelian Galois group of order 6, namely $E = \mathbb{Q}(\zeta)$ with $\zeta := e^{2\pi i/7}$: We have $G := \mathrm{Gal}(E/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times$ which is a cyclic group of order 6. The subgroup $\{1 + 7\mathbb{Z}, -1 + 7\mathbb{Z}\}$ of $(\mathbb{Z}/7\mathbb{Z})^\times$ corresponds to a Galois extension $F/\mathbb{Q}$ of degree $6/2 = 3$, since every subgroup of G is normal in G. The element $1 + 7\mathbb{Z}$ corresponds to the identity of E and $-1 + 7\mathbb{Z}$ corresponds to the automorphism $\tau\colon E \to E$ with $\tau(\zeta) = \zeta^{-1}$. Obviously, $\alpha := \zeta + \zeta^{-1}$ is fixed by τ. Therefore, $\alpha \in F$. If we can show that $\alpha \notin \mathbb{Q}$, we have $F = \mathbb{Q}(\alpha)$, since $[F : \mathbb{Q}] = 3$ is a prime. But if $\zeta + \zeta^6 = \alpha \in \mathbb{Q}$, we can replace ζ^6 using $1 + \zeta + \zeta^2 + \cdots + \zeta^6 = 0$ (remember $\Phi_7 = 1 + X + \cdots + X^6$) and obtain $(a + 1) + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 = 0$ which is impossible, since $1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5$ are a $\mathbb{Q}$-basis of E.

Since $\mathrm{Gal}(E/\mathbb{Q})$ is a cyclic group of order 6, it has exactly one subgroup of order 3, and therefore, there exists exactly one intermediate field M in $E/\mathbb{Q}$ with $[M : \mathbb{Q}] = 2$. Therefore, $\sqrt{7}i \in E$ if and only if $\mathbb{Q}(\sqrt{7}i) = M$. We will compute M. The subgroup of order three in $\mathrm{Gal}(E/\mathbb{Q})$ is obviously given by $\{\sigma_1, \sigma_2, \sigma_4\}$, where $\sigma_i(\zeta) = \zeta^i$ for $i = 1, \ldots, 6$. One can easily find an element which is fixed under these three automorphisms. For example $\beta := \zeta + \zeta^2 + \zeta^4$ has this property.

Moreover, since $1, \zeta, \zeta^2, \zeta^4$ are $\mathbb{Q}$-linearly independent, $\beta \notin \mathbb{Q}$. Next we determine the minimal polynomial of β over $\mathbb{Q}$, which has to be a polynomial of degree 2. From this we should be able to decide, if $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{7}i)$. Using the relation $\zeta^6 = -(1 + \zeta + \cdots + \zeta^5)$, we obtain $\beta^2 = -2 - \zeta - \zeta^2 - \zeta^4 = -2 - \beta$. Therefore, β is a root of the polynomial $X^2 + X + 2$. But we can easily determine its roots by the well-known formula as $(-1 \pm \sqrt{1 - 4 \cdot 2})/2 = (-1 \pm \sqrt{7}i)/2$. Therefore, $2\beta = -1 + \sqrt{7}i$ or $2\beta = -1 - \sqrt{7}i$. This implies $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{7}i)$ and $\sqrt{7}i \in E$.

Remark: One can actually show in general, that if p is an odd prime, then the unique quadratic subfield in the cyclotomic extension $\mathbb{Q}_p/\mathbb{Q}$ is given by $\mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \mod 4$ and by $\mathbb{Q}(\sqrt{p}i)$ if $p \equiv 3 \mod 4$.

2. Obviously, $E := \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field of the polynomial $f(X) := (X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$ over $\mathbb{Q}$. Since $\mathbb{Q}$ has characteristic 0, $f(X)$ is separable over $\mathbb{Q}$. This implies that $E/\mathbb{Q}$ is a Galois extension. Since $\sqrt{2} \notin \mathbb{Q}$, and since $\sqrt{2}$ is a root of the polynomial $X^2 - 2$ of degree 2, $F_1 := \mathbb{Q}(\sqrt{2})/\mathbb{Q}$ has degree 2. We claim that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Assume that $\sqrt{3} = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$. Then $\sqrt{3} - a = b\sqrt{2}$ and squaring both sides gives $3 + a^2 - 2a\sqrt{3} = 2b^2$. But since $\sqrt{3} \notin \mathbb{Q}$, this implies $a = 0$. Therefore, $\sqrt{3} = b\sqrt{2}$. Multiplication by $\sqrt{2}$ gives $\sqrt{6} = 2b \in \mathbb{Q}$ which is a contradiction. Therefore $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ and $[E : F_1] = 2$. Altogether we have $[E : \mathbb{Q}] = [E : F_1][F_1 : \mathbb{Q}] = 2 \cdot 2 = 4$. Therefore $G := \mathrm{Gal}(E/\mathbb{Q})$ has order 4. All groups of order 4 are abelian. There are two possibilities: Either $G \cong \mathbb{Z}/4\mathbb{Z}$ or $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If G is cyclic of order 4 then G would have only one subgroup of order 2 and therefore, $E/\mathbb{Q}$ would have just one intermediate field of degree 2 over $\mathbb{Q}$. But besides $F_1 = \mathbb{Q}(\sqrt{2})$ we immediately see the intermediate field $F_2 := \mathbb{Q}(\sqrt{3})$ of degree 2 over $\mathbb{Q}$. Therefore, $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This group has 3 subgroups of order 2 (anyone of the non-identity elements together with the identity). Therefore, E/F has a third intermediate field F_3 with $[F_3 : \mathbb{Q}] = 2$, and no more.

Besides the identity map there are three more elements in G. Since $E = F_1(\sqrt{3})$, $H_1 := \mathrm{Gal}(E/F_1) = \{1, \sigma_1\}$ with $\sigma_1(\sqrt{2}) = \sqrt{2}$ and $\sigma_1(\sqrt{3}) = -\sqrt{3}$. Similarly, since $E = F_2(\sqrt{2})$, $H_2 := \mathrm{Gal}(E/F_2) = \{1, \sigma_2\}$ with $\sigma_2(\sqrt{2}) = -\sqrt{2}$ and $\sigma_2(\sqrt{3}) = \sqrt{3}$. Since H_1 and H_2 are subgroups of G, $\sigma_1, \sigma_2 \in G$. Moreover, $\sigma_3 := \sigma_1 \circ \sigma_2$ has the properties $\sigma_3(\sqrt{2}) = -\sqrt{2}$ and $\sqrt{3} = -\sqrt{3}$, which shows that the four elements $1, \sigma_1, \sigma_2, \sigma_3$ are pairwise distinct and form the group G. Obviously $\sqrt{6} = \sqrt{2}\sqrt{3} \in E$ and $\sigma_3(\sqrt{6}) = \sqrt{6}$. Therefore, $F_3 := \mathbb{Q}(\sqrt{6})$ is the missing intermediate field

In order to find an element α with $E = \mathbb{Q}(\alpha)$, we only have to find an element $\alpha \in E$ which is not contained in any of the three subfields F_1, F_2, F_3. Therefore, it suffices to find an element $\alpha \in E$ such that $\sigma_i(\alpha) \neq \alpha$ for all $i = 1, 2, 3$. The element $\alpha := \sqrt{2} + \sqrt{3}$ obviously satisfies these conditions.

3. (a) If $a \in \mathbb{Q}$, then a is a root of the polynomial $X - a \in \mathbb{Q}[X]$ and therefore is algebraic over $\mathbb{Q}$. This shows, that $\bar{\mathbb{Q}}$ contains $\mathbb{Q}$. If a and b are in $\bar{\mathbb{Q}}$, then $\mathbb{Q}(a)/\mathbb{Q}$ is a finite field extension, and also $\mathbb{Q}(a, b)/\mathbb{Q}(a)$ is a finite field extension, because b is also algebraic over $\mathbb{Q}(a)$, if it is over $\mathbb{Q}$. Therefore $\mathbb{Q}(a, b)/\mathbb{Q}$ is finite. This implies that $\mathbb{Q}(a, b)/\mathbb{Q}$ is an algebraic field extension. In particular, $a + b$, $a - b$, and ab are in $\mathbb{Q}(a, b)$ and therefore algebraic over $\mathbb{Q}$. Also, if $a \neq 0$, $a^{-1} \in \mathbb{Q}(a)$

and therefore is algebraic over $\mathbb{Q}$. This shows that $a \pm b, ab, a^{-1} \in \bar{\mathbb{Q}}$ and that $\bar{\mathbb{Q}}$ is a subfield of $\mathbb{Q}$.

(b) Let $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \bar{\mathbb{Q}}[X]$ be a polynomial which is not constant. We will show that f has a root in $\bar{\mathbb{Q}}$. Since $\mathbb{C}$ is algebraically closed, f has a root α in $\mathbb{C}$. Consider the field $F := \mathbb{Q}(a_1, \ldots, a_n)$. Since $a_1, \ldots, a_n$ are algebraic over $\mathbb{Q}$, $F/\mathbb{Q}$ is a finite field extension and $f \in F[X]$. Since α is a root of f, $F(\alpha)/F$ is algebraic and finite. Therefore also $F(\alpha)/\mathbb{Q}$ is finite. This implies that α is algebraic over $\mathbb{Q}$ and therefore already in $\bar{\mathbb{Q}}$.

4. Let $F := \mathbb{Z}/3\mathbb{Z}$. Then F is a field with 3 elements. We want to find an irreducible polynomial $f(X) \in F[X]$ of degree 3. To check that such a polynomial is irreducible, it suffices to check that it has no root in F. We try $f(X) = \bar{1} - X + X^3$ and find $f(\bar{0}) = \bar{1}$, $f(\bar{1}) = \bar{1}$, and $f(\bar{2}) = \bar{1}$. Therefore, $f(X)$ is irreducible in $F[X]$ and $E := F[X]/(f(X))$ is a field with $3^3 = 27$ elements. We set $a := \bar{X} = X + (f(X)) \in E$. Then $\bar{1}, a, a^2$ is an F-basis of E and we have $a^3 = a - \bar{1}$. $E^\times$ is a cyclic group with 26 elements. Every element in $E^\times$ has order $1, 2, 13$, or 26. We consider for example a. We have $a \neq 1$, $a^2 \neq 1$, and $a^{13} = a^8 a^4 a$ with $a^4 = a(a - \bar{1}) = a^2 - a$ and $a^8 = (a^2 - a)^2 = a^4 - \bar{2}a^3 + a^2 = (a^2 - a) - \bar{2}(a - \bar{1}) + a^2 = \bar{2}a^2 + \bar{2}$. This gives $a^{12} = a^8 a^4 = (\bar{2}a^2 + \bar{2})(a^2 - a) = \bar{2}a^4 + a^3 + \bar{2}a^2 + a = \bar{2}(a^2 - a) + (a - \bar{1}) + \bar{2}a^2 + a = a^2 + \bar{2}$, and $a^{13} = a^{12}a = (a^2 + \bar{2})a = a^3 - a = -\bar{1}$. Since a has neither order 1, nor 2, nor 13, it has to have order 26 in $E^\times$.

5. If F had a subfield F_0 of order p^{10}, then F would be a vector space of finite dimension k over F_0. But then F would have $(p^{10})^k = p^{10k}$ elements which implies $10k = 25$ and $k = 5/2 \notin \mathbb{N}$. This is a contradiction.

6. $E := \mathbb{Q}(\sqrt[4]{2}, i)$ is a splitting field of $X^4 - 2$ over $\mathbb{Q}$. Assume that the Galois group $G := \mathrm{Gal}(E/F)$ is abelian. Then every subgroup of G is normal in G. This implies that every intermediate field of $E/\mathbb{Q}$ would be a Galois extension of $\mathbb{Q}$. But the intermediate field $F := \mathbb{Q}(\sqrt[4]{2})$ is not a Galois extension of $\mathbb{Q}$, since it is not normal over F. In fact, $X^4 - 2$ has a root in F but does not split into linear factors in $F[X]$, because $X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2})$ and the last factor has no root in the subfield F which consists of real numbers. This is a contradiction, and therefore, G is not abelian.