Math 114 Homework 6

Michael Knopf

(due Thursday, 12 March)

1. (Exercise 1 in DF §14.4.) Determine the Galois closure of $\mathbf{Q}(\sqrt{1+\sqrt{2}})$ over $\mathbf{Q}$.

   (See Corollary 23 on p. 594 in DF for the definition of the Galois closure of an extension E/F. (Properly speaking, we should call it *a* Galois closure, as it is determined by the choice of an algebraic closure of F; in this case you will probably choose to work in (the algebraic closure of $\mathbf{Q}$ inside) $\mathbf{C}$.))

   Proof. The minimal polynomial for $\sqrt{1+\sqrt{2}}$ over $\mathbb{Q}$ is $p(x) = x^4 - 2x^2 - 1$. Clearly, this element is a root of $p(x)$. $p(x)$ is quadratic in x^2, so the quadratic formula gives that its 4 distinct roots are $\pm\sqrt{1 \pm \sqrt{2}}$. Thus $p(x)$ has no linear factors over $\mathbb{Q}$. If it had any quadratic factors over $\mathbb{Q}$, one of the following would need to have rational coefficients:

   $$\left(x - \sqrt{1+\sqrt{2}}\right)^2 = x^2 - 2\sqrt{1+\sqrt{2}}x + \sqrt{2} + 1$$
   $$\left(x + \sqrt{1+\sqrt{2}}\right)\left(x - \sqrt{1+\sqrt{2}}\right) = x^2 - (1+\sqrt{2}).$$

   So $p(x)$ is irreducible, thus it is the minimal polynomial for $\sqrt{1+\sqrt{2}}$ over $\mathbb{Q}$.

   The Galois closure of $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ needs to also contain $\sqrt{1-\sqrt{2}}$. The other roots are just the negations of $\sqrt{1+\sqrt{2}}$ and $\sqrt{1-\sqrt{2}}$, so any field that contains these will contain all the roots of $p(x)$. Therefore, the Galois closure is $\mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}})$. □

2. (Exercise 3 in DF §14.7.) Let F be a field of characteristic not equal to 2. Fix an algebraically closed field L containing F. State and prove a necessary and sufficient condition on $\alpha, \beta \in F$ so that $F(\sqrt{\alpha}) = F(\sqrt{\beta})$. (Here $\sqrt{\alpha}, \sqrt{\beta}$ denote any elements of L whose squares are α and β respectively.)

   Use this to determine whether $\mathbf{Q}(\sqrt{1-\sqrt{2}}) = \mathbf{Q}(i, \sqrt{2})$ (where $\sqrt{1-\sqrt{2}}$, i, $\sqrt{2}$ denote elements of $\mathbf{C}$ with squares $1-\sqrt{2}$, -1, and 2 respectively).

   (You already did part of this exercise on the midterm.)

   $F(\sqrt{\alpha}) = F(\sqrt{\beta})$ if and only if 1) $\alpha\beta$ is a nonzero square in F, or 2) one of α or β is 0 and the other is a square in F.

   Proof. First, we will show that the given condition is sufficient. Assume WLOG that $\alpha = 0$. Then $F(\sqrt{\beta}) = F(\sqrt{\alpha}) = F(0) = F$ if β is a square in F. Next, assume that $\alpha\beta = c^2$ for some nonzero $c \in F$. Then α and β must both be nonzero, so $\sqrt{\beta} = \frac{c}{\sqrt{\alpha}} \in F(\sqrt{\alpha})$ and $\sqrt{\alpha} = \frac{c}{\sqrt{\beta}} \in F(\sqrt{\beta})$. Thus $F(\sqrt{\alpha}) = F(\sqrt{\beta})$.

   We will now show that the given condition is necessary. For us to have $F(\sqrt{\beta}) = F(\sqrt{\alpha})$, we need that $F(\sqrt{\beta}) \subseteq F(\sqrt{\alpha})$. This implies that $a + b\sqrt{\alpha} = \sqrt{\beta}$ for some $a, b \in F$. Squaring gives $a^2 + b^2\alpha + 2ab\sqrt{\alpha} = \sqrt{\beta}$. Therefore, $ab = 0$ and $a^2 + b^2\alpha = \beta$. This gives three cases:

   In the first case, $a = 0$ and $b \neq 0$. This means that $\beta = b^2\alpha$, so either $\alpha = \beta = 0$ or $\alpha\beta = b^2\alpha^2$ is a nonzero square. In the second case, $a \neq 0$ and $b = 0$. This means that $\beta = a^2$ is a nonzero square in F. This also gives that $F(\sqrt{\beta}) = F(a) = F$; so, for us to have $F(\sqrt{\alpha}) = F(\sqrt{\beta}) = F$, we need α to be a square in F as well. So either α and β are both nonzero squares in F, thus $\alpha\beta$ is a square in F, or $\alpha = 0$ and β is a square in F. In the third case, $a = b = 0$; thus, $\beta = 0$. This means that $F(\sqrt{\beta}) = F(0) = F$, so α must be a square in F in order for us to have $F(\sqrt{\alpha}) = F(\sqrt{\beta})$.

   Now, suppose that $\mathbb{Q}(\sqrt{2})(\sqrt{1-\sqrt{2}}) = \mathbb{Q}(\sqrt{1-\sqrt{2}}) = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\sqrt{2})(\sqrt{-1})$. By the previous result, since neither $\sqrt{1-\sqrt{2}}$ nor $\sqrt{-1}$ are 0, we must have

   $$-1 + \sqrt{2} = (-1)(1-\sqrt{2}) = (a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$$

   for some $a, b \in \mathbb{Q}$. This means that $a^2 + 2b^2 = -1$, a contradiction because $a^2 + 2b^2 \geq 0$. Thus, these extensions cannot be equal. □

3. (Exercise 4 in DF §14.7.) Let $n \in \mathbf{N}$ and $a \in \mathbf{Q}$ be such that $a > 0$ and $X^n - a \in \mathbf{Q}[X]$ is irreducible. Let $\beta \in \mathbf{C}$ be any root of $X^n - a$. Let $K = \mathbf{Q}(\beta)$. Let E be any subfield of K, and let $[E : \mathbf{Q}] = d$. Prove that $E = \mathbf{Q}(\gamma)$ where $\gamma^d = a$.

(Hint: Consider $N_{K/E}(\beta) \in E$; see Exercise 17 in §14.2, of which a modified version was assigned on a previous homework, for the definition.)

Proof. Consider the group G of all embeddings of K/E into an algebraic closure of E. By Galois correspondence, $|G| = [K : E] = \dfrac{[K : \mathbb{Q}]}{[E : \mathbb{Q}]} = \dfrac{n}{d}$, where we have let d be the degree of E over $\mathbb{Q}$, which must divide n. Thus $N_{K/E}(t) = t^{n/d}$ for any $t \in \mathbb{Q}$, since this norm is the product of $\sigma(t)$ over all embeddings σ which fix E, so that t must be fixed. Using the multiplicative property of the norm, we now have

$$N_{K/E}(\beta)^n = N_{K/E}(\beta^n) = N_{K/E}(a) = a^{n/d}$$

therefore $N_{K/E}(\beta) = \sqrt[d]{a} \in E$, since the norm always takes a value in the fixed field. Therefore, $\mathbb{Q}(\sqrt[d]{a})$ is a subfield of E, and both E and $\mathbb{Q}(\sqrt[d]{a})$ have degree d over $\mathbb{Q}$. Thus, $\mathbb{Q}(\sqrt[d]{a}) = E$. □

4. (Exercise 12 in DF §14.7.) Let $\alpha \in \mathbf{C}$ be an element algebraic over $\mathbf{Q}$, and let L be the Galois closure (cf. Question 1) of the extension $\mathbf{Q}(\alpha)$ of $\mathbf{Q}$. For any prime p dividing $[L : \mathbf{Q}]$, prove there is a subfield F of L with $[L : F] = p$ and $L = F(\alpha)$.

Proof. Let $G = \mathrm{Gal}(L/\mathbb{Q})$. By Cauchy's Theorem, G must contain a subgroup H of order p. Thus, by Galois correspondence, the fixed field K of H is a subfield of L such that $[L : K] = p$. If $\alpha \notin K$, then $F = K$ would suffice. However, this is not necessarily the case.

There must be some $\sigma \in G$ for which $\sigma(\alpha) \notin K$, otherwise all conjugates of α lie in K, and so the minimal polynomial of α over F splits completely in K. However, this would mean that L contains a proper subfield that is the splitting field for $m_\alpha(x)$, contradicting the minimality of L as the Galois closure of $\mathbb{Q}(\alpha)$.

Now, σ^{-1} is an embedding of K into L. Let F be the image of K under σ^{-1}. Clearly, $[L : F] = [L : K] = p$. We know that $\alpha \notin F$, otherwise there would exist some $k \in K$ such that

$$\alpha = \sigma^{-1}(k) \implies \sigma(\alpha) = k \in K,$$

a contradiction. Since $\alpha \notin F$, we know that $F(\alpha) \subseteq L$ has degree greater than 1 over F. Since its degree must divide p, it has degree p. Therefore, $F(\alpha)$ must equal L, since the degree of L over $F(\alpha)$ is p. □

5. (Exercise 13 in DF §14.7.) Let F be a subfield of the real numbers $\mathbf{R}$, a an element of F, n a positive integer, and $\beta \in \mathbf{R}$ a real n^{th} root of a (i.e., $\beta^n = a$). Prove that if L is any Galois extension of F contained in $K = F(\beta)$, then $[L : F] \leq 2$.

Proof. First, we will check some special cases. Assume that $a = 1$. Then β is either 1 or -1, since these are the only possible real nth roots of unity. In either case, K is a degree 1 extension, so the proposition is trivial.

It is possible that β does not have degree n over F. However, we may assume WLOG that it does. If this were not the case, then it means that a is an mth power in F, where m divides n, so that the degree of β is only $\frac{m}{n}$. But then we could use $a' = \sqrt[m]{a}$ in place of a, $\sqrt[m]{\beta}$ in place of β, and $n' = \frac{n}{m}$ in place of n, and the following proof would hold. The same argument from #3 applies to show that $L = F(\sqrt[d]{a})$ for some d dividing n, where $\sqrt[d]{a}$ is a real dth root of a.

Consider the group G of all embeddings of K/L into an algebraic closure of L. By Galois correspondence, $|G| = [K : L] = \dfrac{[K : F]}{[L : F]} = \dfrac{n}{d}$, where we have let d be the degree of L over F, which must divide n. Thus $N_{K/L}(t) = t^{n/d}$ for any $t \in F$, since this norm is the product of $\sigma(t)$ over all embeddings σ which fix L, so that t must be fixed. Using the multiplicative property of the norm, we now have

$$N_{K/L}(\beta)^n = N_{K/L}(\beta^n) = N_{K/L}(a) = a^{n/d}$$

therefore $N_{K/L}(\beta) = \sqrt[d]{a} \in L$, since the norm always takes a value in the fixed field. Therefore, $F(\sqrt[d]{a})$ is a subfield of L, and both L and $F(\sqrt[d]{a})$ have degree d over F. Thus, $F(\sqrt[d]{a}) = L$.

Since L is assumed to be Galois over F, it must contain all roots of $x^d - a$. So L contains all dth roots of unity. However, L is a real extension of a real field, thus it contains no complex numbers. The only values of d for which all dth roots of unity are real are $d = 1$ and $d = 2$. Thus $L = F(\sqrt[d]{a})$ is an extension of degree $d \leq 2$.

□