Math 121 Homework 7 Solutions

- Section 14.2 # 16, 18abc, 22b
- Section 14.5 # 3, 7
- Section 3.4 # 5

Section 15.2 Problem 16. (a) prove that $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$.

(b) Show that the roots of this quartic are $\alpha_1 = \sqrt{1+\sqrt{3}}$, $\alpha_2 = \sqrt{1-\sqrt{3}}$, $\alpha_3 = -\sqrt{1+\sqrt{3}}$, $\alpha_4 = -\sqrt{1-\sqrt{3}}$.

(c) Let $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$. Show that $K_1 \neq K_2$ and $K_1 \cap K_2 = \mathbb{Q}\left(\sqrt{3}\right) := F$.

(d) Prove that K_1 and K_2 and K_1K_2 are Galois over F with $\mathrm{Gal}(K_1K_2/F)$ the Klein 4-group. Write out the elements of $\mathrm{Gal}(K_1K_2/F)$ explicitly as permutations of the α_i.

(e) Prove that the splitting field of $x^4 - 2x^2 - 2$ over $\mathbb{Q}$ is of degree 8 with dihedral Galois group.

Solution: For (a), note that $x^4 - 2x^2 - 2$ is an Eisenstein polynomial in $\mathbb{Z}[x]$ at the prime 2, so it is irreducible over $\mathbb{Z}$. Since $\mathbb{Z}$ is a unique factorization domain, by Gauss' Lemma, it is irreducible over $\mathbb{Q}$.

For (b), if α is a root of $x^4 - 2x^2 - 2$ then α^2 is a root of $x^2 - 2x - 2$, so by the quadratic equation, $\alpha^2 = 1 \pm \sqrt{3}$.

(c). Since α_1 is real and α_2 is not, $\alpha_2 \notin K_1 \subseteq \mathbb{R}$ so $K_1 \neq K_2$. Since $\sqrt{3} = \alpha_1^2 - 1 = -\alpha_2^2 - 1$ we clearly have $\mathbb{Q}\left(\sqrt{3}\right) \subseteq K_1 \cap K_2$. Now $K_1 \cap K_2$ is a proper subfield of K_1 so $[K_1 \cap K_2 : \mathbb{Q}]$ properly divides $[K_1 : \mathbb{Q}] = \deg(x^4 - 2x^2 - 2) = 4$. Thus

$$[K_1 \cap K_2 : \mathbb{Q}] \leqslant 2 = \left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right]$$

and so $K_1 \cap K_2 = \mathbb{Q}\left(\sqrt{3}\right)$. We apply Proposition 21 on page 529 to learn that

$$\left[K_1K_2 : \mathbb{Q}\left(\sqrt{3}\right)\right] \leqslant \left[K_1 : \mathbb{Q}\left(\sqrt{3}\right)\right]\left[K_2 : \mathbb{Q}\left(\sqrt{3}\right)\right] = 2 \times 2 = 4.$$

Since $\left[K_1K_2 : \mathbb{Q}\left(\sqrt{3}\right)\right]$ is a strict multiple of $\left[K_1 : \mathbb{Q}\left(\sqrt{3}\right)\right] = 2$ it follows that $\left[K_1K_2 : \mathbb{Q}\left(\sqrt{3}\right)\right] = 4$.

(d) Using cycle notation for permutations, $\mathrm{Gal}(K_1K_2/F)$ clearly consists of the identity permutation and $\sigma_1 := (\alpha_1, \alpha_3)$ and $\sigma_2 = (\alpha_2, \alpha_3)$ amd $\sigma_1\sigma_2 = (\alpha_1, \alpha_3)(\alpha_2, \alpha_4)$.

(e) We need one element of $\mathrm{Gal}(K_1K_2 : \mathbb{Q})$ that is not in $\mathrm{Gal}(K_1K_2, F)$. Since α_1 and α_2 are conjugates, there is an automorphism $\tau : K_1K_2 \longrightarrow K_1K_2$ that sends α_1 to α_2. Since

$\alpha_1^2 - 1 = \sqrt{3}$ and $\alpha_2^2 - 1 = -\sqrt{3}$, this element τ must send $\sqrt{3}$ to $-\sqrt{3}$. Therefore it sends α_2 to either α_1 or α_3. If necessary we may replace τ with $\tau\sigma_2$ and arrange that $\tau(\alpha_2) = \alpha_3$. Then since $\alpha_3 = -\alpha_1$, $\tau(\alpha_3) = -\tau(\alpha_2) = -\alpha_1 = \alpha_4$. And $\tau(\alpha_4) = \tau(-\alpha_2) = -\tau(\alpha_2) = -\alpha_3 = \alpha_1$. In summary

$$\tau = (\alpha_1, \alpha_2, \alpha_3, \alpha_4).$$

Now τ and σ_1 satisfy the relations

$$\tau^4 = \sigma_1^2 = 1, \qquad \sigma_1 \tau \sigma_1^{-1} = \tau^{-1}$$

defining the dihedral group D_8.

Section 14.2 Problem 18 (parts a, b, c): With notation as in the previous problem define the *trace* of α from K to F to be

$$\mathrm{Tr}_{K/F}(\alpha) = \sum_{\sigma} \sigma(\alpha),$$

a sum of Galois conjugates of α.

(a) Prove that $\mathrm{Tr}_{K/F}(\alpha) \in F$.

(b) Prove that $\mathrm{Tr}_{K/F}(\alpha + \beta) = \mathrm{Tr}_{K/F}(\alpha) + \mathrm{Tr}_{K/F}(\beta)$, so that the trace is an additive map from K to F.

(c) Let $K = F\left(\sqrt{D}\right)$ be a quadratic extension of F. Show that $\mathrm{Tr}_{K/F}\left(a + b\sqrt{D}\right) = 2a$. **Note:** for this part, assume $\mathrm{char}(F) \neq 2$.

Solution. Consulting Problem 14.2.17 from the book, the assumptions stated there imply that K/F is separable. Indeed, K is embedded in a field L which is Galois over F, hence L/F is a separable extension. Therefore the intermediate extension K/F is separable. Therefore there are $n = [K : F]$ distinct embeddings of K into the "sufficiently large" (in the terminology of the class notes Separable Degree) field L. These embeddings $\sigma_1, \cdots, \sigma_n$ are needed in the definitions of the norma and trace:

$$N(x) = \sigma_1(x) \cdots \sigma_n(x), \qquad \mathrm{Tr}(x) = \sigma_1(x) + \cdots + \sigma_n(x).$$

The norm is the subject of Exercise 14.2.17 (not assigned) and is very similar to the trace (this exercise).

For (a), if $\tau \in \mathrm{Gal}(L/F)$ then $\tau\sigma_i : K \longrightarrow L$ is another embedding of K into L over F, so $\tau\sigma_i = \sigma_j$ for some j. This means that τ permutes the σ_i and we can calculate:

$$\tau(\mathrm{Tr}(x)) = \sum_i \tau\sigma_i(x) = \sum_j \sigma_j(x) = \mathrm{Tr}(x).$$

So $\mathrm{Tr}(x)$ is in the fixed field of $\mathrm{Gal}(L/F)$, and by the fundamental theorem of Galois theory, it lies in F. This proves (a).

(b): This is easy:

$$\mathrm{Tr}(\alpha + \beta) = \sum_i \sigma_i(\alpha + \beta) = \sum_i \sigma_i(\alpha) + \sum_i \sigma_i(\beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta).$$

(c): With $K = F\left(\sqrt{D}\right)$, K/F is Galois so we can take $L = K$. The two automorphisms σ_1 and σ_2 over F are the identity automorphism σ_1 and $\sigma_2\left(a + b\sqrt{D}\right) = a - b\sqrt{D}$. Therefore

$$\mathrm{Tr}\left(a + b\sqrt{D}\right) = \sum_{i=1}^{2} \sigma_i\left(a + b\sqrt{D}\right) = \left(a + b\sqrt{D}\right) + \left(a - b\sqrt{D}\right) = 2a.$$

Section 14.2 Problem 22: (part b) Suppose that K/F is a Galois extension and let σ be an element of the Galois group.

Solution: Only (b) is assigned, but (a) is the same idea. We are now assuming K/F is Galois, and then we may take $L = K$ in the notation of Problems 17 and 18. Then

$$\mathrm{Tr}(\beta) = \sum_{\tau \in \mathrm{Gal}(K/F)} \tau(\beta).$$

Now

$$\mathrm{Tr}(\sigma\beta) = \sum_{\tau \in \mathrm{Gal}(K/F)} \tau\sigma(\beta)$$

but $\tau \mapsto \tau\sigma$ just permutes the elements of $\mathrm{Gal}(K/F)$, so $\mathrm{Tr}(\sigma\beta) = \mathrm{Tr}(\beta)$. Therefore $\mathrm{Tr}(\beta - \sigma\beta) = \mathrm{Tr}(\beta) - \mathrm{Tr}(\sigma\beta) = 0$.

(b) Suppose that $\alpha \in K$ is of the form $\alpha = \beta - \sigma\beta$ for some $\beta \in K$. Prove that $\mathrm{Tr}_{K/F}(\alpha) = 0$.

Section 14.5 Problem 3. Determine the quadratic equation satisfied by the period $\alpha = \zeta_5 + \zeta_5^{-1}$ of the 5-th root of unity ζ_5. Determine the quadratic equation satisfied by ζ_5 over $\mathbb{Q}(\alpha)$ and use this to explicity solve for the 5th root of unity.

Solution. Write $\zeta = \zeta_5$. Then

$$\alpha^2 = \zeta^2 + 2 + \zeta^{-2}$$

so

$$\alpha^2 + \alpha - 1 = \zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} = 0.$$

This is our quadratic equation. The roots are given by the quadratic formula:

$$\alpha = \frac{-1 \pm \sqrt{5}}{2}$$

and since $\alpha = 2\cos\left(\frac{2\pi}{5}\right) > 0$ we want the positive square root here:

$$\alpha = \frac{-1 + \sqrt{5}}{2}. \tag{1}$$

Rewrite the equation $\alpha = \zeta + \zeta^{-1}$ as $\zeta^2 - \alpha\zeta + 1 = 0$ and use the quadratic formula again to write

$$\zeta = \frac{\alpha \pm \sqrt{\alpha^2 - 4}}{2} = \frac{\alpha + \sqrt{4 - \alpha^2} \cdot i}{2} \tag{2}$$

We write it this way since $4-\alpha^2>0$. The sign is determined by noting that $\mathrm{im}(\zeta)>0$. We have

$$4-\alpha^2=\frac{1}{2}\left(5+\sqrt{5}\right). \tag{3}$$

Substituting (1) and (3) into (2) gives:

$$\zeta=\frac{1}{2}\left(\frac{-1+\sqrt{5}}{2}+\sqrt{\frac{1}{2}\left(5+\sqrt{5}\right)}\cdot i\right).$$

Section 14.5 Problem 7. Show that complex conjugation restricts to the automorphism $\sigma_{-1}\in\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ of the cyclotomic field of nth roots of unity. Show that the field $K^+=\mathbb{Q}(\zeta_n+\zeta_n^{-1})$ is the subfield of real elements in $K=\mathbb{Q}(\zeta_n)$, called the *maximal real subfield* of K

Proof: Denote $\tau=\zeta_n+\zeta_n^{-1}$. The assertion is that $\mathbb{Q}(\tau)=\mathbb{Q}(\zeta_n)\cap\mathbb{R}$. Since τ is real, clearly $\mathbb{Q}(\tau)\subseteq\mathbb{Q}(\zeta_n)\cap\mathbb{R}$. On the other hand, the generator ζ_n of $\mathbb{Q}(\zeta_n)$ is quadratic over $\mathbb{Q}(\tau)$, and therefore $[\mathbb{Q}(\zeta_n):\mathbb{Q}(\tau)]=2$. Thus $[\mathbb{Q}(\zeta_n):\mathbb{Q}(\zeta_n)\cap\mathbb{R}][\mathbb{Q}(\zeta_n)\cap\mathbb{R}:\mathbb{Q}(\tau)]=2$. Obviously $[\mathbb{Q}(\zeta_n):\mathbb{Q}(\zeta_n)\cap\mathbb{R}]$ cannot be 1 since $\mathbb{Q}(\zeta_n)$ is not contained in $\mathbb{R}$. Therefore $[\mathbb{Q}(\zeta_n):\mathbb{Q}(\zeta_n)\cap\mathbb{R}]=2$ and $[\mathbb{Q}(\zeta_n)\cap\mathbb{R}:\mathbb{Q}(\tau)]=1$. The last identity shows that $\mathbb{Q}(\tau)=\mathbb{Q}(\zeta_n)\cap\mathbb{R}$, which is what we are asked to prove.

Problem 5 in 3.4. Prove that subgroups and quotient groups of a solvable group are solvable.

Solution. Suppose that G is solvable, and H is a subgroup of G. Since G is solvable, it has a filtration: $1=G_0\trianglelefteq G_1\trianglelefteq G_2\trianglelefteq\cdots\trianglelefteq G_n=G$, where G_{i+1}/G_i is abelian. Let $H_i=H\cap G_i$. Since G_i is normal in G_{i+1}, it is obvious that H_i is normal in H_{i+1}.

Lemma 1. *H_{i+1}/H_i is isomorphic to a subgroup of G_{i+1}/G_i.*

Proof. Consider the composite homomorphism $\pi:H_{i+1}\longrightarrow G_{i+1}\longrightarrow G_{i+1}/G_i$, where the first homomorphism is the inclusion of H_{i+1} as a subgroup of G_{i+1} and the second is the projection of G_{i+1} onto the quotient. The kernel of this map is

$$H_{i+1}\cap G_i=H\cap G_{i+1}\cap G_i=H\cap G_i=H_i.$$

Therefore $\pi(H_{i+1})\cong H_{i+1}/H_i$ by the First Isomorphism Theorem (Theorem 16 on page 97). $\square$

Since H_{i+1}/H_i is a subgroup of an abelian group, it is abelian and $1=H_0\trianglelefteq H_1\trianglelefteq H_2\trianglelefteq\cdots\trianglelefteq H_n=H$, proving that H is solvable.

Next suppose that $Q=G/N$ is a quotient of G, with N some normal subgroup. Let $\phi:G\longrightarrow Q$ be the projection map. Define $Q_i=\phi(G_i)$.

Lemma 2. *The subgroup Q_i is normal in Q_{i+1} and Q_{i+1}/Q_i is isomorphic to a quotient of G_{i+1}/G_i.*

Proof. The normality of $Q_i = \phi(G_i)$ in $Q_{i+1} = \phi(G_{i+1})$ follows from the normality of G_i in G_{i+1}.

Let $\theta : G_{i+1} \longrightarrow Q_{i+1}/Q_i$ be the composition $G_{i+1} \longrightarrow Q_{i+1} \longrightarrow Q_{i+1}/Q_i$. The first homomorphism here is ϕ restricted to G_{i+1}, and the second homomorphism is the projection onto the quotient. Both of these homomorphisms are surjective, so Q_{i+1}/Q_i is isomorphic to $G_{i+1}/\ker(\theta)$. Clearly $G_{i+1} \subseteq \ker(\theta)$ so $G_{i+1}/\ker(\theta)$ is isomorphic to a quotient of G_{i+1}/G_i. $\square$

Now $1 = Q_0 \trianglelefteq Q_1 \trianglelefteq Q_2 \trianglelefteq \cdots \trianglelefteq Q_n = Q$.