Solutions

Exercise 1. Let F be a field, let V be a vector space over F and let V^0 be the set of nonzero vectors in V. For $u, v \in V^0$, say that $u \sim v$ if there exists $a \in F$ such that $au = v$. Prove that this is an equivalence relation on V^0.

Comment. If $[u]$ is an equivalence class under this relation, the set $[u] \cup \{0\}$ is called a *line* in V.

Proof. Reflexivity: If $u \sim v$ then there exists $a \in F$ such that $au = v$, so $a^{-1}v = u$ so $v \sim u$.

Symmetry: $u = 1 \cdot u$ so $u \sim u$.

Transitivity: If $u \sim v$ and $v \sim w$ then there exist $a, b \in F$ with $au = v$ and $bv = w$. Hence $bau = bv = w$, so $u \sim w$. □

Optional Exercise for Extra Credit (20 points total)

[Solutions Posted Separately]

Exercise 2. Let $K \subset F \subset E$ be three fields. Suppose that $\{\alpha_1, \ldots, \alpha_m\}$ is a K-basis of F and $\{\beta_1, \ldots, \beta_n\}$ is an F-basis of E. Prove that $\{\alpha_i\beta_j : \ 1 \le i \le m, 1 \le j \le n\}$ is a K-basis of E.

Comment. This proves that the degree of a field extension is multiplicative: $[E : K] = [E : F][F : K]$.

Proof. Let $\gamma \in E$. Since $\{\beta_1, \ldots, \beta_n\}$ spans E over F, there are $f_j \in F$ such that $\gamma = \sum_{j=1}^n f_j\beta_j$. Since $\{\alpha_1, \ldots, \alpha_m\}$ spans F over Kd, there are, for each j, elements $c_{ij} \in K$ such that $f_j = \sum_{i=1}^m c_{ij}\alpha_i$. Then we have

$$\gamma = \sum_{j=1}^{n} f_j\beta_j = \gamma = \sum_{j=1}^{n}\sum_{i=1}^{m} c_{ij}\alpha_i\beta_j,$$

so $\{\alpha_i\beta_j : \ 1 \le i \le m, 1 \le j \le n\}$ spans E over K.

Suppose we have scalars $c_{ij} \in K$ such that

$$\sum_{j=1}^{n}\sum_{i=1}^{m} c_{ij}\alpha_i\beta_j = 0.$$

Since $\{\beta_1, \ldots, \beta_n\}$ is linearly independent, we have $\sum_{i=1}^m c_{ij}\alpha_i = 0$ for each i. Since $\{\alpha_1, \ldots, \alpha_m\}$ is linearly independent, we have $c_{ij} = 0$ for each i, j. Hence the set $\{\alpha_i\beta_j : \ 1 \le i \le m, 1 \le j \le n\}$ is linearly independent. Since this set spans E and is linearly lindependent over F, it is a an F-basis of E. □

Exercise 3. Let $\alpha = \sqrt[3]{2}$, $\zeta = e^{2\pi i/3}$, $F = \mathbb{Q}(\alpha)$ and $E = F(\zeta)$. Compute $[E : \mathbb{Q}]$.

Comment. On the previous homework, you showed that the roots of $x^3 - 2$ are $\alpha, \alpha\zeta, \alpha\zeta^2$. The field E is smallest subfield of $\mathbb{C}$ containing these roots.

Solution. We have $[E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 3[E : F]$. The minimal polynomial of ζ over $\mathbb{Q}$ is $x^2 + x + 1$, whose roots are complex, and do not lie in F. So $x^2 + x + 1$ is irreducible over F, and is also the minimal polynomial of α over F. It follows that $E = F(\zeta) = 2$, so $[E : \mathbb{Q}] = 3 \cdot 2 = 6$.

□

Exercise 4. Let $p > 2$ be a prime, let $\alpha = 2\cos(2\pi/p)$ and let $p_\alpha(x)$ be the minimal polynomial of α over $\mathbb{Q}$. Compute the degree of $p_\alpha(x)$.
(A formula for $p_\alpha(x)$ was stated in class without proof. Do not use this formula.)

Hint: Note that $\alpha = \zeta + \zeta^{-1}$, where $\zeta = e^{2\pi i/p}$. Compute $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)]$, to deduce $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

Solution. We know that the minimal polynomial of ζ over $\mathbb{Q}$ is $1+x+\cdots+x^{p-1}$, so $[\mathbb{Q}(\zeta):\mathbb{Q}]=p-1$. Since $\alpha=\zeta+\zeta^{-1}$, it follows that $\zeta^2-\alpha\zeta+1=0$, so ζ is a root of the polynomial $f(x)=x^2-\alpha x+1\in\mathbb{Q}(\alpha)[x]$. In fact, the roots of $f(x)$ are ζ and ζ^{-1}, which are complex hence do not lie in $\mathbb{Q}(\alpha)\subset\mathbb{R}$. Hence $f(x)$ is irreducible in $\mathbb{Q}(\alpha)[x]$. This means $[\mathbb{Q}(\zeta):\mathbb{Q}(\alpha)]=\deg f=2$. Hence

$$[\mathbb{Q}(\alpha):\mathbb{Q}]=\frac{[\mathbb{Q}(\zeta):\mathbb{Q}]}{[\mathbb{Q}(\zeta):\mathbb{Q}(\alpha)]}=\tfrac{1}{2}[\mathbb{Q}(\zeta):\mathbb{Q}]=\tfrac{1}{2}(p-1).$$

□

Exercise 5. Let $\alpha,\beta\in\mathbb{C}$ be two algebraic numbers whose minimal polynomials have degrees m,n respectively. Assume that $\gcd(m,n)=1$. Prove that $\mathbb{Q}(\alpha)\cap\mathbb{Q}(\beta)=\mathbb{Q}$.

Solution. Let $F=\mathbb{Q}(\alpha)\cap\mathbb{Q}(\beta)$. Then $n=[\mathbb{Q}(\alpha):\mathbb{Q}]=[\mathbb{Q}(\alpha):F]\cdot[F:\mathbb{Q}]$, so $[F:\mathbb{Q}]$ divides n. Likewises $[F:\mathbb{Q}]$ divides m. Since $\gcd(m,n)=1$, we have $[F:\mathbb{Q}]=1$, that is, $F=\mathbb{Q}$.

□

Exercise 6. Let $\zeta=e^{2\pi i/5}$ and let $\tau=(1+\sqrt{5})/2$ be the golden ratio.

a) Compute $[\mathbb{Q}(\zeta):\mathbb{Q}]$.

b) Show that $\mathbb{Q}(\tau)\subset\mathbb{Q}(\zeta)$.

c) Find the minimal polynomial of ζ over $\mathbb{Q}(\tau)$.
Hint: Factor $x^4+x^3+x^2+x+1=(x^2+ax+1)(x^2+bx+1)$ with $a,b\in\mathbb{R}$.

Solution.

a) The minimal polynomial of ζ over $\mathbb{Q}$ is $x^4+x^3+x^2+x+1$, so $[\mathbb{Q}(\zeta):\mathbb{Q}]=4$.

b) It suffices to show that $\tau\in\mathbb{Q}(\zeta)$. From class, we know that

$$\zeta+\zeta^{-1}=2\cos(2\pi/5)=\tfrac{1}{2}(-1+\sqrt{5})=\tau-1.$$

hence $\tau=1+\zeta+\zeta^{-1}\in\mathbb{Q}(\zeta)$.

c) There are various ways to do this. One way is to use the previous result: $\tau=1+\zeta+\zeta^{-1}$, so $\zeta\tau=\zeta+\zeta^2+1$, so ζ is a root of $x^2+(1-\tau)\zeta+1$.

Another way is to follow the hint and try to factor

$$x^4+x^3+x^2+x+1=(x^2+ax+1)(x^2+bx+1)=x^4+(a+b)x^3+(2+ab)x^2+(a+b)x+1.$$

We must have $b=1-a$, and $2+a(1-a)=1$, or $a^2-a-1=0$. This means $\{a,b\}=\{\tau,1-\tau\}$. Now ζ is root of either $x^2+\tau x+1$ or $x^2+(1-\tau)x+1$. But $\zeta^2+\tau+1$ has positive imaginary part, hence is not zero. So we again find that ζ is a root of $x^2+(1-\tau)\zeta+1$.

□