Solutions to Homework 8 **Math 5591H**

Homework submitted three days after the deadline will have a 5 point penalty for each additional day of delay.

5pt **13.2.13.** *Suppose $F=\mathbb{Q}(\alpha_1,\dots,\alpha_n)$ where $\alpha_i^2\in\mathbb{Q}$ for all i. Prove that $\sqrt[3]{2}\notin F$.*

Solution. For each i, α_i is a root of a quadratic polynomial over $\mathbb{Q}$, so has degree either 1 or 2 over $\mathbb{Q}(\alpha_1,\dots,\alpha_{i-1})$. $[F:\mathbb{Q}]$ is the product of these degrees, so is a power of 2. For any $\alpha\in F$, $\deg_{\mathbb{Q}}\alpha$ divides $[F:\mathbb{Q}]$, so is also a power of 2. Hence, F cannot contain $\sqrt[3]{2}$, which has degree 3 over $\mathbb{Q}$.

5pt **13.2.14.** *Prove that if $[F(\alpha):F]$ is odd, then $F(\alpha)=F(\alpha^2)$.*

Solution. α^2 is contained in the field $F(\alpha)$, and we have the tower of extensions $F(\alpha)/F(\alpha^2)/F$. If $\alpha\notin F(\alpha^2)$, then $[F(\alpha):F(\alpha^2)]=2$, and then $[F(\alpha):F]=[F(\alpha):F(\alpha^2)]\cdot[F(\alpha^2):F]$ is even. So, $\alpha\in F(\alpha^2)$.

5pt **13.2.16.** *Let K/F be an algebraic extension and let R be a ring with $F\subseteq R\subseteq K$. Prove that R is a field.*

Solution. We only have to show that $\alpha^{-1}\in R$ for every nonzero $\alpha\in R$. Let $\alpha\in R$, $\alpha\neq 0$. Then α^{-1} is an element of $F(\alpha)$, and since α is algebraic over F, we have $F(\alpha)=F[\alpha]\subseteq R$.

10pt **13.2.17.** *Let $f\in F[x]$ be irreducible with $\deg f=n$, and let $g\in F[x]$. Prove that every irreducible factor of $f(g(x))$ has degree divisible by n.*

Solution. Let q be an irreducible factor of $f(g(x))$ and let α be a root of q; then $\deg q=\deg_F\alpha$. The field $F(\alpha)$ contains the element $\beta=g(\alpha)$, so $F(\beta)\subseteq F(\alpha)$, and $\deg_F\beta=[F(\beta):F]\,\big|\,[F(\alpha):F]=\deg_F\alpha$. We have $f(\beta)=f(g(\alpha))=0$, so β is a root of f, and has degree n over F; so, $n\,\big|\,\deg_F\alpha$.

10pt **13.2.20.** *Find the minimal polynomial of $1+\sqrt[3]{2}+\sqrt[3]{4}$ over $\mathbb{Q}$.*

Solution. Let $\theta=\sqrt[3]{2}$, and let $K=\mathbb{Q}(\theta)$; then $\{1,\theta,\theta^2\}$ is a basis of K. Let $\alpha=1+\sqrt[3]{2}+\sqrt[3]{4}=1+\theta+\theta^2$. We have $\alpha\cdot 1=1+\theta+\theta^2$, $\alpha\theta=\theta+\theta^2+\theta^3=2+\theta+\theta^2$, and $\alpha\cdot\theta^2=(\alpha\theta)\theta=2\theta+\theta^2+\theta^3=2+2\theta+\theta^2$. So, the matrix of multiplication by α is $A=\left(\begin{smallmatrix}1&2&2\\1&1&2\\1&1&1\end{smallmatrix}\right)$. The characteristic polynomial of A is $f(x)=(x-1)^3-6(x-1)-6=x^3-3x^2-3x-1$. Since α is contained in the extension $\mathbb{Q}(\theta)/\mathbb{Q}$ of degree 3 and $\alpha\notin\mathbb{Q}$, it must be that $\deg_{\mathbb{Q}}\alpha=3$, so f is the minimal polynomial of α.

Another solution. We find the Smith normal form of $xI-A$:

$$xI-A=\begin{pmatrix}x-1&-2&-2\\-1&x-1&-2\\-1&-1&x-1\end{pmatrix}\mapsto\begin{pmatrix}1&1&-x+1\\x-1&-2&-2\\-1&x-1&-2\end{pmatrix}\mapsto\begin{pmatrix}1&1&-x+1\\0&-x-1&x^2-2x-1\\0&x&-x-1\end{pmatrix}\mapsto\begin{pmatrix}1&0&0\\0&-x-1&x^2-2x-1\\0&x&-x-1\end{pmatrix}$$
$$\mapsto\begin{pmatrix}1&0&0\\0&-1&x^2-3x-2\\0&x&-x-1\end{pmatrix}\mapsto\begin{pmatrix}1&0&0\\0&-1&x^2-3x-2\\0&0&x^3-3x^2-3x-1\end{pmatrix}\mapsto\begin{pmatrix}1&0&0\\0&1&0\\0&0&x^3-3x^2-3x-1\end{pmatrix}.$$

We see that the minimal polynomial of A, and so, of α is x^3-3x^2-3x-1 (and since A has a single invariant factor, we also see that α generates K, $K=\mathbb{Q}(\alpha)$).

10pt **13.2.22.** *Let K_1/F and K_2/F be finite subextensions of an extension K/F. Prove that $K_1\otimes_F K_2$ is a field iff $[K_1K_2:F]=[K_1:F]\cdot[K_2:F]$.*

Solution. We have an F-algebras homomorphism $\varphi\colon K_1\otimes K_2\longrightarrow K_1K_2$ defined by $\varphi(\alpha_1\otimes\alpha_2)=\alpha_1\alpha_2$, $\alpha_1\in K_1$, $\alpha_2\in K_2$. Since K_1K_2 is generated (even spanned) by the products $\alpha_1\alpha_2$ with $\alpha_1\in K_1$, $\alpha_2\in K_2$, φ is surjective. We have $\dim_F K_1\otimes_F K_2=\dim_F K_1\cdot\dim_F K_2=[K_1:F]\cdot[K_2:F]$, so if $\dim_F K_1K_2=[K_1K_2:F]=[K_1:F]\cdot[K_2:F]$ as well, φ is an isomorphism and $K_1\otimes_F K_2$ is a field. If $\dim_F K_1K_2<[K_1:F]\cdot[K_2:F]$, then φ has a nonzero kernel, which is then a nontrivial ideal in $\dim_F K_1\otimes_F K_2$, so this ring cannot be a field.

5pt **13.1.1.** *Show that $p=x^3+9x+6$ is irreducible over $\mathbb{Q}$. Let θ be a root of p (in some extension of $\mathbb{Q}$); represent $(1+\theta)^{-1}$ in the form $a+b\theta+c\theta^2$ with $a,b,c\in\mathbb{Q}$.*

Solution. p is irreducible by Gauss's lemma and Eisenstein's criterion. Thus, $\mathbb{Q}(\theta)\cong\mathbb{Q}[x]/(p)$ is a field, in which $\theta^3=-9\theta-6$ and $\{1,\theta,\theta^2\}$ is a basis over $\mathbb{Q}$. Now if $(1+\theta)^{-1}=a+b\theta+c\theta^2$, then

$$1=(1+\theta)(a+b\theta+c\theta^2)=a+b\theta+c\theta^2+a\theta+b\theta^2+c\theta^3=a-6c+(a+b-9c)\theta+(b+c)\theta^2,$$

so $b+c=0$, $a+b-9c=0$, and $a-6c=1$. From this we obtain that $c=1/4$, $b=-1/4$, $a=5/2$.

Another solution. Consider the action of $1+\theta$ on $\mathbb{Q}(\theta)$ by multiplication; in the basis $\{1,\theta,\theta^2\}$ the matrix of this action is $A = \begin{pmatrix} 1 & 0 & -6 \\ 1 & 1 & -9 \\ 0 & 1 & 1 \end{pmatrix}$. The first column of the inverse A^{-1} of A is the vector of coordinates of $(1+\theta)^{-1}\cdot 1 = (1+\theta)^{-1}$; it equals $\begin{pmatrix} 5/2 \\ -1/4 \\ 1/4 \end{pmatrix}$, so $(1+\theta)^{-1} = \frac{5}{2} - \frac{1}{4}\theta + \frac{1}{4}\theta^2$.

5pt **13.1.3.** *Show that $p = x^3 + x + 1$ is irreducible over $\mathbb{F}_2$. Let θ be a root of p (in some extension of $\mathbb{F}_2$); compute the powers of θ in $\mathbb{F}_2(\theta)$ (in the form $a + b\theta + c\theta^2$).*

Solution. $p \in \mathbb{F}_2[x]$ is irreducible since it has no roots in $\mathbb{F}_2$. (Both 0 and 1 are not roots of p.) So, $\mathbb{F}_2(\theta) \cong \mathbb{F}_2[x]/(p)$ is a field, of cardinality $2^3 = 8$, in which $\theta^3 = \theta + 1$, and $\{1,\theta,\theta^2\}$ is a basis over $\mathbb{F}_2$. The powers of θ in this basis are

$$1,\ \theta,\ \theta^2,\ 1+\theta,\ \theta+\theta^2,\ 1+\theta+\theta^2,\ 1+\theta^2,\ 1,\ \theta,\ ,\ldots$$

(Notice that this sequence runs over all nonzero elements of $\mathbb{F}_2(\theta)$, that is, the multiplicative group of this field is cyclic, generated by θ.)

5pt **13.4.2.** *Determine the splitting field (as a subfield of $\mathbb{C}$) and find its degree over $\mathbb{Q}$ of $f = x^4 + 2$.*

Solution. Fortunately, we have the field $\mathbb{C}$, which contains all roots of f, $\pm\alpha, \pm\beta$, where $\alpha = \frac{1+i}{\sqrt{2}}\sqrt[4]{2} = \frac{1+i}{\sqrt[4]{2}}$ and $\beta = \frac{1-i}{\sqrt{2}}\sqrt[4]{2} = \frac{1-i}{\sqrt[4]{2}}$. It suffices to adjoin these roots: the splitting field is $K = \mathbb{Q}\big(\pm\alpha,\pm\beta\big) = \mathbb{Q}(\alpha,\beta)$. Clearly, $K = \mathbb{Q}(\sqrt[4]{2}, i)$ (since $\alpha,\beta \in \mathbb{Q}(\sqrt[4]{2}, i)$ and, on the other hand, $\sqrt[4]{2} = 2(\alpha+\beta)^{-1} \in K$ and $i = \sqrt[4]{2}\alpha - 1 \in K$), and has degree 8 over $\mathbb{Q}$.

5pt **13.4.4.** *Determine the splitting field (as a subfield of $\mathbb{C}$) and find its degree over $\mathbb{Q}$ of $f = x^6 - 4$.*

Solution. We have $x^6 - 4 = (x^3-2)(x^3+2)$. The roots of $x^3 - 2$ are α, $\alpha\omega$, and $\alpha\omega^2$ where $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$, and the splitting field of $x^3 - 2$ is $K = \mathbb{Q}(\alpha,\omega)$. But the second factor $x^3 + 2$ also splits in K: $x^3 + 2 = (x+\alpha)(x+\omega\alpha)(x+\omega^2\alpha)$. So, K is the splitting field of $x^6 - 4$. We have $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$ and $[\mathbb{Q}(\omega):\mathbb{Q}] = 2$, and since 2 and 3 are coprime, it follows that $[K:\mathbb{Q}] = 6$.

5pt **13.4.3.** *Determine the splitting field (as a subfield of $\mathbb{C}$) and find its degree over $\mathbb{Q}$ of $f = x^4 + x^2 + 1$.*

Solution. The roots of f in $\mathbb{C}$ are $\pm\alpha,\pm\beta$, where $\alpha = \sqrt{\frac{-1+\sqrt{-3}}{2}}$ and $\beta = \sqrt{\frac{-1-\sqrt{-3}}{2}}$, and so the splitting field K of f is $\mathbb{Q}(\alpha,\beta)$. (This fact however doesn't provide enough information on $[K:F]$.) We have $\alpha\beta = \sqrt{1} = 1$ (or -1, dependently on how we interprete the radicals), so $\beta \in \mathbb{Q}(\alpha)$, and the splitting field of f is $K = \mathbb{Q}(\alpha)$. f is reducible: $f = (x^2+x+1)(x^2-x+1)$, so α is a root of a quadratic polynomial (actually, $\alpha = \frac{1+\sqrt{-3}}{2}$) so $[K:\mathbb{Q}] = 2$ (and $K = \mathbb{Q}(\sqrt{-3})$.

(Alternatively, we can notice that $f(x)(x^2-1) = x^6 - 1$, so K is the 6th cyclotomic field.)