Chapter 5

Exercise 5.1

We have

$$\begin{aligned}(\alpha^2+\alpha+1)(\alpha^2+\alpha) &= (\alpha^3+\alpha^2+\alpha)(\alpha+1)\\ &= (\alpha^3+\alpha^2+\alpha+2)(\alpha+1)-2(\alpha+1)\\ &= 2\alpha+2,\end{aligned}$$

and

$$(\alpha-1)(a\alpha^2+b\alpha+c) = a\alpha^3+(b-a)\alpha^2+(c-b)\alpha-c,$$

$$\begin{aligned}b-a=a &\Leftrightarrow b=2a,\\ c-b=a &\Leftrightarrow c=3a,\\ -c &= 2a+1,\end{aligned}$$

whence $a=-1/5$, and if we factor out a, we get

$$\begin{aligned}a(\alpha-1)(\alpha^2+2\alpha+3) &= a(\alpha^3+2\alpha^2+3\alpha-\alpha^2-2\alpha-3)\\ &= a(\alpha^3+\alpha^2+\alpha-3)\\ &= a(-5)\\ &= 1\end{aligned}$$

so

$$(\alpha-1)^{-1} = \frac{-1}{5}\alpha^2+\frac{-2}{5}\alpha+\frac{-3}{5}.$$

Exercise 5.2

We have that $[E:F]=[F(\alpha):F(\alpha^2)][F(\alpha^2):F]$ by Prop 5.1.2, so $[F(\alpha):F(\alpha^2)]$ must be odd. But $X^2-\alpha^2\in F(\alpha^2)[X]$ has α as a root, so $[F(\alpha):F(\alpha^2)]$ is both odd and less than or equal to 2, hence equal to 1 and $E=F(\alpha)=F(\alpha^2)$.

Exercise 5.3

Let $g_1,g_2\in F(\alpha)[X]$ be such that $g_1g_2=g$. Then at least one of $g_1(\beta)=0$ or $g_2(\beta)=0$. Suppose $g_1(\beta)=0$. Then $[F(\alpha,\beta):F(\alpha)]=\deg(g_1)$. But

$$\begin{aligned}\deg(g_1)\deg(f) &= [F(\alpha,\beta):F(\alpha)][F(\alpha):F]\\ &= [F(\alpha,\beta):F]\\ &= [F(\alpha,\beta):F(\beta)][F(\beta):F]\\ &= [F(\alpha,\beta):F(\beta)]\deg(g),\end{aligned}$$

and since $(\deg(g),\deg(f))=1$, we must have $\deg(g)|\deg(g_1)$. But $\deg(g_1)\le\deg(g)$ since $g_1|g$, so $\deg(g_1)=\deg(g)$ and $g=g_1$. Hence g is irreducible in $F(\alpha)[X]$.

Exercise 5.4

Let $Q(\alpha) \supsetneq L \supsetneq Q$, and $f = X^4 - 2$ be the minimal polynomial of α in Q. It follows from Prop 5.1.2 that $[L : Q] = 2$. Then let g_L be the minimal polynomial of α in L. Then $\deg g_L = 2$, $g_L | f$, and since $L[X]$ is a UFD, we have that $f = (x - \beta_1)(x - \beta_2)g_L$ for some $\beta_1, \beta_2 \in Q(\alpha)$. Furthermore, since $L \subset R$ is real, we must have $g_L = (x - \alpha)(x + \alpha)$, since the other roots of f are $\pm i\alpha$, and no other combination of the roots of f yields a real polynomial. We have $g_L = x^2 - \sqrt{2}$, hence $L \supseteq Q(\sqrt{2})$, but since $[Q(\alpha) : Q(\sqrt{2})] = [Q(\sqrt{2}) : Q] = 2$, we have $L = Q(\sqrt{2})$ and this is the only field which lies strictly between Q and $Q(\alpha)$.

Exercise 5.5

Let α be a root of $f(X) = X^6 + X^3 + 1$. Then $f(X)(X^3 - 1) = X^9 - 1$, so α is a root of $g(X) = X^9 - 1$ as well. In other words, α is a 9-th root of unity which isn't a 3-rd root of unity.

Any field homomorphism which has a domain which contains Q must fix Q, hence any $\sigma : Q(\alpha) \to C$ can be seen as an embedding of $Q(\alpha)$ over Q into C. It the follows from Proposition 2.7 that the number of such σ is 6, since there are 6 9-th roots of unity which aren't 3-rd roots of unity.

Exercise 5.6

First of, we have $\alpha = \sqrt{2} + \sqrt{3} \in Q(\sqrt{2})(\sqrt{3})$, so α has at most degree 4. Moreover, we have

$$\alpha \frac{\sqrt{3} - \sqrt{2}}{5} = 1,$$

so

$$\sqrt{2} = \frac{\alpha - 5\alpha^{-1}}{2}, \ \sqrt{3} = \frac{\alpha + 5\alpha^{-1}}{2},$$

and $\sqrt{2}, \sqrt{3} \in Q(\alpha)$. Finally, note that $\sqrt{2} \notin Q(\sqrt{3})$ since $(a\sqrt{3} + b)^2 = 9a^2 + 2\sqrt{3}ab + b^2$ can never equal 2 for rational a, b. Indeed, $\sqrt{3}$ is irrational, so we'd need $b = 0$ (as $a = 0$ isn't an option), but then $a = \sqrt{9/2} = 3/\sqrt{2}$ which is also irrational. It follows that $Q(\sqrt{2} + \sqrt{3}) = Q(\sqrt{2})(\sqrt{3}) \supsetneq Q(\sqrt{3})$ has degree 4.

Exercise 5.7

We have $[EF : k] = [EF : E][E : k]$, so we need to prove that $[EF : E] \leq [F : k]$ with whenever $([F : k], [E : k]) = 1$. Let $a_1, \ldots, a_n$ be a k-basis for F. Then since $E \supseteq k$, we have that $a_1, \ldots, a_n$ spans EF in E, which shows $[EF : E] \leq [F : k]$. Now consider the case when $([F : k], [E : k]) = 1$. Then since $[EF : k] = [EF : F][F : k]$, we have that both $[F : k]$ and $[E : k]$ divide $[EF : k]$, and the equlity follows.

Exercise 5.8

Let $f = g_1 g_2 \dots g_m$ be a decomposition into irreducible polynomials, and K_i be the splitting field of g_i in K_{i-1} where $K_0 = k, K_m = K$. Then $[K_{i+1} : K_i]$ Then K

We proceed by induction on n. If $n = 1$, then the statement is clear. Now suppose it holds for all degrees $< n$.

Let α be a root of f, and $\hat{f} = f/(X - \alpha) \in K[X]$. Then $\deg \hat{f} = n - 1$, and deg

Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of f in K. Define $K_0 = k$, and inductively $K_{i+1} = K_i(\alpha_{i+1})$. Let g_{i+1} be the minimal polynomial of α_{i+1} in K_i, and $d_i = \deg g_{i+1}$. Then $[K : k] = \prod d_i$, and we are done if we can show that $\prod d_i | n!$. First note that $d_1 \leq n$ since $g_1 | f$. Moreover, if

Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of f in K, and set $\hat{f} = f/(X - \alpha_1)$.

Then $\hat{K} = k(\alpha_2, \alpha_3, \dots, \alpha_n)$ is a splitting field of $\hat{f}$. Since $\deg \hat{f} = n - 1$ it follows by our inductive hypothesis that $[\hat{K} : k] | (n-1)!$. Moreover, the minimal polynomial of α_1 in $\hat{K}$ divides

Let g_1 be the minimal polynomial of α_1 in $K_0 = K$, and let $K_1 = K_0(\alpha_1)$. Then $[K_1 : K_0] = \deg g_1$, and $\deg g_1 | n!$ since $g_1 | f$. Let $f_1 = f/(X - \alpha_1)$.

,

and g be its minimal polynomial. Then $g|f$ and so $\deg g < n \Rightarrow \deg g | n!$. It follows that [] Let k^a be an algebraic closure of K. Then K contains all the roots of f in k^a, call them $\alpha_1, \alpha_2, \dots, \alpha_n$. Hence

$$k(\alpha_1, \alpha_2, \dots, \alpha_n) \subseteq K.$$

For any α_i, we have that f is it's minimal polynomial and $[k(\alpha_i) : k] = n$