1. A prime field is a field with no proper subfields. The prime subfield of a field $F$ is the intersection of all subfields of $F$. If $P$ be the prime subfield of a field $F$. If $Q \neq P$ were a proper subfield it were a subfield of $F$ and thus $P \subseteq Q$, a contradiction.

2. If $r \in \mathbb{R}$ but not algebraic over $\mathbb{Q}$. Then $r$ is algebraic over $\mathbb{R}$ but not over $\mathbb{Q}$.

3. If $f, g \in \mathbb{Q}$ then $f(x) = 0 = g(x)$, then $(f-g)(x) = 0$ and $f, g \in \mathbb{Q}$. The zero polynomial is in $\mathbb{Q}$ and for $f \in \mathbb{Q}$ and $g \in \mathbb{Q}$ we have $(f)(x) = f(a) g(x) = 0$, thus $f \in \mathbb{Q}$. Therefore, $\mathbb{Q}$ is an ideal of $\mathbb{K}[x]$.

4. (a) $\sqrt{2} \in \mathbb{Q}$ but $\sqrt{2}^2 - 2 = 0$ thus $x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$, and the degree is 2.

(b) $\sqrt{2} \in \mathbb{R}$ and thus $x - \sqrt{2}$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{R}$, the degree is 1.

(c) We have $i + 1 \notin \mathbb{R}$ so the degree is $> 1$. $(i + 1)^2 = 2i$ thus $(i + 1)^2 - 2(i + 1) + 2 = 0$ and $x^2 - 2x + 2$ is the minimal polynomial of $i + 1$ over $\mathbb{R}$, the degree is 2.

(d) For $b \neq 0$ we have $a + b\sqrt{2} \notin \mathbb{Q}$ and thus $x - a$ is the minimal polynomial and the degree is 1. For $b = 0$ we have $a + b\sqrt{2} \in \mathbb{Q}$ thus the degree is $> 1$.

Since $(a + b\sqrt{2})^2 = a^2 + 2b^2 + (2\sqrt{2} a) b$ we get that $(a + b\sqrt{2})$ is a root of $x^2 - 2ax + (a^2 - 2b^2)$, which is the minimal polynomial of $a + b\sqrt{2}$ (the degree is 2).

5. Assume $\sum_{i=1}^{m} a_i u_i$ for some $a_i \in F$. For $e \in E$ arbitrary, we can express $e$ as a linear combination of $u_{m+1}, \ldots, u_{m+3}$. If $e = \sum_{i=1}^{m} a_i u_i$, then:

$$e = \sum_{i=1}^{m} b_i u_i + \sum_{i=m+1}^{m+3} a_i u_i = \sum_{i=m+1}^{m+3} b_i (u_i + \lambda a_i) u_i.$$  Since this works for arbitrary $e \in E$, we have shown that $u_{m+1}, \ldots, u_{m+3}$ span $E$ over $F$.

6. (a) Consider the field extension $Q \subseteq Q(\sqrt{3}) \subseteq Q(\sqrt{3}, i)$, the first has degree 2 since $\sqrt{3} \notin \mathbb{Q}$ (as the polynomial $x^2 - 3$). We know: $\{1, \sqrt{3}\}$ is a $\mathbb{Q}$-basis of $Q(\sqrt{3})$. However, since $Q(\sqrt{3}) \subseteq \mathbb{R}$ we have $i \notin Q(\sqrt{3})$, thus $X^2 + 1$ is irreducible in $Q(\sqrt{3})[X]$. Thus $Q(\sqrt{3}, i)$ is an extension of degree 2 over $Q(\sqrt{3})$ with basis $\{1, i\}$. In the lecture we conclude that $[Q(\sqrt{3}, i) : Q] = 4$ and that $\{1, i, \sqrt{3}, i \sqrt{3}\}$ is a $\mathbb{Q}$-basis of $Q(\sqrt{3}, i)$ over $Q$. In particular, it is linearly independent.
6. (c) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has degree 2 over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{7}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let $\alpha = \sqrt{2}, \beta = \sqrt{3}, \gamma = \sqrt{7}$. Since 2, 3, and 7 are primes in $\mathbb{Q}[\alpha, \beta, \gamma]$, we have $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a subextension of $\mathbb{Q}(\sqrt{7})$. Now, $2, \sqrt{3} \in \mathbb{Q}(\sqrt{7})$? No, because $(\alpha + \beta \beta^2)^2 = 3$ would imply:

$$a^2 + 2b^2 + 3c^2 - 2d^2 = 3 \implies \alpha b = 0 \implies \text{either } a \text{ or } b \text{ is zero}.$$  
But neither $a^2 = 3$ nor $2b^2 - 3$ has a rational solution. \(\Rightarrow \sqrt{3} \notin \mathbb{Q}(\sqrt{7})\)

\(\therefore [\mathbb{Q}(\sqrt{7}, \sqrt{3}) : \mathbb{Q}] = 4 \). And $\{1, \sqrt{7}, \sqrt{3}, \sqrt{7}\sqrt{3} \}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{7}, \sqrt{3})$.

Now $5 \notin \mathbb{Q}(\sqrt{7}, \sqrt{3})$? Suppose $5 = (a + b \sqrt{7} + c \sqrt{3} + d \sqrt{7} \sqrt{3})^2$ with $a, b, c, d \in \mathbb{Q}$. \(\Rightarrow 5 = a^2 + 2b^2 + 3c^2 + 6d^2 + 2bc \sqrt{21} + 2bd \sqrt{21} + (2ac + 4bd) \sqrt{21} + (2ad + 2bc) \sqrt{21} \Rightarrow \quad 6bc + 12bd = 0 = a(2ac + 4bd)

If $d = 0$, then $ab = 0$. \(\Rightarrow \alpha c = bc \Rightarrow \text{all but two of } a, b, c \text{ are zero} \), and

$$5 = a^2 \text{ or } 5 = 2b^2 \text{ or } 5 = 3c^2 \text{ has a rational solution, no solution unless } d \neq 0.$$

If $d = 0$, then $a = - \frac{bc}{d} \implies \frac{bc}{d} + 3cd = 0 = -\frac{bc^2}{d} + 2bd = -\frac{bc^2}{d} + bc$

\(\Rightarrow \frac{bc^2}{d} + 2bd = \frac{2bd^2 - d^2}{d^2} \cdot c(3d^2 - d^2) = 0 = \mathbb{Q}(2d^2 - c^2)$

\(\Rightarrow \) none the square in both have no rational solution, both $d$ and $c$ must be 0, thus also $a = 0$.

But $5 = 6d^2$ also does not have a rational solution.

Thus we have shown: $[\mathbb{Q}(\sqrt{7}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{7}, \sqrt{3})] = 2$ and $\{1, \sqrt{7}, \sqrt{3}, \sqrt{7} \} \}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{7}, \sqrt{3}, \sqrt{5})$.

In particular, $\{1, \sqrt{7}, \sqrt{3}, \sqrt{5} \}$ is linearly independent.

7. First we have to show that $\mathbb{A}$ is a subfield of $\mathbb{C}$:

- $\mathbb{A}$ contains $\mathbb{Q}$ and $1$ and $\mathbb{Q}$.
- Let $a, b \in \mathbb{A}$, then both are algebraic over $\mathbb{Q}$, thus $\mathbb{Q}(a)$ and $\mathbb{Q}(b)$ are finite extensions of $\mathbb{Q}$. But then $\mathbb{Q}(a, b)$ is also a finite extension of $\mathbb{Q}(a) = \mathbb{Q}(c, e)$.

Thus every element of $\mathbb{Q}(a, b)$ is algebraic over $\mathbb{Q}$.

Therefore, in particular $a+b, a-b, a^{-1}$ and $a, b^n$ (if $a > 0, b^0$) are in $\mathbb{Q}(a, b)$ and thus algebraic. \(\Rightarrow \mathbb{A} \) over $\mathbb{Q}$ is algebraic.

Now we need to show that $\mathbb{A}$ is not finite over $\mathbb{Q}$:

We use: If $f \in \mathbb{Z}[x]$ monic with $f = a_n x^n + \cdots + a_0$ and $a_n = 1$ and that is a prime $p \in \mathbb{Z}$ such that all $a_i$ for $0 \leq i < n$ are divisible by $p$ and $a_0$ is not divisible by $p^2$, then $f$ is irreducible in $\mathbb{Q}[x]$.

Thus there are irreducible polynomials $x^2 - 7$ of arbitrary high degree $\Rightarrow \dim_{\mathbb{Q}} (\mathbb{A}) = \infty$.  

8. \( \alpha \) is a root of the polynomial \( X^5 - 7 \). This is irreducible by the criterion of 7.

\( (a) \) \( [\mathbb{Q} : \mathbb{Q}(\alpha)] = 5 \)

\( (b) \) \( \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[5]{7}, (\sqrt[5]{7})^2, (\sqrt[5]{7})^3, (\sqrt[5]{7})^4, \alpha) \)

\( (c) \) \( \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, \sqrt[5]{7}, (\sqrt[5]{7})^2, (\sqrt[5]{7})^3, \alpha) \)

\( a, b, c, d, e \in \mathbb{Q} \)

9. \( \frac{3}{1}, \ldots, \frac{3}{1}, \ldots, \frac{3}{1} \)

\( (b) \) Write \( \mathbb{Q}(\alpha) \) for all \( a^2 + b^2 + c \) with \( a, b, c \in \mathbb{Q}(\alpha) \)

(c) \( \theta^4 = \theta(\theta + 1) = \theta^2 + \theta \)

\( (\theta^2 + \theta)^3 + \theta^2 + \theta + 1 = \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta + 1 \)

\( = (\theta + 1)^2 + \theta^2 + \theta + 1 + \theta^2 + 1 + \theta + 1 \)

\( = \theta^3 + 1 + \theta + 1 + \theta^2 + \theta^2 + 1 + \theta^2 + 1 + \theta + 1 \)

\( = 0 \)

\( (\theta^2 + \theta + 1)^3 + \theta^2 + 1 = \theta^6 + \theta^3 + \theta + 1 = (\theta + 1)^2 + \theta^2 + 1 = \theta^2 + \theta + \theta^2 + 1 = 0 \)

\( \Rightarrow \theta^2 \) is another root of \( X^5 + X + 1 \)

\( \Rightarrow X^5 + X + 1 = (X + \theta)(X + \theta^2)(X + \theta^4) \)

(d) As, it did not occur!
10. (a) \( \mathbb{Q}(\sqrt{-5}) \cdot \mathbb{Q}(i \sqrt{5}) \) is the splitting field since
\[(x^2 + 6) = (x - i \sqrt{5})(x + i \sqrt{5})\]

(b) \( \mathbb{Q}(\sqrt[3]{5}) \) has degree 3 over \( \mathbb{Q} \) but is contained in \( \mathbb{Q} \).

Then, the other two roots, \( 3/5 \cdot 5 \) and \( 3 \sqrt[3]{5} \cdot 5^2 \), for \( 5 = e^{\frac{2 \pi i}{3}} \) are not in \( \mathbb{Q}(\sqrt[3]{5}) \). They are contained in \( \mathbb{Q}(\sqrt[3]{5}, 5) \) which we get from \( \mathbb{Q}(\sqrt[3]{5}) \) by adjoining a root of \( x^2 + x + 1 \) to get \( 5 \). This is an extension of degree 2 and thus \([\mathbb{Q}(\sqrt[3]{5}, 5) : \mathbb{Q}] = 6\).

11. (a) Both have one root in \( \mathbb{F}_3 \) and are thus irreducible because their degree is 2.

(b) \( L \) contains one root and then the other of \( x^2 + 1 \) (it is the negative of the root).

Thus, \( L \) is the splitting field.

(c) \((x+1)^2 + (x+1) - 1 = x^2 + 2x + 1 + x + 1 - 1 = x^2 + 3x + 1 = 0 \)

\( \Rightarrow \) \( L \) contains a root of \( g \). Thus, \( L \) contains the other root
\[ g = (x - (x+1))(x - \beta) \text{ for some } \beta \in L. \]