Tutorial sheet 2

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.
Let P be the prime subfield of a field F. If $Q \subsetneq P$ were a proper subfield it were a subfield of F and thus $P \subseteq Q$, a contradiction.

2. $\pi \in \mathbb{R}$ but not algebraic over $\mathbb{Q}$. Thus π is algebraic over $\mathbb{R}$ but not over $\mathbb{Q}$.

3. If $f, g \in J$ then $f(\alpha) = 0 = g(\alpha)$, thus $(f-g)(\alpha) = 0$ and $f - g \in J$. The zero polynomial is in J and for $f \in J$ and $g \in K[x]$ we have $(fg)(\alpha) = f(\alpha) \cdot g(\alpha) = 0$, thus $fg \in J$. Therefore, J is an Ideal of $K[x]$.

4. (a) $\sqrt{2} \notin \mathbb{Q}$ 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 $b = 0$ we have $a + b\sqrt{2} \in \mathbb{Q}$ and thus $x - a$ is the minimal polynomial and the degree is 1. For $b \neq 0$ we have $a + b\sqrt{2} \notin \mathbb{Q}$ thus the degree is > 1.
Since $(a + b\sqrt{2})^2 = a^2 + 2b^2 + (2\sqrt{2}ab)$ 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 $u_m = \sum_{i=1}^{m-1} a_i u_i$ for some $a_i \in F$. For $e \in E$ arbitrary, we can express e as linear combination of $\{u_1, \dots, u_m\}$. If $e = \sum_{i=1}^{m} b_i u_i$, then
$$e = \sum_{i=1}^{m-1} b_i u_i + b_m \cdot \left(\sum_{i=1}^{m-1} a_i u_i \right) = \sum_{i=1}^{m-1} (b_i + b_m a_i) u_i .$$
Since this works for arbitrary $e \in E$, we have shown that $\{u_1, \dots, u_{m-1}\}$ span E over F.

6. (a) Consider the field extensions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}, i)$, the first has degree 2 since $\sqrt{3} \notin \mathbb{Q}$ (use the polynomial $X^2 - 3$), we know: $\{1, \sqrt{3}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{3})$. However, since $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$, we have $i \notin \mathbb{Q}(\sqrt{3})$, thus $X^2 + 1$ is irreducible in $\mathbb{Q}(\sqrt{3})[x]$. Thus $\mathbb{Q}(\sqrt{3}, i)$ is an extension of degree 2 over $\mathbb{Q}(\sqrt{3})$ with basis $\{1, i\}$. As in the lecture we conclude that $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}]$ is 4 and that $\{1, \sqrt{3}, i, i\sqrt{3}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{3}, i)$ over $\mathbb{Q}$. In particular, it is linearly independent.

6. (b) $\mathbb{Q}(\sqrt{2})$ has degree 2 over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, $\{1, \sqrt{2}\}$ is a basis over $\mathbb{Q}$.

Is $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$? NO: because $(a+b\sqrt{2})^2 = 3$ would imply:

$$a^2+2b^2+2ab\sqrt{2} = 3 \Rightarrow ab = 0 \Rightarrow \text{either } a \text{ or } b \text{ are zero.}$$

But neither $a^2=3$ nor $2b^2=3$ has a rational solution. $\Rightarrow \sqrt{3} \notin \mathbb{Q}(\sqrt{2})$

$\Rightarrow [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$ and $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

Is $\sqrt{5} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$? Look for $5 = (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})^2$ with $a, b, c, d \in \mathbb{Q}$. $\Rightarrow 5 = a^2 + 2b^2 + 3c^2 + 6d^2 + (2ab + 6cd)\sqrt{2} + (2ac + 4bd)\sqrt{3} + (2ad + 2bc)\sqrt{6}$

$\Rightarrow ab + 3cd = 0 = ac + 2bd = ad + bc$

If $d = 0$, then $ab = 0 = ac = bc \Rightarrow$ at least two of a, b, c are 0 and neither $5 = a^2$ nor $5 = 2b^2$ nor $5 = 3c^2$ has a rational solution, so no solution with $d = 0$.

If $d \neq 0$, then $a = -\frac{bc}{d} \Rightarrow -\frac{b^2c}{d} + 3cd = 0 = -\frac{bc^2}{d} + 2bd = -\frac{bcd}{d} + bc$

$\Rightarrow c(3d^2 - b^2) = 0 = b(2d^2 - c^2)$

$\Rightarrow$ since the brackets both have no rational solution, both b and c must be 0, thus also $a = 0$.

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

Thus we have shown: $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) : \mathbb{Q}(\sqrt{2},\sqrt{3})] = 2$ and

$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}, \sqrt{5}, \sqrt{10}, \sqrt{15}, \sqrt{60}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$

In particular, $\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}\}$ is linearly independent.

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

- It contains 0 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 $\mathbb{Q}(a)$:

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(a,b) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(a) \arrow[dr, dash] & & \mathbb{Q}(b) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

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

Therefore, in particular $a+b$, $a \cdot b$, $-a$, $-b$ and a^{-1} and b^{-1} (if $a \neq 0$, $b \neq 0$) 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 $\mathbb{Q}$:

<u>We use:</u> If $f \in \mathbb{Z}[x]$ monic with $f = \sum_{i=0}^{n} a_i x^n$ and $a_n = 1$ and there 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 $\mathbb{Q}[x]$.

$\Rightarrow$ There are irreducible polynomials $X^n - 7$ of arbitrary high degree $\Rightarrow \dim_{\mathbb{Q}}(\mathbb{A}) = \infty$.

8. α is a root of the polynomial X^5-7. This is irreducible by the criterion of 7.
$\Rightarrow$ (a) $[K:\mathbb{Q}]=5$
(b) $\{1, \sqrt[5]{7}, (\sqrt[5]{7})^2, (\sqrt[5]{7})^3, (\sqrt[5]{7})^4\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\alpha)$.
(c) $\mathbb{Q}(\alpha)=\{a+b\sqrt[5]{7}+c(\sqrt[5]{7})^2+d(\sqrt[5]{7})^3+e(\sqrt[5]{7})^4 \mid a,b,c,d,e\in\mathbb{Q}\}$.

9. (a) $\{0,1,\theta,\theta+1,\theta^2,\theta^2+1,\theta^2+\theta,\theta^2+\theta+1\}$
(b) Write abc for $a\theta^2+b\theta+c$ with $a,b,c\in\{0,1\}$

•	000	001	010	011	100	101	110	111
000	000	000	000	000	000	000	000	000
001	000	001	010	011	100	101	110	111
010	000	010	100	110	011	001	111	101
011	000	011	110	101	111	100	001	010
100	000	100	011	111	110	010	101	001
101	000	101	001	100	010	111	011	110
110	000	110	111	001	101	011	010	100
111	000	111	101	010	001	110	100	011

$\theta^3=\theta+1$
$(\theta+1)^2=\theta^2+1$
$(\theta+1)(\theta^2+\theta)=\theta^3+\theta$
$=1$
$(\theta+1)(1+\theta^2)=1+\theta+\theta^2+\theta^3=\theta^2$
$(\theta^2+1)^2=\theta^4+1$
$=\theta^2+\theta+1$

(c)

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

$$(\theta^2+\theta)^3+\theta^2+\theta+1 = \theta^6+\theta^5+\theta^4+\theta^3+\theta^2+\theta+1$$
$$=(\theta+1)^2+\theta^2(\theta+1)+\theta(\theta+1)+\theta^2+1+\theta+1+\theta$$
$$=\theta^2+1+\theta+1+\theta^2+\theta^2+\theta+\theta^2+1+\theta+1+\theta = 0$$

$$(\theta^2)^3+\theta^2+1=\theta^6+\theta^2+1=(\theta+1)^2+\theta^2+1=\theta^2+1+\theta^2+1=0$$
$\Rightarrow \theta^2$ is another root of X^3+X+1

$$\Rightarrow X^3+X+1=(X+\theta)(X+\theta^2)(X+\theta^2+\theta)$$

(d)

No, it did not occur!

10. (a) $\mathbb{Q}(\sqrt{-6}) = \mathbb{Q}(i\sqrt{6})$ is the splitting field since

$$(X^2+6) = (X - i\sqrt{6})(X + i\sqrt{6})$$

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

11. (a) Both have no root in $\mathbb{F}_3$ and are thus irreducible because their degree is 2.

(b) L contains one root and thus the other of x^2+1 (it is the negative of that root).
Thus L is the splitting field.

(c) $(\alpha+1)^2 + (\alpha+1) - 1 = \alpha^2 + 2\alpha + 1 + \alpha + 1 - 1 = -1 + 1 + 1 - 1 = 0$

$\Rightarrow$ L contains a root of g. Thus it contains the other since

$$g = (X - (\alpha+1))(X - \beta) \quad \text{for some } \beta \in L.$$