1. Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$.

(a) Use Galois theory to prove that $\alpha = \sqrt{3} + \sqrt{7}$ is a primitive element for $K/\mathbb{Q}$, i.e. that $K = \mathbb{Q}(\alpha)$. **(6 points)**

Since none of 3, 7, and ~~21~~ 21 are squares in $\mathbb{Q}$, by HW we know $\mathrm{Gal}(K/\mathbb{Q}) \cong C_2 \times C_2$ gen by $\tau: \begin{matrix} \sqrt{3} \to -\sqrt{3} \\ \sqrt{7} \to \sqrt{7} \end{matrix}$ and $\sigma: \begin{matrix} \sqrt{3} \to \sqrt{3} \\ \sqrt{7} \to -\sqrt{7} \end{matrix}$. Let $H \leq \mathrm{Gal}(K/\mathbb{Q})$ be the subgp cor to $\mathbb{Q}(\alpha)$ under the fund. thm. As $\tau(\alpha) = -\sqrt{3} + \sqrt{7} \neq \alpha$ and $\tau(\alpha) = \sqrt{3} - \sqrt{7} \neq \alpha$ and $(\sigma\tau)(\alpha) = -\sqrt{3} - \sqrt{7} \neq \alpha$ we have none of $\sigma, \tau, \sigma\tau$ are in $H$. So $H = \{1\} \Rightarrow \mathbb{Q}(\alpha) = K_H = K$, as needed.

(b) Consider the $\mathbb{Q}$-linear transformation $T\colon K \to K$ where $T(\beta) = \alpha \cdot \beta$. Give the matrix $A$ of $T$ with respect to the $\mathbb{Q}$-basis $\{1, \sqrt{3}, \sqrt{7}, \sqrt{21}\}$ of $K$. **(2 points)**

$\alpha \cdot 1 = \sqrt{3} + \sqrt{7}$

$\alpha \cdot \sqrt{3} = 3 + \sqrt{21}$

$\alpha \cdot \sqrt{7} = 7 + \sqrt{21}$

$\alpha \cdot \sqrt{21} = 7\sqrt{3} + 3\sqrt{7}$

$$A = \begin{pmatrix} 0 & 3 & 7 & 0 \\ 1 & 0 & 0 & 7 \\ 1 & 0 & 0 & 3 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

(c) Describe how you could use the marix $A$ to find express $\alpha^{-1}$ as $a + b\sqrt{3} + c\sqrt{7} + d\sqrt{21}$, where $a, b, c, d \in \mathbb{Q}$. **(2 points)**

$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$ is the $1^{st}$ column of $A^{-1}$.

2. Let $\mathbb{Q} \subset K \subset \mathbb{C}$, where $K/\mathbb{Q}$ is a finite Galois extension. Let $\tau \in \mathrm{Aut}(\mathbb{C})$ by complex conjugation. Prove or disprove: $\tau(K) = K$ and so $\tau$ gives an element of $\mathrm{Gal}(K/\mathbb{Q})$.
**(8 points)**

<u>Claim</u>: $\tau(K) = K$.

Know $K$ must be the splitting field of some separable $f(x) \in \mathbb{Q}(x)$. In particular,

$K = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ where the $\alpha_i$ are all the roots of $f$. For each $i$, we have

$$0 = \tau(f(\alpha_i)) \overset{\text{as } f \in \mathbb{Q}[x]}{=} f(\tau(\alpha_i))$$

and so $\tau(\alpha_i)$ is some other $\alpha_j$. In particular, ~~since~~ $\tau$ gives a bijection of $\{\alpha_1, \ldots, \alpha_k\}$ (the inverse is $\tau$ itself). 

Thus $\tau(K) = \mathbb{Q}(\tau(\alpha_1), \ldots, \tau(\alpha_k)) = K$

as desired.

3. Let $R$ be a principal ideal domain.

(a) If $\alpha$ is an irreducible element of $R$, prove that the ideal $I = (\alpha)$ is maximal. **(4 points)**

Suppose $J$ is an ideal with $I \subseteq J \subseteq R$. As $R$ is a PID, $J = (\beta)$. As $\alpha \in J$, have $\alpha = \gamma\beta$. ~~If~~ As $\alpha$ is irred, one of $\gamma, \beta$ is a unit. If $\gamma$ is unit, then $I = J$. If instead $\beta$ is a unit, $J = R$. Thus $I$ is maximal.

(b) Prove that any proper ideal $I$ of $R$ is contained in a maximal ideal. **(6 points)**

Suppose $I = (\alpha)$ and $\alpha = \gamma \alpha_1 \cdot \alpha_2 \cdots \alpha_k$ where $\gamma$ is a unit and the $\alpha_i$ are irred. Must have at least one $\alpha_i$ or else $I = R$.

Then $J = (\alpha_1)$ is maximal by (a) and contains $I$ since $\alpha = \alpha_i(\text{stuff})$.

(c) Does (a) remain true if $R$ is just a UFD? Prove your answer. **(2 points)**

No. $\mathbb{Q}[x,y]$ is a UFD where $x$ is irred ~~for~~ but $\mathbb{Q}[x,y]/(x) \cong \mathbb{Q}[y]$ is not a field.

4. Consider the cyclotomic field $K = \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/5}$. We know $K/\mathbb{Q}$ is Galois with group $G \cong (\mathbb{Z}/5\mathbb{Z})^\times$.

(a) What is the minimal polynomial of $\zeta$ over $\mathbb{Q}$? **(2 points)**

The prob reminds us that $[K:\mathbb{Q}] = |G| = 4 = \varphi(5)$

so $\Phi_4(x) = x^4 + x^3 + x^2 + x + 1$ with $\Phi_4(x)\cdot(x-1) = x^5 - 1$

(b) How many subfields $L$ of $K$ are there with $[L:\mathbb{Q}] = 2$? **(2 points)**

Have $G \cong C_4$ generated by $2 \in (\mathbb{Z}/5\mathbb{Z})^\times$ and $C_4$ has a single nontrivial subgp ($\cong C_2$). So exactly one such $L$.

(c) Let $\sigma \in G$ send $\zeta \mapsto \zeta^2$. Find the corresponding fixed field $K_{\langle\sigma\rangle}$. **(4 points)**

Note $|\sigma| = 4$ since $\zeta \to \zeta^2 \to \zeta^4 \to \zeta^8 = \zeta^3 \to \zeta$

and $\{\zeta, \zeta^2, \zeta^3, \zeta^4\}$ are distinct elts of $K$.

In part, $\langle\sigma\rangle = G$ and so $K_{\langle\sigma\rangle} = \mathbb{Q}$.

(d) Find the minimal polynomial of $\overbrace{\zeta^2 + \zeta^3}^{=\alpha}$ over $\mathbb{Q}$. Your answer should not involve $\zeta$. **(4 points)**

Applying $\sigma$, we see $\sigma(\alpha) = \zeta^4 + \zeta =: \beta$ and $\sigma(\beta) = \alpha$.

So $G\cdot\alpha = \{\alpha, \beta\}$ and

$m_{\alpha,\mathbb{Q}}(x) = (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta$

Now $\alpha + \beta = \zeta + \zeta^2 + \zeta^3 + \zeta^4 = -1$ (by (a))

and $\alpha\cdot\beta = (\zeta^2+\zeta^3)(\zeta+\zeta^4) = \zeta^3 + \zeta^6 + \zeta^4 + \zeta^7 = -1$

So $m_{\alpha,\mathbb{Q}}(x) = x^2 + x - 1$.

5. Let $F$ be a field of characteristic 0. Let $K$ be the splitting field of an irreducible *cubic* $f(x) \in F[x]$. Let $\alpha_1, \alpha_2, \alpha_3 \in K$ be the roots of $f$, and suppose that $G = \mathrm{Gal}(K/F)$ is all of $S_3$.

(a) Show that $F = \mathbb{Q}$ and $f(x) = x^3 + x + 1$ is an example of this situation, i.e. that $f$ is irreducible in $\mathbb{Q}[x]$ and $G = S_3$. **(4 points)**

$f$ is irred as $\bar{f} \in \mathbb{F}_2[x]$ has no roots in $\mathbb{F}_2$ and $\deg \leq 3$.
As $f'(x) = 3x^2+1$ has no real roots, $f$ has only one real root. In part, complex conj gives an elt of $G$ of order 2. As $G$ is either $C_3$ or $S_3$, it must be $S_3$.

(b) Returning to the general case, for each $j$ find the subgroup of $G$ that corresponds to $F(\alpha_j)$. **(2 points)**

$F(\alpha_1) \longleftrightarrow \langle (23) \rangle \qquad F(\alpha_3) \longleftrightarrow \langle (12) \rangle$

$F(\alpha_2) \longleftrightarrow \langle (13) \rangle$

(c) Prove that $F(\alpha_1) \cap F(\alpha_2) = F$. **(2 points)**

The subgp of $G$ coor to $F(\alpha_1) \cap F(\alpha_2)$ is $\langle (23), (13) \rangle$ which contains $(123) = (23)\cdot(13)$ and hence is all of $G$. Thus $F(\alpha_1) \cap F(\alpha_2) = F$. by the Fund Thm.

(d) Prove that $\mathrm{Aut}(F(\alpha_1)/F)$ is trivial. **(4 points)**

If $\sigma \in \mathrm{Aut}(F(\alpha_1)/F)$, then $\sigma(\alpha_1)$ is one of $\{\alpha_1, \alpha_2, \alpha_3\}$ since $f \in F[x]$. By (c), $\alpha_2 \notin F(\alpha_1)$ and the same follows for $\alpha_3$. So $\sigma(\alpha_1) = \alpha_1$ and since $\alpha_1$ generates $F(\alpha_1)$ we have $\sigma = \mathrm{id}_{F(\alpha_1)}$

(e) Consider $\beta = \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2$. Prove that $K \neq F(\beta)$. **(2 points)**

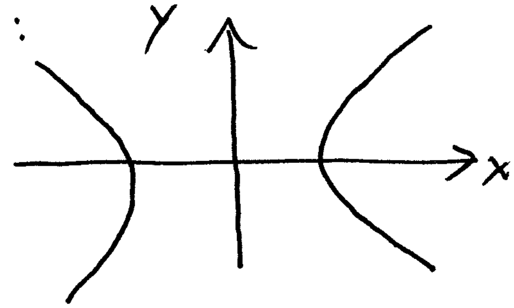
Note $\sigma = (123)$ fixes $\beta$ since
$\sigma(\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2) = \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2 + \alpha_1\alpha_2^2$. So
$\beta \in K_{\langle\sigma\rangle}$ where $[K : K_{\langle\sigma\rangle}] = |\langle\sigma\rangle| = 3$. So $[K:F] \geq 3$.

6. Consider the plane curve $X = \mathbf{V}(\overbrace{x^2 - y^2 - 1}^{f}) \subset \mathbb{R}^2$.

(a) Prove that $X$ is smooth, and draw a picture of it. **(4 points)**

$\nabla f = (2x, -2y)$ and so $\nabla f = 0 \Rightarrow (x,y) = (0,0)$ which is not in $X$. So $X$ is smooth:

$x = \pm\sqrt{1+y^2}$



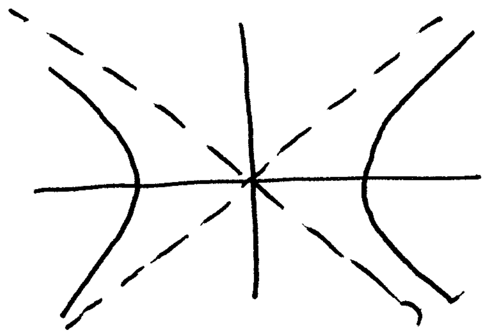

(b) Let $\overline{X}$ be the corresponding curve in $\mathbb{P}^2_{\mathbb{R}}$. Find the defining equation for $\overline{X}$ in $\mathbb{R}[x, y, z]$, and find all the points in $\overline{X} - X$, i.e. all points at infinity. **(2 points)**

$g = x^2 - y^2 - z^2 \quad \overline{X} \cap \mathbb{P}^1_\infty = \{(x:y:0) \mid g(x,y,0) = 0\}$

$= \{(x:y:0) \mid x^2 = y^2 \Rightarrow x = \pm y\} = \{(1:1:0), (1:-1:0)\}$

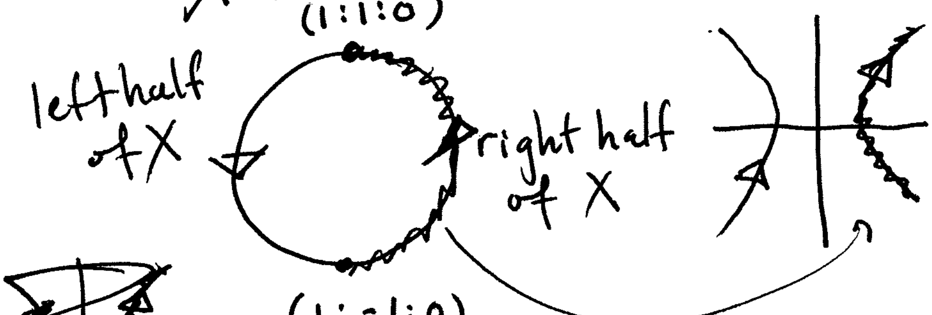
(c) Explain why your answers in (a) and (b) are consistent with the view that $\mathbb{P}^2_{\mathbb{R}}$ is $\mathbb{R}^2$ plus one point for each family of parallel lines in $\mathbb{R}^2$. **(2 points)**

The asymptotes of the hyp. $X$ corr to the pts at infinity



(d) What is the topology of $\overline{X}$? What about if we replace with $\mathbb{R}$ with $\mathbb{C}$? You do not need to justify your answer, but should draw pictures. **(2 points)**

$\overline{X}$ is a circle




Over $\mathbb{C}$, $\overline{X}$ is  $\cong \mathbb{P}^1_{\mathbb{C}}$ like any smooth conic.

7. Let $V$ be the plane curve $\mathbf{V}(x^2 - y^2 - 1) \subset \mathbb{C}^2$, which is irreducible. Let $K = \mathbb{C}(V)$ be the function field.

(a) Consider the rational function on $V$ given by

$$f = \frac{x^2 - y - 1}{y - 1} \in K$$

Prove that $\mathrm{dom}(f) = V$, even though the denominator vanishes at $(\sqrt{2}, 1) \in V$. **(4 points)**

In $\mathbb{C}[V]$, have $x^2 = y^2 + 1$, so can rewrite the numerator as $y^2 - y = y(y-1)$. So $f = y/1$ is another valid expression for $f$ and so $\mathrm{dom}(f) = V$.

(b) Consider $h(x, y) = x$ in $\mathbb{C}[V]$ as a map $V \to \mathbb{C}$. Let $F = \mathbb{C}(\mathbb{C}) = \mathbb{C}(t)$, and consider $h^*\colon F \to K$ be the induced homomorphism of fields. As this is 1-1, identify $F$ with its image under $h^*$. Describe the extension $K/F$ as $F[u]/(p(u))$ for some *irreducible* polynomial $p(u) \in F[u]$. **(6 points)**

As $h^*(t) = x$, have $h^*(\mathbb{C}(t)) = \mathbb{C}(x)$ inside $K$. Now $K/\mathbb{C}$ is gen. by $x, y$ and so $K = F(y)$. Since $x^2 - y^2 - 1 = 0$ in $\mathbb{C}[V]$, if $p(u) = u^2 + (1 - x^2)$ in $F[u]$ then $p(y) = 0$. Moreover, $p(u)$ is red $\Leftrightarrow$ $p$ has a root in $F \overset{\text{Gauss}}{\Leftrightarrow}$ $p$ has a root in $\mathbb{C}[x] \Leftrightarrow x^2 - 1$ is a square in $\mathbb{C}[x]$. The latter is false as if $x^2 - 1 = (f(x))^2$ then $f$ is monic and linear (i.e $= x + a$) and so $f^2$ has a nonzero linear term. So $p(u) = m_{y,F}(u)$ and $K \cong F[u]/p(u)$.

(c) Is $K/F$ Galois? If it is, describe how each element of $\mathrm{Gal}(K/F)$ acts on $K$. **(2 points)**

Yes since $[K : F] = 2$. $\mathrm{Gal}(K/F) \cong C_2$ generated by $\sigma : y \longmapsto -y$.

8. Throughout, let $k$ be an algebraically closed field.

(a) Suppose $V_1, V_2 \subset k^n$ are affine varieties defined by $V_i = \mathbf{V}(I_i)$. Prove directly from the definitions that $V_1 \cup V_2 = \mathbf{V}(I_1 \cap I_2)$ **(4 points)**

($\subseteq$): If $p \in V_1 \cup V_2$ and $f \in I_1 \cap I_2$ then $p$ in one $V_i$. Since $V_i = \mathbb{V}(I_i)$ and $f \in I_i$ we have $f(p) = 0$ $\Rightarrow p \in \mathbb{V}(I_1 \cap I_2)$.

($\supseteq$) Suppose $p \in \mathbb{V}(I_1 \cap I_2)$ is not in ~~$V_1 \cap V_2$~~ $V_1 \cup V_2$. Pick $f_i \in I_i$ with $f_i(p) \neq 0$. Then $f_1 f_2 \in I_1 \cap I_2$ since the $I_i$ are ideals, but $(f_1 f_2)(p) = f_1(p) \cdot f_2(p) \neq 0$, a contrad. So $p \in V_1 \cup V_2$.

(b) Let $J_1$ and $J_2$ be radical ideals in $k[x_1, \ldots, x_n]$. Prove that $I = J_1 \cap J_2$ is also a radical ideal, i.e. that $f^n \in I \Rightarrow f \in I$. **(2 points)**

Suppose $f^n \in I$. Then for each $i$, ~~the~~ have $f^n \in J_i \Rightarrow f \in J_i$ as $J_i$ is radical. So $f \in J_1 \cap J_2 = I$.

(c) Show that $\mathbf{I}(V_1 \cup V_2) = \mathbf{I}(V_1) \cap \mathbf{I}(V_2)$. **(4 points)**

Nullstellensatz time!

Set $I_i := \mathbb{I}(V_i)$ so that $V_i = \mathbb{V}(I_i)$ as "$\mathbb{V}(\mathbb{I}(V)) = V$". By (a), have $V_1 \cup V_2 = \mathbb{V}(I_1 \cap I_2)$. By the Null-satz, $\mathbb{I}(V_1 \cup V_2) = \mathbb{I}(\mathbb{V}(I_1 \cap I_2)) = \mathrm{rad}(I_1 \cap I_2) = I_1 \cap I_2$ by (b). So $\mathbb{I}(V_1 \cup V_2) = \mathbb{I}(V_1) \cap \mathbb{I}(V_2)$ as desired.