January 2014:

(5) - M invertible $n\times n$ matrix with real entries and $\det(M)>0$. We want $M=RK$ where R is a rotation (some guy in $SO(n)$) and K upper triangular, with positive entries in the diagonal.

M is invertible, so its column vectors form a basis. By orthogonalization, we can find a change of basis matrix (which will be R), and then what remains will be K. What remains to check is that the diagonal of K has positive entries.

Say $M=[v_1 \cdots v_n]$, where $v_i\in\mathbb{R}^n$ form a basis. By Gram-Schmidt we can find an orthonormal basis:

$$x_1 := \frac{v_1}{\sqrt{\langle v_1, v_1\rangle}}, \text{ then}$$

$$x_i := \frac{v_i}{\sqrt{\langle v_i, v_i\rangle}} - \sum_{j<i} \frac{\langle x_j, v_i\rangle}{\langle x_j, x_j\rangle}\cdot x_j \qquad (\Delta)$$

Then the matrix $R = [x_1 \cdots x_n]$ is orthogonal / orthonormal

(because Gram-Schmidt says so).

We want:

$$[v_1 \cdots v_n] \underset{\text{I}}{=} [x_1 \cdots x_n] \begin{bmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & & \vdots \\ m_{n1} & \cdots & m_{nn} \end{bmatrix}$$

Now: $v_1 = x_1 \cdot \sqrt{\langle v_1, v_1 \rangle}$, so $m_{11} := \sqrt{\langle v_1, v_1 \rangle}$

$m_{j1} := 0$ for $j \neq 1$.

Note: $$\frac{\langle x_i, v_j \rangle}{\langle x_i, x_i \rangle} \cdot x_i = \langle x_i, v_j \rangle \cdot x_i$$

because x_i has norm 1 by construction.

Using this in the definition of x_i we find:

$$(\text{A}) \quad v_i = x_i \cdot \sqrt{\langle v_i, v_i \rangle} + \sum_{j<i} \langle x_j, v_i \rangle \cdot x_j$$

$$K = \begin{bmatrix} * & * & * \\ & \ddots & * \\ 0 & & \ddots \end{bmatrix}$$

this is the multiplication I !!!

So $m_{ij} = \langle x_j, v_i \rangle$ for $j<i$. (above diagonal).

$m_{ii} = \sqrt{\langle v_i, v_i \rangle}$ (for $i = 1, \dots, n$). (diagonal).

$m_{ij} = 0$ for $i > j$. (below diagonal).

defines K.

Indeed the diagonal of K has all positive entries.

7 - $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$.

Prove the Galois group is $\mathbb{Z}/(4)$, find a generator and determine action on roots.

Roots: $\pm\sqrt{2 \pm \sqrt{2}}$. Then $\mathbb{E} = \mathbb{Q}(\pm\sqrt{2\pm\sqrt{2}})$.

Say $\alpha := \sqrt{2+\sqrt{2}}$. Now: $\underset{2+\sqrt{2}}{\alpha^2} \in \mathbb{E}$ so $\sqrt{2} \in \mathbb{E}$.

Then:

$$-\sqrt{2+\sqrt{2}} = -\alpha \ ; \ \frac{\alpha^2 - 2}{\alpha} = \sqrt{2-\sqrt{2}}$$

$$; \ \frac{\alpha^2 - 2}{-\alpha} = -\sqrt{2-\sqrt{2}}$$

So $\mathbb{E} = \mathbb{Q}(\alpha)$.

G permutes the roots, so it suffices to see where an element of G sends α.

$\mathrm{id}: \alpha \longmapsto \alpha$ the identity.

$\sigma: \alpha \longmapsto -\alpha$ has order 2.

$\tau: \alpha \longmapsto \dfrac{\alpha^2-2}{\alpha}$ has order 4. generates them all

$\gamma: \alpha \longmapsto \dfrac{\alpha^2-2}{-\alpha}$ has order 4.

$\tau^2 = \sigma$.
$\tau^3 = \gamma$.
$\tau^4 = \mathrm{id}$.

So $G \cong \langle \tau \rangle \cong \mathbb{Z}/(4)$.

Why do τ or γ exist?

$$\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{E} = \mathbb{Q}(\alpha), \qquad \mathbb{F} = \mathbb{Q}(\sqrt{2})$$

In $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ we do have:

$\mathrm{id}|_{\mathbb{F}}: 2+\sqrt{2} \longmapsto \alpha^2 = 2+\sqrt{2}$

$\delta: 2+\sqrt{2} \longmapsto -\alpha^2$. And these guys <u>do</u> exist.

In $\mathrm{Gal}(\mathbb{Q}(\alpha), \mathbb{Q}(\sqrt{2}))$ we do have:

$\mathrm{id}|_{\mathbb{F}}$ extends by sending $\frac{\alpha^2-2}{\alpha} \longmapsto \frac{\alpha^2-2}{\alpha}$:

$\frac{\alpha^2-2}{\alpha} \longmapsto \frac{\alpha^2-2}{-\alpha}$

$\mathrm{id}: \sqrt{2}+2 \longmapsto \sqrt{2}+2$

$\alpha \longmapsto \alpha$

$\sigma: \sqrt{2}+2 \longmapsto \sqrt{2}+2$

$\alpha \longmapsto -\alpha$

δ extends by sending $\frac{\alpha^2-2}{\alpha} \longmapsto \frac{\alpha^2-2}{\alpha}$:

$\frac{\alpha^2-2}{\alpha} \longmapsto \frac{\alpha^2-2}{-\alpha}$

$\tau: \sqrt{2}+2 \longmapsto -\sqrt{2}-2$

$$\frac{\alpha^2-2}{\alpha} = \tau\left(\frac{\alpha^2-2}{\alpha}\right) = \frac{\tau(\alpha^2-2)}{\tau(\alpha)} = \frac{\tau(\alpha^2)-2}{\tau(\alpha)} =$$

$$= \frac{-\alpha^2-2}{\tau(\alpha)} \Rightarrow \tau(\alpha) = \frac{\alpha(-\alpha^2-2)}{\alpha^2-2} =$$

$$= \frac{\alpha\cdot(-\sqrt{2}-2-2)}{\sqrt{2}+2-2} =$$

$$= \alpha \cdot \frac{-\sqrt{2}-4}{\sqrt{2}}$$

$\gamma: \sqrt{2} \longmapsto \sqrt{2}$

$\alpha \longmapsto -\alpha$

$$\frac{\alpha^2-2}{-\alpha}$$

$$\frac{\alpha^2-2}{\alpha}$$ annihilates it.

$\alpha^2 = \sqrt{2}+2$ annihilates it

$$x^4-4x^2+2 = f(x) = \overbrace{(x^2-\sqrt{2}-2)}(\overbrace{x^2+\sqrt{2}-2})$$

$$= (x+\sqrt{2+\sqrt{2}})(x-\sqrt{2+\sqrt{2}})(x-\sqrt{2-\sqrt{2}})(x+\sqrt{2-\sqrt{2}})$$

⑧ - p, q prime numbers

(a) Define surj. map:

$$\phi : \mathbb{Q}(\sqrt{p}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{q}) \to \mathbb{Q}(\sqrt{p}, \sqrt{q})$$

that is $\mathbb{Q}$-linear and ring homomorphism.

$$\Phi : \mathbb{Q}(\sqrt{p}) \times \mathbb{Q}(\sqrt{q}) \longrightarrow \mathbb{Q}(\sqrt{p}, \sqrt{q})$$

$$(a+b\sqrt{p}, c+d\sqrt{q}) \longmapsto ac + bc\sqrt{p} + ad\sqrt{q} + bd\sqrt{pq}.$$

This is $\mathbb{Q}$-balanced ($\mathbb{Q}$-bilinear and for all $r \in \mathbb{Q}$ $\Phi(\alpha \cdot r, \beta) = r \cdot \Phi(\alpha, \beta) = \Phi(\alpha, r\cdot\beta)$).

This gives $\phi: \mathbb{Q}(\sqrt{p}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{q}) \longrightarrow \mathbb{Q}(\sqrt{p}, \sqrt{q})$.

a surjective group homomorphism with $\phi(\alpha \otimes \beta) = \alpha \cdot \beta$.

$\mathbb{Q}(\sqrt{p}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{q})$ has identity, addition as a $\mathbb{Q}$-v.s., and component-wise multiplication:

$$\alpha \otimes \beta \cdot \gamma \otimes \delta := (\alpha\gamma) \otimes (\beta\delta)$$

$$r \otimes 1 \cdot 1 \otimes s := r \otimes s = rs \otimes 1 = sr \otimes 1 =$$
$$= s \otimes r = s \otimes 1 \cdot 1 \otimes r$$

for all $r, s \in \mathbb{Q}$. So multiplication is well defined.

This gives $\mathbb{Q}(\sqrt{p}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{q})$ a ring structure.

For ϕ to be a ring homomorphism we need:

(i) $\phi(1 \otimes 1) = 1$. ← true

ϕ group hom.

(ii) $\phi(\alpha \otimes \beta + \gamma \otimes \delta) = \phi(\alpha \otimes \beta) + \phi(\gamma \otimes \delta)$

(iii) $\phi((\alpha \otimes \beta) \cdot (\gamma \otimes \delta)) = \phi(\alpha \otimes \beta) \cdot \phi(\gamma \otimes \delta)$ ← true.

(b) If p, q distinct, show ϕ is iso.

If p, q distinct primes, then $\mathbb{Q}(\sqrt{p},\sqrt{q})$ has dimension 4.

Also $\mathbb{Q}(\sqrt{p})\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{q})$ has dimension 4:

$\{1\otimes 1, \sqrt{p}\otimes 1, 1\otimes\sqrt{q}, \sqrt{p}\otimes\sqrt{q}\}$ is a basis.

Since ϕ is surj., it is inj., and ϕ is iso.

(c) If $p = q$, find a $\mathbb{Q}$-basis of $\ker(\phi)$.

Look at matrix representation of ϕ:

$e_1 \quad 1\otimes 1 \longmapsto 1$

$e_2 \quad \sqrt{p}\otimes 1 \longmapsto \sqrt{p}$

$e_3 \quad 1\otimes\sqrt{p} \longmapsto \sqrt{p}$

$e_4 \quad \sqrt{p}\otimes\sqrt{p} \longmapsto \sqrt{p}^2 = p$, basis on $\mathbb{Q}(\sqrt{p})$ is $\{1, \sqrt{p}\}$.

$$4 \xrightarrow{M} 2$$

$$\begin{bmatrix} * \\ * \\ * \\ * \end{bmatrix} \qquad \begin{bmatrix} * \\ * \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 & p \\ 0 & 1 & 1 & 0 \end{bmatrix}\begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{bmatrix}$$

This says that $\ker(\phi)$ has dimension 2. So we need to find two linearly independent vectors in $\ker(\phi)$.

$$\left.\begin{array}{l}\phi(v_1 - \frac{1}{p}v_4) = 0 \\ \phi(v_2 - v_3) = 0\end{array}\right\}$$ and $v_1 - \frac{1}{p}v_4$, $v_2 - v_3$ are linearly independent.

So $\ker(\phi) = \langle v_1 - \frac{1}{p}v_4, v_2 - v_3 \rangle$.

January 2013:

① - $|G| = 56 = 2^3 \cdot 7$. Show G is not simple.

By Sylow 3 we have: $n_7 = 1$ or 8.
If $n_7 = 1$, we are done.
If $n_7 = 8$, we look at $n_2 = 1$ or 7.
We have $8 \cdot 6 = 48$ elements of order 7. We then have 8 elements left, since the Sylow 2-subgroup must have order 8, we must have $n_2 = 1$. We are done.

② - $|G| = 200 = 2^3 \cdot 5^2$. We want $\phi : G \longrightarrow S_8$ with proper, non-trivial kernel.

We have a Sylow 5-subgroup H with 25 elements, by Sylow 1. Take $A := \{g_1 H, \ldots, g_8 H\}$ the left cosets, we have $8 = \frac{200}{25} = [G:H]$ of them. take $g_1 = e \in G$

We have a left translation inducing $G \curvearrowright A$. This induces a group homomorphism $\phi : G \longrightarrow S_8$

$$g \mapsto \left(\begin{aligned} \tilde{g} : A &\longrightarrow A \\ g_i H &\longmapsto (g g_i) H \end{aligned} \right).$$

Notice that any $h \in H$ is in $\ker(\phi)$:

$\phi(h)(H) = (h g_1) H = h H = H$ but $h \neq e$. Thus $\ker(\phi)$ is not trivial.

$g_i H = H$ iff $g_i \in H$.

Suppose $g \in G \setminus H$, we want to see that $gH \neq H$. Since being in the cosets is an equivalence class, this holds.

③ - Examples of:

(i) Eisenstein $p = 5$ over $\mathbb{Q}$: $x^2 + 5x + 10$.

(ii) UFD not PID: $k[x,y]$ is UFD.
(x,y) is not principal.

(iii) Finite extension of $\mathbb{F}_p(x)$ that is normal, not separable:

An extension E/K is normal if it satisfies any of the following:

1. Every embedding $\sigma : E \to \overline{K}$ over K induces an automorphism of E. $(\sigma(E) = E)$.
2. E is the splitting field of K for some polynomials in $K[x]$.
3. Every irreducible poly. of $K[x]$ with a root in E must split in E.

An extension E/K is separable whenever every element of E is separable over K, that is the irreducible polynomial over K of every element in E has no repeated roots (in $\overline{K}$).

Candidate: $t^p - x$ is irreducible in $\mathbb{F}_p(x)$.

The splitting field of $t^p - x$ is normal but not separable (since $t^p - x$) has only one root.

④ - R comm. ring with $1 \neq 0$. M is f.g., N Noetherian.

Show $M \otimes_R N$ is Noetherian.

We want to see that every submodule of $M \otimes_R N$ is finitely generated.

Take $L \subseteq M \otimes_R N$ an R-submodule. We want to see that L is f.g., that is, L is the homomorphic image of a free module, that is, there is $\ell \in \mathbb{N}$ with

$$R^\ell \xrightarrow{\phi} L.$$

So it is good enough to find some exact sequence:

$$0 \to \ker \phi \to R^\ell \to L \to 0.$$

Idea: use functor $? \otimes_R N$.

Note: M is f.g. So we have $\psi : R^m \twoheadrightarrow M$ a module homomorphism, surjection, $m \in \mathbb{N}$. Now:

$$0 \to \operatorname{Ker}\psi \to R^m \to M \to 0 \quad \text{is exact.}$$

Apply $? \otimes_R N$, we obtain:

$$\operatorname{Ker}\psi \otimes_R N \longrightarrow \underset{\substack{\cong\\ N^m}}{R^m \otimes_R N} \xrightarrow{\psi \otimes 1_N} M \otimes_R N \longrightarrow 0$$

is exact.

☑ M f.g.
☐ N Noetherian.

we want this to be Noetherian.

Recall: direct sums of Noetherian modules are Noetherian. Hungerford VIII.1.7.

So N^m is Noetherian.

Homomorphic images of Noetherian modules are Noetherian. Hungerford VIII.1.6.

So $M \otimes_R N \cong \operatorname{Im}(\psi)$ is Noetherian.
$= \psi(N^m)$

<u>Alternatively:</u> ascending chain condition.

5 – TBD.

6 –

7 –

8 – R ring with $1 \neq 0$, M a f.g. R-mod.

(a) Suppose M is projective, we want elements $m_1, \dots, m_k \in M$ and $f_i : M \longrightarrow R$, $1 \leq i \leq k$ such that:

$$m = \sum_{i=1}^{k} f_i(m) m_i .$$

M is f.g. so $R^k \xrightarrow{\phi} M$ a surjective homomorphism exists.

$$m = \sum_{i=1}^{k} r_i m_i$$ by M f.g., m_i generators over R. $r_i \in R$.

$$\begin{tikzcd} & M \arrow[dl, dashed, "h"'] \arrow[d, "1_M"] & \\ F = R^k \arrow[r, "\phi"] & M \arrow[r] & 0 \end{tikzcd}$$

By projectivity of M there is $h : M \to F$ with $\phi h = 1_M$.

Define $f_i(m) := \phi(r_i)$ for $f_i : M \longrightarrow R$.

Write:

$$m = 1_M(m) = \phi h(m) = \phi h\left(\sum_{i=1}^{k} r_i m_i\right) =$$
$$= \phi\left(\sum_{i=1}^{k} r_i h(m_i)\right) = \sum_{i=1}^{k} \phi(r_i h(m_i)) =$$
$$= \sum_{i=1}^{k} r_i \, \phi(h(m_i)) = \sum_{i=1}^{k} f_i(m) m_i .$$

(b) Prove that the converse is true.

We want M to be projective knowing that there are $m_1, \dots, m_k \in M$ and $f_i : M \longrightarrow R$, $1 \leq i \leq k$ with
$$m = \sum_{i=1}^{k} f_i(m) m_i .$$