January 2013:

⑤ - R comm. ring with $1 \neq 0$, N left R-mod.

P prime ideal, R_P, N_P localizations. Show:

$N = \{0\} \Leftrightarrow N_P = \{0\}$ for all $P \Leftrightarrow N_M = \{0\}$ for all maximal M.

(i) $\Rightarrow$ (ii): If $N = \{0\}$ then any two elements in N_P are $(0, r), (0, s)$ for some $r, s \in R \setminus P$. Since: $r \cdot 0 = 0 = s \cdot 0$ then $(0, r) = 0 = (0, s)$. so $N_P = \{0\}$.

(ii) $\Rightarrow$ (iii): Every maximal ideal over a ring with unity is prime.

(iii) $\Rightarrow$ (i): Trick: proof by contrapositive.

Assume $N \neq \{0\}$, then we will show

that $N_M \neq \{0\}$ for a M maximal.

Take $x \in N$ not zero, $A(x)$ the

annihilator of x:

$$\{r \in R \mid r \cdot x = 0\} =: \mathcal{A}(x).$$

We have $\mathcal{A}(x) \subseteq R$, and $\mathcal{A}(x) \neq \emptyset$

since $0 \in \mathcal{A}(x)$, and $\mathcal{A}(x) \neq R$

since $1 \notin \mathcal{A}(x)$ because $1 \cdot x = x \neq 0$.

Either use or prove that $\mathcal{A}(x)$ is ideal.

Thus there is a maximal ideal M

containing $\mathcal{A}(x)$. We claim that

$N_M \neq \{0\}$, because $(x,1) \neq (0,1)$.

Suppose $(x,1) = (0,1)$, then there is

$r \in R \setminus M$ such that $r \cdot (1 \cdot x - 1 \cdot 0) = 0$,

but then $0 = r \cdot x$, so $r \in \mathcal{A}(x) \subset M$.

Contradiction. Thus $N_M \neq \{0\}$.

⑥ - $V = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, $K = \mathbb{Q}(\sqrt{2})$

(a) $V/\mathbb{Q}$ is a Galois extension. Determine $\mathrm{Gal}(V/\mathbb{Q})$.

For $V/\mathbb{Q}$ to be Galois it needs to be normal and separable.

Take $\alpha = \sqrt{2}+\sqrt{3}$, proceed to compute $\alpha^2, \alpha^3, \alpha^4$, and find relations between them.

$$\underbrace{\sqrt{2}+\sqrt{3}}_{\alpha_1},\quad \underbrace{-(\sqrt{2}+\sqrt{3})}_{\alpha_2},\quad \underbrace{\sqrt{2}-\sqrt{3}}_{\alpha_3},\quad \underbrace{-\sqrt{2}+\sqrt{3}}_{\alpha_4}$$

<u>Claim:</u> The polynomial:

$$f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4) =$$

$$= (x^2-5-2\sqrt{6})(x^2-5+2\sqrt{6}) = x^4-10x^2+1.$$

This usually works for $\sqrt{p}+\sqrt{q}$, p,q coprime, and $\sqrt{p+\sqrt{q}}$ (for $\pm\sqrt{p\pm\sqrt{q}}$).

is the minimal polynomial of $\sqrt{2}+\sqrt{3}$.

For this we will show that f is irreducible over $\mathbb{Q}$.

Since f is primitive, it is good enough to show that f is irreducible over $\mathbb{Z}$.

Hungerford III.6.13

Since the roots of f are <u>not</u> in $\mathbb{Z}$, if it were to factor over $\mathbb{Z}$ it would have to be in quadratic terms:

$$f(x) = (x^2+ax+b)(x^2+cx+d) \quad , \; a,b,c,d \in \mathbb{Z}$$

$$\left.\begin{aligned} &(a+c)x^3 = 0 . \\ &(b+d+ac)x^2 = -10x^2 . \\ &(ad+bc)\,x = 0 . \\ &bd = 1 . \end{aligned}\right\} \quad \begin{aligned} &c = -a , \\ &b,d = \pm 1 , \\ &\text{so: } \; -a^2 = -12 . \\ &\text{or: } \; -a^2 = -8 . \end{aligned}$$

This has no solutions in $\mathbb{Z}$.

So f indeed is irreducible over $\mathbb{Q}$.

Claim: V is the splitting field of f.

$$\underset{\alpha_1}{\sqrt{2}+\sqrt{3}}, \quad \underset{\alpha_2}{-(\sqrt{2}+\sqrt{3})}, \quad \underset{\alpha_3}{\sqrt{2}-\sqrt{3}}, \quad \underset{\alpha_4}{-\sqrt{2}+\sqrt{3}}$$

$$\alpha_2 = -\alpha_1 \in \mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha).$$

$$\alpha_3 = \frac{-1}{\alpha_1} \in \mathbb{Q}(\alpha_1).$$

$$\alpha_4 = -\alpha_3 \in \mathbb{Q}(\alpha_1).$$

$\sqrt{p+\sqrt{q}}$ works for the same reason.

So all the roots of f are in V.

So V is the splitting field of f irreducible polynomial, everything over $\mathbb{Q}$.

normal

separable

Hungerford V.3.11.

To compute $\mathrm{Gal}(V/\mathbb{Q})$ use magic:

Hungerford V.4.11

$a = \alpha_1\alpha_2 + \alpha_3\alpha_4 = -10.$

$b = \alpha_1\alpha_3 + \alpha_2\alpha_4 = -2.$

$c = \alpha_1\alpha_4 + \alpha_2\alpha_3 = 2.$

Then $\mathbb{Q} = \mathbb{Q}(a,b,c)$, so:

$$\mathrm{Gal}(V/\mathbb{Q}) \cong \mathbb{Z}/(2) \oplus \mathbb{Z}/(2).$$

<u>Comment:</u> The isomorphism extension theorem: 1.8 Papanikolas also works.

(b) $T: V \longrightarrow V$. Check: T linear.

$\alpha \longmapsto (1+\sqrt{2})\alpha$

Choose a basis of V, represent T in matrix form, find $\mathrm{char}(T)$.

Notice: if $(1+\sqrt{2})\alpha \in V$ then using $\alpha^{-1} \in V$ we have $\sqrt{2} = \dfrac{(1+\sqrt{2})\alpha}{\alpha} - 1 \in V.$

We need to justify $\sqrt{2} \in V$, and/or $\sqrt{3} \in V$. (*)

$(\sqrt{2}+\sqrt{3}) + (\sqrt{2}-\sqrt{3}) = 2\cdot\sqrt{2}$ in V so $\sqrt{2} \in V$.

Similarly $\sqrt{3} \in V$. Notice: $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

$\supseteq$ clear

$\subseteq$ by (*).

Now:

$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ must be a basis of V, because

x^2-3 irreducible over $\mathbb{Q}(\sqrt{2})$

so $V = \mathbb{Q}(\sqrt{2})(\sqrt{3})$.

Up til now, we have seen that T is well defined.

Now $T(\alpha) = r\cdot\alpha$ for some $r \in V$, so T will be linear because it is a multiplication by a scalar.

Alternatively, hand check that:

$$T(\alpha+\beta) = T(\alpha) + T(\beta)$$

$$T(s\cdot\alpha) = s\cdot T(\alpha) \quad , \quad \alpha,\beta \in V, \ s \in \mathbb{Q}.$$

To write T using the basis:

$T(1) = 1 + \sqrt{2}$

$T(\sqrt{2}) = 2 + \sqrt{2}$

$T(\sqrt{3}) = \sqrt{3} + \sqrt{6}$

$T(\sqrt{6}) = 2\sqrt{3} + \sqrt{6}$

so $T = \begin{bmatrix} 1 & 2 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 \end{bmatrix}$.

Hence:

$$\mathrm{char}(T) = \det(\mathbb{1} - \lambda T) = \cdots = ((1-\lambda)^2 - 2)^2$$

(c) $id : K \to K$, $K = \mathbb{Q}(\sqrt{2})$, find a K basis for $K \otimes_{\mathbb{Q}} V$ consisting of eigenvectors of:

$$id \otimes T : K \otimes_{\mathbb{Q}} V \longrightarrow K \otimes_{\mathbb{Q}} V$$

present the eigenvectors as linear combinations of pure tensors.

Usual approach: tensoring basis for K, V will give a basis for $K \otimes_{\mathbb{Q}} V$.

A K-basis for V is $\{1, \sqrt{3}\}$, a K-basis for K
$\overset{\shortparallel}{\mathbb{Q}(\sqrt{2}, \sqrt{3})}$

is $\{1\}$. So $\{1\otimes 1, 1\otimes\sqrt{3}\}$ is a K-basis for $K\otimes_{\mathbb{Q}} V$. Now let's see how $id\otimes T$ acts on it (just to find eigenvectors).

$$id\otimes T(1\otimes 1) = id(1)\otimes T(1) = 1\otimes(1+\sqrt{2}) =$$
$$= (1+\sqrt{2}).(1\otimes 1).$$

$$id\otimes T(1\otimes\sqrt{3}) = 1\otimes(\sqrt{3}+\sqrt{6}) = (1+\sqrt{2})\cdot(1\otimes\sqrt{3}).$$

Rmk: $1\otimes\sqrt{2} = \sqrt{2}\cdot(1\otimes 1) = \sqrt{2}\otimes 1$.

V is K-v.s. using action of K on V.

K is K-v.s. using action of K on K.

$\underbrace{1\otimes\sqrt{2}}_{\sqrt{2}\cdot 1} \in K\otimes_{\mathbb{Q}} V$

scalar in K.

rewrite $1\otimes\sqrt{2}$ in $\{1\otimes 1, 1\otimes\sqrt{3}\}$.

What we are NOT doing is:

$$1\otimes\sqrt{2} = 1 \otimes \sqrt{2}\cdot 1 = 1\cdot\sqrt{2}\otimes 1 =$$
$$= \sqrt{2}\otimes 1.$$

It turns out that $\{1 \otimes 1, 1 \otimes \sqrt{3}\}$ is already an eigenbasis for $\mathrm{id} \otimes T$ (this is not true in general, we would need to do a change of basis in general).

Hence:

$$\mathrm{id} \otimes T = \begin{bmatrix} 1+\sqrt{2} & 0 \\ 0 & 1+\sqrt{2} \end{bmatrix}.$$

⑦ - $f, g \in \mathbb{Q}[x]$ non-constant, $H \subseteq \mathbb{C}$ splitting field of f.
$K \subseteq \mathbb{C}$ splitting field of g.
$L \subseteq \mathbb{C}$ splitting field of $f \cdot g$.

(a) Find injective group hom:

$$\phi : \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow \mathrm{Gal}(H/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q}).$$
$$\sigma \longmapsto (\sigma|_H, \sigma|_K).$$

To check:

$\sigma|_H$ lies inside H because fg have f as a factor.

$\sigma|_K$ lies inside K because fg have g as a factor.

(b) For $(\sigma, \tau) \in \mathrm{Gal}(H/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q})$, find a necessary and sufficient condition for (σ, τ) to be in $\mathrm{im}(\phi)$.

Isomorphism extension theorem.

<u>Given:</u> f and g cannot share roots.

(8) - (b) Prove that if there are elements $m_1, \ldots, m_k \in M$ and R-mod homs $f_i : M \longrightarrow R$, $1 \leq i \leq k$ with

$$m = \sum_{i=1}^{k} f_i(m)\, m_i \quad \text{for all } m \in M, \text{ then}$$

M is projective.

Let:

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "h"] & B \arrow[r, "g"] & M \arrow[r] \arrow[l, dashed, bend left, "\phi"] & 0 \end{tikzcd}$$

be an exact sequence. It is enough to show it splits, to see M is projective.

Since g surjective, for $m_i \in M$ we have $b_i \in B$

Note: ϕ may depend on the choice of b_i. But we do not care.

with $g(b_i) = m_i$. Define: $\phi : M \to B$.

$$m \mapsto \sum_{i=1}^{k} f_i(m) b_i$$

Suppose $m = m'$, then $f_i(m) = f_i(m')$.

Then $\phi(m) = \sum_{i=1}^{k} f_i(m) b_i = \sum_{i=1}^{k} f_i(m') b_i = \phi(m')$.

Now ϕ is an R-mod homomorphism (do it in the exam), and $g \circ \phi = id_M$ since:

$$(g \circ \phi)(m) = g\left(\sum_{i=1}^{k} f_i(m) b_i\right) = \sum_{i=1}^{k} \underbrace{f_i(m)}_{\in R} g(b_i) =$$

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

August 2014:

① - $M = \begin{bmatrix} 0 & 0 & -y \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$, y indeterminate.

(a) Show $\mathrm{char}(M) =: f_M(x)$ is irreducible in $\mathbb{Q}(y)[x]$.

$$\mathrm{char}(M) = \det(\mathbb{1} - x \cdot M) = \cdots = -x^3 - y.$$

Attempt 1: roots...

Attempt 2: Eisenstein's criterion.

__Thm:__ Let D be UFD with field of fractions F. Let $f(x) = \sum_{i=0}^{n} a_i x^i \in D[x]$ with f non-constant. Then if p is an irreducible element of D such that $p \nmid a_n$, $p \mid a_i$ for $i \leq n-1$, and $p^2 \nmid a_0$, then f is irreducible over $F[x]$.

Note: $D := \mathbb{Z}[y]$, F is $\mathbb{Q}(y)$, and $p = y$ is irreducible in D.

Now: $y \nmid x^3$, $y \mid 0$, $y \mid -y$, and $y^2 \nmid -y$. So by Eisenstein's we have $-x^3 - y$ is irreducible.

(5) Show M is diagonalizable over $\overline{\mathbb{Q}(y)}$.

M in some basis has to look diagonal.

<u>Recall:</u> $N = \begin{bmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{bmatrix}$ a diagonal matrix has characteristic polynomial

$\det(\mathbb{1} - \lambda \cdot N)$ where all entries are roots.

The minimal polynomial will also annihilate N, and the roots will be roots of $\mathrm{char}(N)$.

<u>Prop:</u> A matrix is diagonalizable over k iff its minimal polynomial splits in k and has <u>no</u> multiple roots.

Chapter: "Representation of one Endomorphism", Exercise 13, Algebra by Lang.

Jordan blocks: $\begin{bmatrix} \square & & & \\ & \square & & \\ & & \ddots & \\ & & & \square \end{bmatrix}$ where the blocks have diagonal entries, 1 either above or below the diagonal, and 0 elsewhere.

The kernels of the matrices depend on the size of the blocks. $\begin{bmatrix} \lambda & 0 \\ 1 & \lambda \end{bmatrix}$ gives element in the kernel.

By Cayley-Hamilton Theorem, the minimal polynomial $q_M(x)$ Hungerford VII.5.2(ii) divides the characteristic polynomial, since $\overline{\mathbb{Q}(\gamma)}$ is algebraically closed, both $q_M(x)$ and $f_M(x)$ split over $\overline{\mathbb{Q}(\gamma)}$. It remains to see that $q_M(x)$ has no multiple roots. A root of a polynomial is multiple iff it is a root and it is also a root of the formal derivative of the polynomial. Hungerford III.6.10(i).

$$\underbrace{f_M(x) = -x^3 - 7}_{\text{does not have } 0 \text{ as a root.}} \; ; \; \underbrace{f_M'(x) = -3x^2}_{\text{only has } 0 \text{ as root}}$$

So $f_M(x)$, f_M' have all roots different, so $f_M(x)$ has no multiple roots.

(c) Show that M is not diagonalizable over $\overline{\mathbb{F}_3(7)}$.

From (b), notice $f_M'(x) = 0$. Then $f_M(x)$ has multiple roots (it splits over $\overline{\mathbb{F}_3(7)}$, so it has roots, and they will also be roots of $f_M'(x)$).

$x^3+7 \in \overline{\mathbb{F}_3(7)}$, so it has to have a root,
so $7^{1/3} \in \overline{\mathbb{F}_3(7)}$.

So M is not diagonalizable.