Problem 1.  (1) Let $k$ be a field. For $r \geq 0$, we denote by $k_r[X]$ the vector space of all polynomials in $k[X]$ with degree $\leq r$. Let $P, Q \in k[X]$ polynomials with respective degrees $p$ et $q$. Consider the map

$$R : k_{q-1}[X] \times k_{p-1}[X] \to k_{p+q-1}[X] \quad (A, B) \mapsto AP + BQ.$$  

We call resultant of $P$ et $Q$ and we denote by $Res(P, Q)$ the determinant of this linear map. Give a condition on $P$ and $Q$ which is equivalent to $Res(P, Q) = 0$. Recall that the determinant of this map is nonzero if and only if the map is injective, if and only if it is surjective. The surjectivity condition should remind you of Bezout theorem.

(2) Application : Show that the set of algebraic numbers $\Omega$ is a field. Hints.

— The determinant of a matrix is a polynomial expression in the coefficients of the matrix.

— If $\alpha$ is a root for $P \in \mathbb{Q}[X] \setminus \{0\}$ and $\beta$ is a root for $Q \in \mathbb{Q}[X] \setminus \{0\}$, let $\gamma := \alpha + \beta$ and $Q_\gamma := Q(\gamma - X)$. What can you say about the resultant of $P$ and $Q_\gamma$ (which are both polynomials in $\mathbb{C}[X]$) ?

— Once you find a polynomial expression in $\gamma$ which is zero, you still have to prove that this gives you a nonzero polynomial which has root $\gamma$... For this, you are probably going to use the fact that a nonzero polynomial has finitely many roots.

Given a ring $R$ and a $R$-module $M$, we say that $M$ is simple if the only submodules of $M$ are $M$ and $\{0\}$.

Problem 2. Consider the symmetric group $S_3$ and let $k$ be an arbitrary field of characteristic different from 2. Let $R$ be the group ring $k[S_3]$.

(1) Check for yourself that an $R$-module is also a $k$-vector space. Show that there exactly are two nonisomorphic $R$-modules which are 1-dimensional as $k$-vector spaces. One of them will be called the trivial character and will be denoted by $k_{triv}$, and the other one the sign character which will be denoted by $k_{sign}$ (it has something to do with the signature of $S_3$...).

We discussed this in class. We said that $k_{triv}$ is the one dimensional vector space $k$ on which $g \in S_3$ acts trivially namely $(g, \lambda) \mapsto \lambda$ and $k_{sign}$ is the one dimensional vector space $k$ on which $g \in S_3$ acts by the signature character $\epsilon$ namely $(g, \lambda) \mapsto \lambda \epsilon(g)$ and where $\epsilon : S_3 \to k^\times$ is the unique homomorphism of groups sending a transposition to $-1 \in k^\times$ (it is called the signature character).

(2) Consider the $k$-linear morphism of rings $k[S_3] \to M_3(k)$ sending $\sigma$ onto the corresponding permutation matrix. This endows the vector space $V_3 = ke_1 \oplus ke_2 \oplus ke_3$ with a structure of $R$-module such that $\sigma \in S_3$ acts on $e_i$ by $(\sigma, e_i) \mapsto e_{\sigma(i)}$.

(a) Does $V_3$ contain a sub-$R$-module that is isomorphic to $k_{triv}$ or $k_{sign}$ ?

We discussed this in class. We said that the only one dimensional submodule contained in $V_3$ is $k(e_1 + e_2 + e_3)$ and that it is isomorphic to $k_{triv}$. A little detail again : let $v = x_1e_1 + x_2e_2 + x_3e_3$ be a vector in $V_3$ and suppose that $kv$ is isomorphic to $k_{triv}$. It means that $g \in S_3$ acts on $v$ by $(g, v) \mapsto v$. For example, when $g = (1, 2)$ it gives

$$x_1e_1 + x_2e_2 + x_3e_3 = v = (1, 2). v = x_1e_2 + x_2e_1 + x_3e_3$$

so $x_1 = x_2$... Likewise, with $(2, 3)$ you prove that $x_2 = x_3$...

I think in class we did the calculation to prove that $V_3$ cannot contain a vector $v$ on which $S_3$ acts by the sign character.

(b) Show that $\{e_1 - e_2, e_2 - e_3\}$ spans a sub-vector-space of $V_3$ which is a sub-$R$-module. Let $V_2$ denotes the sub-vector-space of $V_3$ spanned by $\{e_1 - e_2, e_2 - e_3\}$. We just need to prove (since $S_3$ is generated by the transpositions), that the transposition $(i, j)$ stabilizes $V_2$. For example, $(1, 2), (e_1 - e_2) = e_2 - e_1 \in V_2$ and $(1, 2), (e_2 - e_3) = e_1 - e_3 = (e_1 - e_2) + (e_2 - e_3) \in V_2$

(check the same kind of thing for the other transpositions $(1, 3)$ and $(2, 3)$.)
(i) If \( k \) has characteristic different from 3, show that \( V_3 \) is the direct sum of two simple modules. As a vector space, we claim that \( V_3 \) is the direct sum of \( V_1 := k(e_1 + e_2 + e_3) \) and \( V_2 \) defined above. You can see this by proving that \( \{ e_1 + e_2 + e_3, e_1 - e_2, e_2 - e_3 \} \) is a basis for \( V_3 \) (compute the determinant of this family of vectors in the canonical basis as we did in class). So we have a decomposition

\[
V_3 = V_1 \oplus V_2
\]
as vector spaces. Since furthermore \( V_1 \) and \( V_2 \) are sub-\( R \)-modules, it is a direct sum of sub-\( R \)-modules.

(ii) If \( k \) has characteristic 3, give an inclusion of \( R \)-modules

\[
0 \subset V_1 \subset V_2 \subset V_3
\]
where \( V_i \) has dimension \( i \). Describe the quotient representations \( V_{i+1}/V_i \). If \( V_3 \) has characteristic 3, we see that in fact \( V_1 \) is contained in \( V_3 \). This is because

\[
e_1 + e_2 + e_3 = e_1 - e_2 + 2e_2 + e_3 = e_1 - e_2 - e_2 + e_3 = (e_1 - e_2) - (e_2 - e_3)
\]

Does the short exact sequence

\[
0 \rightarrow V_1 \rightarrow V_3 \rightarrow V_3/V_1 \rightarrow 0
\]
split?

We study a bit \( V_3/V_1 \). It contains the element \( y := e_1 - e_2 \mod V_1 \). We have

\[
(1,2).y = (1,2).((e_1 - e_2) \mod V_1) = e_2 - e_1 \mod V_1 = -y
\]

and

\[
(2,3).y = (2,3).((e_1 - e_2) \mod V_1) = e_1 - e_3 \mod V_1 = e_1 + e_2 + e_3 + (e_3 - e_2) \mod V_1 = e_3 - e_2 \mod V_1 = -y.
\]

Lastly \((1,2)(2,3)(1,2) = (1,3)\) so \((1,3).y = -y\). This proves that \( V_3/V_1 \) contains a sub-\( R \)-module which is isomorphic to \( k_{sign} \). If the sequence split, we would have

\[
V_3 \cong V_1 \oplus V_3/V_1
\]
as \( R \)-modules, so \( V_3 \) would contain a sub-\( R \)-module which is isomorphic to \( k_{sign} \). We know it is not true by a previous question. So the sequence does not split.

**Problem 3.** Let \( R \) be a ring with identity element and \( M \) a left \( R \)-module. Describe a structure of left \( R \)-module on \( \text{Hom}_R(R, M) \). Show that

\[
M \cong \text{Hom}_R(R, M)
\]
as left \( R \)-modules.

**Structure of \( R \)-module on \( \text{Hom}_R(R, M) \):**

\[
R \times \text{Hom}_R(R, M) \rightarrow \text{Hom}_R(R, M), \quad (r, f) \mapsto [R \rightarrow M, s \mapsto f(sr)].
\]

Then check that the map

\[
\text{Hom}_R(R, M) \rightarrow R, \quad f \mapsto f(1_R)
\]
is an isomorphism of \( R \)-modules.

**Problem 4.** Let \( m, n \in \mathbb{Z} \), both \( \geq 1 \) and \( d := \gcd(m, n) \). Show that we have an isomorphism of \( \mathbb{Z} \)-modules

\[
\text{Hom}_\mathbb{Z}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}
\]
First denote by \( H \) the subgroup of \( \mathbb{Z}/n\mathbb{Z} \)

\[
H := \{ x \mod n, \, mx = 0 \mod n \}
\]
of all elements of order dividing \( m \). Let
\[
\text{Hom}_\mathbb{Z}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \longrightarrow \mathbb{Z}/n\mathbb{Z} \\
f \longmapsto f(1 \mod m)
\]
Check that this is a homomorphism of abelian groups. It is easy to see that it is injective. Furthermore, \( mf(1 \mod m) = f(0 \mod m) = 0 \) so in fact it has image in \( H \). Let \( h \in H \). Then define the morphism of groups \( \phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \) by \( \phi(1) = h \). We have \( \phi(m) = mh = 0 \) so it factors through a morphism of groups \( \tilde{\phi} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, 1 \mod m \mapsto h \). This proves that the map above is surjective. So it is an isomorphism
\[
\text{Hom}_\mathbb{Z}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong H.
\]
It remains to prove that \( H \cong \mathbb{Z}/d\mathbb{Z} \) which was probably be done in math 322 :) more precisely, it is easy to prove that \( H = (n/d)\mathbb{Z}/n\mathbb{Z} \) namely that \( H \) is the ideal of \( \mathbb{Z}/n\mathbb{Z} \) generated by \( n/d \). Then \( \mathbb{Z} \to H, z \mapsto nz/d \mod n \) is a surjective homomorphism of groups with kernel \( d\mathbb{Z} \).