Solutions to Final exam in MM7033, 2023-12-14, 14:00–19:00

1. (a) $x^2+x+1 \in \mathbb{F}_2[x]$ is irreducible because if it was reducible it would have a root but neither $x=0$ nor $x=1$ are roots. In the extension $E = \mathbb{F}_2[x]/(x^2+x+1)$ we have the root $\alpha = \overline{x}$ and $x^2+x+1 = (x-\alpha)\big(x-(\alpha+1)\big)$ splits completely. Thus E is the splitting field and it has degree 2.

   (b) We let $\alpha = \sqrt[4]{2}$. Then the roots of x^4-2 are $\pm\alpha$ and $\pm i\alpha$. The splitting field is thus $E = \mathbb{Q}(\alpha, i)$. Since $x^4-2 \in \mathbb{Q}[x]$ is irreducible, by Eisenstein's criterion for $p=2$, it follows that $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$. Since $\mathbb{Q}(\alpha)$ is real, it does not contain i so $[E:\mathbb{Q}(\alpha)] = 2$. The degree of the splitting field is $2 \cdot 4 = 8$.

2. Two algebraic subsets are isomorphic if and only if their coordinate rings are isomorphic as $\mathbb{C}$-algebras. The first coordinate ring is

$$\mathbb{C}[X_1] = \mathbb{C}[x,y]/(y-x^2) \simeq \mathbb{C}[x].$$

   The second coordinate ring is

$$\mathbb{C}[X_2] = \mathbb{C}[x,y]/(xy-1) \simeq \mathbb{C}\Big[x, \frac{1}{x}\Big].$$

   These are both integral domains but the units of the first coordinate ring is $\mathbb{C}^\times$ whereas the second coordinate ring also has the units x^n, for $n \in \mathbb{Z}$. Thus, they cannot be isomorphic.

   The third coordinate ring is

$$\mathbb{C}[X_3] = \mathbb{C}[x,y]/(y^2+x^2)$$

   which is not a domain since $(y+ix)(y-ix) = 0$, hence not isomorphic to the previous two.

3. (a) Since $(x+1)$ is a principal ideal, it is a cyclic module and $(x+1) \cong R/I$ where $I = \operatorname{Ann}_R(x+1)$. For $f(x) \in \mathbb{Z}[x]$, we have that $f(x)(x+1) \in (x^2-1)$ if and only if $f(x) \in (x-1)$ (here we use that $\mathbb{Z}[x]$ is a domain). This means that $\operatorname{Ann}_R(x+1) = (x-1)$ so $(x+1) \cong R/(x-1)$.

   (b) First note that $R/(x-1) = \mathbb{Z}[x]/(x-1) \cong \mathbb{Z}$ as an $\mathbb{Z}$-module. Since $R/(x-1)$ is cyclic, a potential splitting $s\colon R/(x-1) \to R$ is determined by the image $s(1)$ of 1. Since $0 = s(x-1) = (x-1)s(1)$, we have that $s(1) \in \operatorname{Ann}_R(x-1) = (x+1)$, that is $s(1) = r(x+1)$ for some $r \in R$. But $\pi(x+1) = 2$ where $\pi\colon R \to R/(x-1)$ is the quotient homomorphism. Thus, $1 = (\pi \circ s)(1)$ is divisible by 2 which is impossible since $R/(x-1) \cong \mathbb{Z}$.

   (c) As abelian groups, we have that R is free of rank 2 with basis $1, x$. The other two modules are free of rank 1 with bases $x-1$ and 1 respectively. We thus have the sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\begin{bmatrix} -1 \\ 1 \end{bmatrix}} \mathbb{Z}^2 \xrightarrow{\begin{bmatrix} 1 & 1 \end{bmatrix}} \mathbb{Z} \longrightarrow 0.$$

   A splitting is given by any map $\mathbb{Z} \mapsto \mathbb{Z}^2$, $1 \mapsto (a,b)$ where $a+b=1$, e.g., $n \mapsto (n,0)$.

   We could also immediately conclude that the sequence is split since the $R/(x-1) \cong \mathbb{Z}$ is free, hence projective, as a $\mathbb{Z}$-module.

4. (a) We have a short exact sequence $0 \to I \to R \to R/I \to 0$. Tensoring this with R/J over R gives a right-exact sequence

$$I \otimes_R R/J \to R/J \to R/I \otimes_R R/J \to 0.$$

The kernel of the second map $R/J \to R/I \otimes_R R/J$ is the image of the first map which is $I(R/J)$. By composition, we get a surjective map $R \to R/J \to R/I \otimes_R R/J$ and the kernel is exactly $\pi^{-1}(IR/J) = I + J$ where $\pi\colon R \to R/J$. The result follows.

Alternative solution: There is a homomorphism of R-modules $\bar{q}\colon R \to R/I \otimes_R R/J$ defined as the following composition

$$R \xrightarrow{\cong} R \otimes_R R \to R/I \otimes_R R/J.$$

Here the first homomorphism can be defined by the formula $r \mapsto r \otimes 1$. The second homomorphism is the tensor product of the quotient homomorphisms $R \to R/I$ and $R \to R/J$. Notice that $r \otimes 1 = 1 \otimes r$ in $R \otimes_R R$, because of the R-bilinearity of $- \otimes_R -$.

Suppose $x \in I$. Then $x + I = 0 + I$ and $\bar{q}(x) = (x + I) \otimes (1 + J) = (0 + I) \otimes (1 + J) = 0$. Suppose $x \in J$. Then, again

$$\bar{q}(x) = (x + I) \otimes (1 + J) = (1 + I) \otimes (x + J) = (1 + I) \otimes (0 + J) = 0.$$

We have shown that $I \subset \ker(\bar{q})$ and $J \subset \ker(\bar{q})$. It follows that $I + J \subset \ker(\bar{q})$, and therefore $\bar{q}$ factors through a homomorphism $q\colon R/(I + J) \to R/I \otimes_R R/J$. Explicitly, $q(r + I + J) = (r + I) \otimes (1 + J)$.

To prove that q is an isomorphism, we construct an inverse homomorphism $\mu\colon R/I \otimes_R R/J \to R/(I + J)$. To construct such a homomorphism is equivalent to constructing an R-bilinear map $\bar{\mu}\colon R/I \times R/J \to R/(I+J)$. We define $\bar{\mu}$ by the formula $\bar{\mu}(x+I, y+J) = xy + I + J$. To check that $\bar{\mu}$ is well-defined we have to check that if $i \in I$ and $j \in J$ then $xy+I+J = (x+i)(y+j)+I+J$. But $(x+i)(y+j) = xy+xj+iy+ij \in xy+I+J$. Once we know that $\bar{\mu}$ is well-defined it is clear that it is R-bilinear, because multiplication in R is R-bilinear. So $\bar{\mu}$ induces a well-defined R-module homomorphism $\mu\colon R/I \otimes_R R/J \to R/(I + J)$, determined by the formula $\mu\big((x + I) \otimes (y + J)\big) = (xy + I + J)$.

It remains to check that q and μ are inverses of each other, and thus are isomorphisms. We have

$$\mu\big(q(r + I + J)\big) = \mu\big((r + I) \otimes (1 + J)\big) = r + I + J$$

and

$$q\big(\mu((x + I) \otimes (y + J))\big) = q(xy + I + J) = (xy + I) \otimes (1 + J) = (x + I) \otimes (y + J)$$

where the last equality follows from the R-bilinearity of $- \otimes_R -$.

(b) If M is a finitely generated non-zero R-module, then by the fundamental theorem of modules over a PID, we have that M is a direct sum of cyclic R-modules:

$$M = R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_n)$$

where $(a_i) \neq R$ and $n \geq 1$. Since tensor products distribute over direct sums, we obtain

$$M \otimes_R M = \bigoplus_{1\leq i,j\leq n} R/(a_i) \otimes_R R/(a_j) = \bigoplus_{1\leq i,j\leq n} R/(a_i, a_j)$$

where we in the last step have used (a). For $i = j$, we have that $R/(a_i, a_j) = R/(a_i) \neq 0$ so $M \otimes_R M \neq 0$.

(c) Let $R = \mathbb{Z}$ and $N = \mathbb{Q}/\mathbb{Z}$. Then $N \otimes_R N = 0$. Indeed, if $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}/\mathbb{Z}$, then $\frac{a}{b} \otimes \frac{c}{d} = \frac{a}{b} \otimes \frac{bc}{bd} = a \otimes \frac{c}{bd} = 0$. This shows that all pure tensors are zero in $N \otimes_R N$, hence every tensor is zero in $N \otimes_R N$.

5. (a) Let $y = x^2 + x$. Note that $x \notin \mathbb{F}(y)$. Indeed, every element of $\mathbb{F}(y)$ has a presentation as a ratio $\frac{p(x^2+x)}{q(x^2+x)}$, where p and q are polynomials with coefficients in $\mathbb{F}$ and $q \neq 0$. Considered as polynomials in x, the degrees of $p(x^2 + x)$ and $q(x^2 + x)$ differ by an even number. It follows that their ratio cannot be equal to x.

   Next, note that $E = \mathbb{F}(x)$ is the smallest subfield of E containing $\mathbb{F}$ and x. We have shown that $[E : \mathbb{F}(y)] > 1$. Since x satisfies the degree 2 equation $x^2 + x - y = 0$ with coefficients in the subfield $\mathbb{F}(y)$, it follows that $[E : \mathbb{F}(y)] = 2$ and the minimal polynomial of x is $m(t) := m_{x,\mathbb{F}(y)}(t) = t^2 + t - y$.

   (b) Recall that $p(t)$ is separable if and only if $p(t)$ and $p'(t)$ are relatively prime. We see that $m'(t) = 2t + 1 = 1$ so $m(t)$ is separable. An arbitrary element of E is of the form $ax + b$ where $a, b \in \mathbb{F}(y)$. If $a = 0$, then the minimal polynomial is $t - b$, hence separable. If $a \neq 0$, then the minimal polynomial has degree 2 and we calculate it as follows. We have that $(ax + b)^2 + a^2(x - y) - b^2 = 0$ so $ax + b$ has minimal polynomial $m(t) := m_{ax+b,\mathbb{F}(y)}(t) = t^2 + a(t - b - ay) - b^2 = t^2 + at + (ab + a^2y + b^2)$. The derivative is $m'(t) = a$ which is a unit, hence coprime to $m(t)$, so $m(t)$ is separable. We have thus shown that E is separable over $\mathbb{F}(y)$.

   (c) The extension E of $\mathbb{F}(y)$ is however inseparable: the minimal polynomial of x is $t^2 - y$ which has the repeated root x in the splitting field which is E.

6. Let $R = \mathbb{F}[x_1, x_2, \ldots, x_n]$. Suppose that $S = \{a_1, \ldots, a_d\}$ is finite. Then $\mathcal{I}(S) = M_1 \cap M_2 \cap \cdots \cap M_d$ where $M_i = (x_1 - a_{i1}, x_2 - a_{i2}, \ldots, x_d - a_{id})$. Since the M_i's are distinct maximal ideals, they are pairwise coprime: $M_i + M_j = (1)$ for $i \neq j$. Thus, by the Chinese remainder theorem, we have that

$$R/\mathcal{I}(S) = R/M_1 \times R/M_2 \times \cdots \times R/M_d \simeq \mathbb{F}^d$$

which is an $\mathbb{F}$-vector space of dimension d.

Conversely, suppose that $R/\mathcal{I}(S)$ is a vector space of dimension d but that S is infinite. Then we can pick a subset $S' \subset S$ of $d + 1$ distinct points. This gives us $\mathcal{I}(S) \subseteq \mathcal{I}(S')$ and a surjection $R/\mathcal{I}(S) \twoheadrightarrow R/\mathcal{I}(S')$. But we previously showed that $R/\mathcal{I}(S')$ has dimension $d + 1$ which contradicts that $R/\mathcal{I}(S)$ has dimension d.