Math 30820 Honors Algebra 4
Homework 4

Andrei Jorza

Due Wednesday, 2/15/2017

Do 6 of the following questions. Some questions may be obligatory. Artin a.b.c means chapter a, section b, exercise c. You may use any problem to solve any other problem.

Throughout this problem set R is an **integral domain**, unless otherwise specified.

1. (You must do this problem) Suppose R is a commutative ring such that every ideal of R is finitely generated. Suppose M is an R-submodule of a finite rank free module R^n. Show that M is also finitely generated. [Hint: Consider the image and kernel of M under the homomorphism $R^n \to R^{n-1}$ which is given by $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{n-1})$ and then argue by induction.]

   Proof. By induction on n. The base case is $n = 1$. Every submodule of R is an ideal and this is finitely generated by assumption. Suppose every submodule of R^k is finitely generated for $k < n$. Let $M \subset R^n$ and let π be the homomorphism from the hint. Also denote by π the restriction $\pi : M \to R^{n-1}$. From homework 3, to show that M is finitely generated it suffices to show that $\ker \pi$ and $\operatorname{Im} \pi$ are finitely generated. Since $\operatorname{Im} \pi \subset R^{n-1}$ is a submodule it is finitely generated by the inductive hypothesis. What about $\ker \pi$? By definition it is $\ker \pi = \{m \in M \mid \pi(m) = 0\}$. But $M \subset R^n$ is a submodule and if we write $m = (r_1, \ldots, r_n) \in R^n$ as an n-tuple then $m \in \ker \pi$ if and only if $r_1 = \ldots = r_{n-1} = 0$ so $\ker \pi = \{(0, \ldots, 0, r) \mid r \in R\} \cap M$. But visibly $\ker \pi$ is then a submodule of R (the last coordinate) and by hypothesis $\ker \pi$ has to be finitely generated. □

2. Artin 14.7.7 on page 439.

   Proof. Consider the homomorphism of free R-modules $f : R^2 \to R^2$ given by left-multiplication by the matrix $A = \begin{pmatrix} 1+i & 2-i \\ 2 & 5i \end{pmatrix}$. Then V is defined as $R^2/\operatorname{Im} f = \operatorname{coker} f$. From the example done in class it suffices to transform A into its diagonal echelon form. Here are the matrices

   $$\begin{pmatrix} 1+i & 2-i \\ 2 & 5i \end{pmatrix} \mapsto \begin{pmatrix} 1+i & 4-3i \\ 2 & i \end{pmatrix} \mapsto \begin{pmatrix} 7+9i & 4-3i \\ 0 & i \end{pmatrix} \mapsto \begin{pmatrix} 7+9i & 0 \\ 0 & i \end{pmatrix}$$

   where the transformations are $c_2 \mapsto c_2 - 2ic_1$, $c_1 \mapsto c_1 + 2ic_2$, $r_1 \mapsto r_1 - i(4-3i)r_2$. Thus $V \cong R^2/\operatorname{Im} f = R \oplus R/(7+9i) \oplus (i) \cong \mathbb{Z}[i]/(7+9i)$. □

3. Artin 14.7.8 on page 439.

   Proof. (a): Suppose $\mathbb{F}_p$ has the structure of a $\mathbb{Z}[i]$-module. Suppose now that $i \cdot 1 = k$ with $k \in \mathbb{F}_p$. Then $i \cdot (i \cdot 1) = i \cdot k = k(i \cdot 1) = k^2$ but this is also equal to $i^2 \cdot 1 = -1 \cdot 1 = -1$. Therefore it's necessary that $k^2 = -1$ in $\mathbb{F}_p$. From last semester we know that such a k can exist if and only if $p \equiv 1 \pmod 4$ or $p = 2$. If $p = 2$ then define $z \cdot x = x$ for all $z \in \mathbb{Z}[i]$ and $x \in \mathbb{F}_p$ and this yields a module structure because $-1 = 1$ in $\mathbb{F}_2$. If $p \equiv 1 \pmod 4$ let k be such that $k^2 = -1$ in $\mathbb{F}_p$ and define $(m + ni) \cdot x = (m + nk)x \in \mathbb{F}_p$. This yields a $\mathbb{Z}[i]$-module structure on $\mathbb{F}_p$.

(b): From homework 3 it's enough to give an $\mathbb{F}_p$-linear homomorphism of vector spaces on $\mathbb{F}_p^2$ such that $\varphi \circ \varphi = -\operatorname{id}$. Multiplication on the left by $\begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$ works. $\square$

4. Artin 14.8.6 on page 440.

Proof. Caution: while every ideal of $\mathbb{C}[\varepsilon]$ is principal (indeed, by the correspondence theorem ideals of $\mathbb{C}[\varepsilon] = \mathbb{C}[X]/(X^2)$ are of the form $I/(X^2)$ where I is an ideal of $\mathbb{C}[X]$ containing (X^2)), the ring $\mathbb{C}[\varepsilon]$ is not a domain ($\varepsilon^2 = 0$) so it is not a PID and the theorem from class is not applicable.

Recall from a previous homework that if $f : R \to S$ is a ring homomorphism and M is an S-module then f^*M defined as an abelian group by $f^*M = M$ with R-multiplication via $r \cdot_R m = f(r) \cdot_S m$ is an R-module. Consider this for the projection homomorphism $\pi : \mathbb{C}[X] \to \mathbb{C}[\varepsilon] = \mathbb{C}[X]/(X^2)$. If M is a finitely generated $\mathbb{C}[\varepsilon]$-module then π^*M is a finitely generated $\mathbb{C}[X]$-module (check this, it's not hard, you can use the same generators). Since $\mathbb{C}[X]$ is a PID we have

$$\pi^*M \cong \mathbb{C}[X]^r \oplus \bigoplus \mathbb{C}[X]/(P_i(X))$$

for $P_1 \mid \ldots \mid P_n$.

The identity map $m \mapsto m$ on $\pi^*M \to M$ is R-linear and as M is an $\mathbb{C}[\varepsilon]$-module it follows that $X^2 \cdot m = \varepsilon^2 \cdot m = 0$. But multiplication by X^2 is not the 0 map on $\mathbb{C}[X]$ so the rank of M as a $\mathbb{C}[X]$-module is 0. Moreover, on $\mathbb{C}[X]/(P_i(X))$ we need multiplication by X^2 to be 0 which immediately implies that $X^2 \in (P_i(X))$. Therefore $P_i(X) \mid X^2$ so each P_i is either 1, X or X^2. Suppose among the P_i, a are 1, b are X and c are X^2. Then

$$\pi^*M = (\mathbb{C}[X]/(1))^a \oplus (\mathbb{C}[X]/(X))^b \oplus (\mathbb{C}[X]/(X^2))^c = \mathbb{C}^b \oplus \mathbb{C}[\varepsilon]^c$$

and this is also M as a $\mathbb{C}[\varepsilon]$-module. $\square$

5. Artin 15.2.3 on page 472.

Proof. Suppose the equation $\sum x_i^2 = -1$ had a solution in the field $\mathbb{Q}(\zeta\sqrt[3]{2})$. Consider the unique field isomorphism $f : \mathbb{Q}(\zeta\sqrt[3]{2}) \cong \mathbb{Q}(\sqrt[3]{2})$ that is the identity on $\mathbb{Q}$. Then $f(\sum x_i^2) = \sum x_i^2 = -1$ would have a solution in $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$. But $\sum x_i^2 = -1$ has no solution in $\mathbb{R}$. $\square$

6. Artin 15.3.2 on page 472.

Proof. By Eisenstein the polynomial is irreducible over $\mathbb{Q}$ and if $\alpha \in \mathbb{C}$ is a root then from class $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. If the polynomial were reducible over $\mathbb{Q}(\sqrt[3]{2})$ then the minimal polynomial of α over $\mathbb{Q}(\sqrt[3]{2})$ would have degree < 4 so $[\mathbb{Q}(\sqrt[3]{2}, \alpha) : \mathbb{Q}(\sqrt[3]{2})] < 4$. But then $[\mathbb{Q}(\sqrt[3]{2}, \alpha) : \mathbb{Q}] < 12$. However, we know that $3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ and $4 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ divide this degree and the smallest number divisible by 3 and 4 is 12. $\square$

7. Artin 15.3.9 on page 473.

Proof. As in the previous problem, $f(x)$ is irreducible over $\mathbb{Q}(\beta)$ if and only if $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f(x)$. But this is equivalent to $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}]$. This condition is symmetric with respect to α and β so it is also equivalent to $g(x)$ being irreducible over $\mathbb{Q}(\alpha)$. $\square$

8. Artin 15.4.1 on page 473.

Proof. Note that $\alpha\gamma = \alpha + \alpha^3 = 2\alpha + 1$ so we solve $\alpha = 1/(\gamma - 2)$. But α satisfies $\alpha^3 = \alpha + 1$ so we get the equation $(\gamma - 2)^{-3} = (\gamma - 2)^{-1} + 1$ which gives $1 = (\gamma - 2)^2 + (\gamma - 2)^3$. We get that γ is a root of the polynomial

$$f(X) = (X - 2)^3 + (X - 2)^2 - 1 = X^3 - 5X^2 + 8X - 5$$

We only need to check that $f(X)$ is irreducible over $\mathbb{Q}$. Otherwise $f(X)$ would have a rational root as $f(X)$ would have to have a linear factor. Alternatively, $[\mathbb{Q}(\gamma) : \mathbb{Q}] < 3$. But since $\gamma \in \mathbb{Q}(\alpha)$ we have $\mathbb{Q}(\gamma) \subset \mathbb{Q}(\alpha)$ so $[\mathbb{Q}(\gamma) : \mathbb{Q}] \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. It would have to be that $[\mathbb{Q}(\gamma) : \mathbb{Q}] =$ so $\gamma \in \mathbb{Q}$ as $2 \nmid 3$.

So it's enough to show that $f(X)$ does not have a rational root. But $f(X)$ is monic so its roots are integral over $\mathbb{Z}$. But from homework 2 we know that the only rationals which are integral over $\mathbb{Q}$ are the integers. So it's enough to check that $f(X)$ has no integral roots. Either you use a computer to check that $\gamma = \alpha^2 + 1$ is not integral (it has decimals) or you note that $f(X + 1) = X^3 - 2X^2 + X - 1$ would also have to have an integral root. But γ^{-1} is a root of $X^3 f(1/X)$ which is monic with integral coefficients. Therefore γ^{-1} is integral over $\mathbb{Z}$ and rational so $\gamma^{-1} \in \mathbb{Z}$. But then $\gamma = \pm 1$ and you can easily check that ± 1 is not a root of $f(X)$. $\square$