Math 210B Algebra: Homework 1

Jan 18th, 2019

Professor Sharifi

Anish Chedalavada

Exercise 1. *Let R be the ring of $\mathbb{Z}$-module endomorphisms of $M = \bigoplus_{i\in\mathbb{N}} \mathbb{Z}$. Show that $R \cong R^n$ as R-modules.*

Proof. We have that $\bigoplus_{i\in\mathbb{N}} \mathbb{Z} = (\bigoplus_{i\in\mathbb{N}} \mathbb{Z}) \oplus (\bigoplus_{i\in\mathbb{N}} \mathbb{Z})$ by dividing along even and odd indices. $R = \text{Hom}_{\mathbb{Z}}(M, M) \cong \text{Hom}_{\mathbb{Z}}(M, M \oplus M) \cong \text{Hom}_{\mathbb{Z}}(M, M) \oplus \text{Hom}_{\mathbb{Z}}(M, M)$. We have that R is an R-module over itself under left translation, which corresponds to composition in the endomorphism ring. As direct sums decompose over this operation as well, we have that $R \cong R^2$ as R-modules. Proceeding recursively for each summand yields the result. □

Exercise 2. *Show that the infinite direct product of infinite cyclic groups is not a free abelian group.*

Proof. Assume it is free. We have that the cardinality of $G = \prod_{i=1}^{\infty} \mathbb{Z}$ is uncountable and thus any basis must be uncountable. Furthermore, if we consider any countable subgroup H (s.t. $G = G_1 \oplus G_2$ with $H \subset G_2$, can restrict s.t. G_2 is countable as only countably many basis elements appear in it)* then we may quotient out s.t. $G = G_1 \oplus G_2/H$. Let H be the set of all integer sequences with only finitely many nonzero terms: clearly, this is a subgroup of G. We quotient G/H s.t. $G = G_1 \oplus G_2/H$. Let $x \in G_1$, then clearly x is an infinite integer sequence of the form $[a_1, a_2, ..]$. Let p be an arbitrary prime. We have that the set of all strictly increasing integer sequences is also uncountable using Cantor's diagonal argument. Therefore, set of all prime powered sequences $[p^{n_1}, p^{n_2}, ...]$ with $\{n_i\}_{i\in\mathbb{N}}$ strictly increasing is also uncountable, and there is some sequence of that form that lies in the uncountable free part of G/H. We have that the representative $[p^{n_1}, p^{n_2}, p^{n_3}, p^{n_4}, ...] \equiv [0, p^{n_2}, p^{n_3}, p^{n_4}, ...] \mod H \equiv [0, 0, p^{n_3}, p^{n_4}, ...] \mod H \equiv ...$ and so this class is divisible by p^{n_2} for arbitrarily large powers of p. However, this class was assumed to lie in the free part of G/H, a contradiction. Thus, G cannot be free. □

* This lemma was found online on mathematics stackexchange in order to bridge the gap in my original proof. The rest is original work.

Exercise 3. *Let $\alpha = \sqrt{\sqrt{3} + \sqrt{5}}$.*
a. Find $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.
b. What are the conjugates of α over $\mathbb{Q}$?

Proof. We have that $\alpha^2 = \sqrt{3} + \sqrt{5}$. This yields the following chain of simplifications:

$$\begin{aligned}
&(\sqrt{3} + \sqrt{5})^2 = 3 + \sqrt{3} \cdot \sqrt{5} + 5 \\
&\to \text{Ans} - 8 = \sqrt{3} \cdot \sqrt{5} \implies \text{Ans} \cdot \frac{1}{3} = \frac{\sqrt{5}}{\sqrt{3}} \in \mathbb{Q}(\alpha) \\
&\to \text{Ans} \cdot \sqrt{3} + \sqrt{5} = \sqrt{5} + \frac{5}{\sqrt{3}} \implies \text{Ans} - \sqrt{3} - \sqrt{5} = \frac{2}{\sqrt{3}} \in \mathbb{Q}(\alpha) \\
&\implies \sqrt{3} \text{ and thus } \sqrt{5} \in \mathbb{Q}(\alpha)
\end{aligned}$$

Thus, $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subset \mathbb{Q}(\alpha)$, and we know $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 2$. The minimal polynomial of α over $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ is $t^2 - \sqrt{3} - \sqrt{5}$, and it must satisfy this identity over $\mathbb{Q}(\sqrt{3}, \sqrt{5})$, containing them as subfields. We thus can extend this embedding of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ to one of the root of that minimal polynomial, yielding that the degree is 8 over $\mathbb{Q}$. For each conjugate of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ we have different distinct roots that α is sent to as algebraic extension over the image of the minimal polynomials under each conjugates of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. We thus have 8 conjugates, given by:

$$\alpha = \pm\sqrt{\pm\sqrt{3} + \pm\sqrt{5}}$$

□

Exercise 4. *Show that $K = \mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, ...)$ is an algebraic extension of $\mathbb{Q}$ of infinite degree.*

Proof. Any element in K is a finite sum of some $a_0 + a_{i_1}\sqrt{p_{i_1}} + ... + a_{i_n}\sqrt{p_{i_n}} + e$ where e is some combination of products of the same, and thus lies in the subfield $\mathbb{Q}(\sqrt{p_{i_1}}, ..., \sqrt{p_{i_n}})$, which is clearly a finite degree extension, and thus is algebraic over $\mathbb{Q}$; thus, K is algebraic over $\mathbb{Q}$. Finally, assume that $\mathscr{B} = \{\sqrt{p_1}, ..., \sqrt{p_n}, (\sqrt{p_i} \cdot \sqrt{p_j})_{i\neq j}, ..., (\sqrt{p_1} ... \sqrt{p_n}\}$

are linearly independent over $\mathbb{Q}$. Suppose $\sqrt{p_{n+1}} = a_0 + \sum_{i=1}^n a_i\sqrt{p_i} + \sum_{i\neq j} a_{ij}\sqrt{p_i}\sqrt{p_j}$ for not all $a_{i\neq 0} = 0$. Then we have $p_{n+1} = \big(a_0 + \sum_{i=1}^n a_i\sqrt{p_i} + ... + a_{1...n}(\sqrt{p_1}...\sqrt{p_n})\big)^2$ which is another linear combination in $\mathscr{B}$ above where not all coefficients are zero, and furthermore that at least one nonconstant coefficient in the new linear combination is nonzero. However, subtracting p_{n+1} from both sides yields another linear combination in $\mathscr{B}$ that is equal to zero, and thus all coefficients must be equal to zero by linear independence. This yields a contradiction, and thus $\sqrt{p_{n+1}} \notin \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_n})$. By induction on n, this yields algebraic extensions of $\mathbb{Q}$ of arbitrarily large degree in K, and thus K is of infinite degree. □

Exercise 5. *a. Find the degree of* $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$
b. How many embeddings of $\mathbb{Q}(\sqrt[4]{2})$ *into* $\mathbb{R}$ *are there?*
c. How many extensions of each of the embeddings in part b to an embedding of $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$*are there? To what value does each send* $\sqrt[6]{6}$*.*

Proof. a. The degree of $\mathbb{Q}(\sqrt[4]{2})$ over $\mathbb{Q}$ is 4. We have that $\sqrt[6]{2}$ is a solution to the polynomial $t^3 - \sqrt{2}$ in $\mathbb{Q}(\sqrt[4]{2})[t]$, which is irreducible as it does not have a root in $\mathbb{Q}(\sqrt[4]{2})$. Thus, $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$ is of degree $4 \cdot 3 = 12$ over $\mathbb{Q}$.
b. Any embedding of $\mathbb{Q}(\sqrt[4]{2})$ into $\mathbb{R}$ is the identity on $\mathbb{Q}$ as 1 goes to 1, and thus is completely determined by the embedding of $\sqrt[4]{2}$. By linearity, any image of $\sqrt[4]{2}$ must be a root of the polynomial $t^4 - 2$, for which only two roots lie in $\mathbb{R}$, $\pm\sqrt[4]{2}$. Thus, there are only two embeddings of $\mathbb{Q}(\sqrt[4]{2})$ into $\mathbb{R}$.
c. Any embedding of $\mathbb{Q}(\sqrt[4]{2})$ into $\mathbb{R}$ send $(\sqrt[4]{2})^2$ to $\sqrt{2}$, implying that any extension of this embedding to $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$ must send $\sqrt[6]{2}$ to a root of the minimal polynomial $t^3 - \sqrt{2}$ as this is the image of the minimal polynomial of $\sqrt[6]{2}$ under the embedding of $\mathbb{Q}(\sqrt[4]{2})$ into $\mathbb{R}$. However, the only root of this polynomial that lies in $\mathbb{R}$ is the positive $\sqrt[6]{2}$, and thus we have one unique extension for each embedding of $\mathbb{Q}(\sqrt[4]{2})$ that sends $\sqrt[6]{2}$ to the positive $\sqrt[6]{2} \in \mathbb{R}$. □

Exercise 6. *Let* ζ_p *be a primitive pth root of unity for* $p = 2^{2^n} + 1$ *a Fermat prime. Find the degree* $[\mathbb{F}_2(\zeta_p) : \mathbb{F}_2]$.

Proof. We have that the degree of this extension is equal to the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$. We may start by considering $2^{2^n} = p - 1$. Clearly, the order of 2 is greater than 2^{2^n}. We have that $2^{m+2^n} \equiv -2^m \mod p$ simply by this fact. Thus, it is immediate that $2^{2^n+2^n} = 2^{2^{n+1}} \equiv -2^{2^n} \mod p \equiv 1 \mod p$, and for all values $2^n < m < 2^{n+1}$ we have that $2^{m+2^n} \equiv -2^m modp$, the least positive representative of which is always greater than 1 in the ordering of $\mathbb{Z}$ unless $m = 2^n$. Thus, the order of 2 is 2^{n+1} and the degree $[\mathbb{F}_2(\zeta_p) : \mathbb{F}_2] = 2^{n+1}$. □

Exercise 7. *Determine the number of irreducible polynomials of degree n in* $\mathbb{F}_p[x]$ *for n a positive integer, p a prime.*

Proof. We have that the splitting field of $t^{p^n} - t$ is the splitting field of all ireducible polynomials of degree $d \mid n$ (As $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$. Therefore, all irreducible polynomials of degree $d \mid n$ divide $t^{p^n} - t$, and in fact the product of all these polynomials is $t^{p^n} - t$ as the sum of their degrees is the sum of all of their roots, which is the total number of elements p^n. Let N_d denote the number of irreducible polynomials of degree d. We have that $p^n = \sum_{d|n} N_d d$ from the above result. Using the Möbius Inversion Formula, we thus have:

$$N_n n = \sum_{n|d} p^{\frac{n}{d}}\mu(d) \implies N_n = \frac{1}{n}\sum_{n|d} p^{n/d}\mu(d)$$

This yields the total number of monic polynomials. The total number of irreducibles is given by multiplying (p-1) into the above quantity for every element of the multiplicative group of the field. □

Exercise 8. *Suppose F a field of characteristic p. Show that $[F(x,y) : F(x^p, y^p)] = p^2$ yet there exist infinitely many intermediate fields in the extension.*

Proof. We may construct the extension $F(x, y^p)$ as a p^{th} order extension of $F(x^p, y^p)$ as the minimal poynomial of x is $t^p - y^p$. Similarly, $F(x, y)$ can be constructed as a p^{th} order extension of $F(x, y^p)$ using the same minimal polynomial. Thus, we have that $[F(x, y) : F(x^p, y^p)] \mid p^2$. If the order of the extension were p then there would exist some element w algebraic of degree p over the base field that generates $F(x, y)$. Assume w is some combination $c_1x^a + c_2y^b + c_3x^cy^d$, $c_1, c_2 \in F(x^p, y^p), a, b, c, d < p$. Suppose $x = a_{p-1}w^{p-1} + ... + a_0$. Then $0 = a_{p-1}(c_1x^a + c_2y^b + c_3x^cy^d)^p + ... + a_0 - x$, which is not possible as y^b, x^a, x^cy^d are linearly independent indeterminates over the base field for all $0 < a, b, c, d < p$ so $b, c, d = 0$ implying $w = c_1x$, which does not generate the extension field. Therefore, the extension field is of order p^2, and we can further say that for any $w = c_1x + c_2y$, $\nexists\, d_1x + d_2y \in F(x^p, y^p)(w)$ s.t. $c_2d_1 \neq c_1d_2$, as if this were true then we may obtain 2 different equations in 2 variables, allowing us to use Guassian elimination to yield $x, y \in F(x^p, y^p)(w)$. Thus, we have infinitely many intermediate fields in this extension, given by $F(x^p, y^p)(x + y), F(x^p, y^p)(x + x^py), F(x^p, x^{2p}y^p)(x + x^{3p}y)$... for infinitely many np. These are algebraic extensions of degree p as the minimal polynomial is $t^p - (x^p + x^{3p^2}y^p)$. □

Exercise 9. *Show that the algebraic closure of a countable field is countable.*

Proof. Let K be a countable field. We may compute the cardinality of the algebraic closure by first acknowledging the cardinality of the algebraic closure is the same as the cardinality of all elements that are algebraic over K. Any element that is algebraic over K has an associated minimal polynomial that it is the solution of, which we may represent as an n-tuple for n the degree of the algebraic element. Thus, for each natural number n, the number of elements algebraic over K of degree n is countable (number of n-tuples in K, n roots per each tuple). Thus, the cardinality of the algebraic closure can be represented as:

$$|\widetilde{K}| = \left| \bigcup_{n\in\mathbb{N}} \left(\bigcup_{i=1}^{n} \mathbb{Q} \right) \right|$$

Which is countable. □