

MATH 101B: HOMEWORK

4. HOMEWORK 04 ANSWERS

The following problems were due Thursday (3/1/7).

1. Show that unique factorization domains (UFDs) are integrally closed.

Suppose that R is a UFD with quotient field QR . Then we want to show that any element $x = a/b \in QR$ which is integral over R lies in R . By writing a, b as products of primes, we may assume that they are relatively prime. If x is integral over R then there are elements $c_1, \dots, c_n \in R$ so that

$$x^n + c_1x^{n-1} + \dots + c_n = 0$$

Multiplying by b^n gives

$$a^n + c_1a^{n-1}b + \dots + c_nb^n = 0$$

So, b divides a^n . This is impossible unless b is a unit in which case $a/b \in R$.

2. Show that the integral closure of $\mathbb{Z}[\sqrt{5}]$ (in its fraction field) is $\mathbb{Z}[\alpha]$ where

$$\alpha = \frac{1 + \sqrt{5}}{2}$$

Let R be the integral closure of $\mathbb{Z}[\sqrt{5}]$ in its fraction field $\mathbb{Q}[\sqrt{5}]$. Then R contains α and R is integral over \mathbb{Z} . So it suffices to show that any $a + b\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$ which is integral over \mathbb{Z} lies in $\mathbb{Z}[\alpha]$.

You can prove this using the trace: $\text{Tr} : R \rightarrow \mathbb{Z}$ which is given by

$$\text{Tr}(a + b\sqrt{5}) = (a + \sqrt{5}) + (a - \sqrt{5}) = 2a$$

$2a \in \mathbb{Z} \Rightarrow a = n/2$ for some $n \in \mathbb{Z}$ and the norm: $N : R \rightarrow \mathbb{Z}$ given by

$$N(a + b\sqrt{5}) = (a + \sqrt{5})(a - \sqrt{5}) = a^2 - 5b^2$$

Using the unique factorization of b we see that this is an integer iff $b = m/2$ where $m \in n + 2\mathbb{Z}$. So, $a + b\sqrt{5}$ lies in either $\mathbb{Z}[\sqrt{5}]$ or $\alpha + \mathbb{Z}[\sqrt{5}]$ in either case $a + b\sqrt{5}$ lies in $\mathbb{Z}[\alpha]$. So, $R = \mathbb{Z}[\alpha]$ is the integral closure of \mathbb{Z} and thus of $\mathbb{Z}[\sqrt{5}]$ in $\mathbb{Q}[\sqrt{5}]$.

3. Combining these we see that $\mathbb{Z}[\sqrt{5}]$ is not a UFD. Find a number which can be written in two ways as a product of irreducible elements. [Look at the proof of problem 1 and see where it fails for the element α in problem 2.]

The proof in problem 1 fails for $\alpha = \frac{1+\sqrt{5}}{2}$ because, although the numerator $a = 1 + \sqrt{5}$ and the denominator 2 are relatively prime, the denominator divides the square of the numerator:

$$(1 + \sqrt{5})^2 = 6 + 2\sqrt{5} = 2(3 + \sqrt{5})$$

This gives two factorizations of the same number $6 + 2\sqrt{5}$ into irreducible factors. To show that $1 + \sqrt{5}, 2, 3 + \sqrt{5}$ are irreducible note that their norms are $-4, 4, 4$ respectively.

Lemma 4.1. *Any element of $\mathbb{Z}[\sqrt{5}]$ with norm ± 4 is irreducible.*

Proof. This follows from the following two statements:

- (1) There is no element of $\mathbb{Z}[\sqrt{5}]$ with norm ± 2 .
- (2) Any element of $\mathbb{Z}[\sqrt{5}]$ with norm ± 1 is a unit.

The first follows immediately from the fact that 2 and 3 are not squares modulo 5. The second follows from that fact that if the norm of $a + b\sqrt{5}$ is ± 1 then its inverse is given by $\pm(a - b\sqrt{5})$.

Given these two facts, any element of $\mathbb{Z}[\sqrt{5}]$ with norm ± 4 must be irreducible since, if it factors, one factor must have norm ± 1 since the only way that ± 4 factors as a product of integers is $\pm 1 \cdot 4$ and $\pm 2 \cdot 2$. \square

4. If E is a finite separable extension of K and $\alpha \in E$ show that the trace $\text{Tr}_{E/K}(\alpha)$ is equal to the trace of the K linear endomorphism of E given by multiplication by α . [Show that the eigenvalues of this linear transformation are the Galois conjugates of α and each eigenvalue has the same multiplicity.]

The first proof ignores the hint. For any $\alpha \in E$ take the intermediate field $K(\alpha)$. Then $n = [K(\alpha) : K]$ is the degree of the minimal polynomial of α which is given by

$$f(X) = \prod (X - \alpha_i) = X^n + c_1 X^{n-1} + \cdots + c_n$$

where $c_1 = -\sum \alpha_i$ and $c_n = (-1)^n \prod \alpha_i$. A basis for $K(\alpha)$ over K is given by $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$. Let x_1, \dots, x_m be a basis for E as a vector space over $K(\alpha)$. Then $b_{ij} = \alpha^i x_j, i = 0 \cdots, n-1, j = 1, \dots, m$ forms a basis for E over K . The linear function $\alpha_E : E \rightarrow E$ given by

multiplication by α takes b_{ij} to $b_{i+1,j}$ if $i \neq n-1$ and

$$\alpha_E(b_{n-1,j}) = \alpha^n x_j = - \sum_{k=1}^n c_k \alpha^{n-k} x_j = - \sum_{k=1}^n c_k b_{n-k,j}$$

So, the trace of α_E is

$$\text{Tr}(\alpha_E) = - \sum_{j=1}^m c_1 = m \sum \alpha_i$$

We need to show that this is equal to $\text{Tr}_{E/K}(\alpha)$. Let $\phi_i : K(\alpha) \rightarrow \overline{K}$, $i = 1, \dots, n$ be the n distinct embeddings of $K(\alpha)$ over K . Then $\phi_i(\alpha) = \alpha_i$ are the Galois conjugates of α . Each embedding ϕ_i extends in exactly m ways to an embedding $\psi_{ij} : E \rightarrow \overline{K}$ over K since E is a separable extension of $K(\alpha)$. Therefore,

$$\text{Tr}_{E/K}(\alpha) = \sum \psi_{ij}(\alpha) = m \sum \phi_i(\alpha) = m \sum \alpha_i$$

which is the same as the trace of α_E .

Now, a proof using the hint. Let $g(X) \in K[X]$ be the minimal polynomial of the K -linear endomorphism $\alpha_E : E \rightarrow E$. Since $g(\alpha) = g(\alpha_E)(1) = 0$ it follows that $f(X)|g(X)$. Conversely, $g(X)|f(X)$ since $f(\alpha_E)$ is multiplication by $f(\alpha) = 0$. Therefore $g(X) = f(X)$ (assuming they are chosen to be monic). So, $\deg(g) = \deg(f) = n = [K(\alpha), K]$. Choose a basis x_1, \dots, x_m for E over $K(\alpha)$. Then

$$E = K(\alpha)x_1 \oplus K(\alpha)x_2 \oplus \dots \oplus K(\alpha)x_m$$

and each summand $K(\alpha)x_j$ is invariant under the endomorphism α_E . By the same argument as above, the minimal polynomial of α_E restricted to each summand is $f(X)$. So, the characteristic polynomial of α_E is $f(X)^m$. The eigenvalues of α_E are the roots of the characteristic polynomial which are the roots of $f(X)$ each with multiplicity m . Therefore, the trace of the matrix of α_E is $m \sum \alpha_i = \text{Tr}_{E/K}(\alpha)$.

This proof uses the following two facts about the characteristic polynomial of a linear endomorphism ϕ of a vector space V

- (1) If $V = V_1 \oplus V_2$ where V_1, V_2 are both invariant under ϕ then the characteristic polynomial of ϕ is the product of the characteristic polynomials of $\phi|_{V_i}$.
- (2) The minimal polynomial of ϕ divides the characteristic polynomial of ϕ . In particular, they are equal if they have the same degree.