

Final Exam with solutions

MAT 535
Spring 2000

Name:

ID #:

This is a closed book exam: no notes, books, or laptops running *Maple* allowed.

You can use any results discussed in class, in the homeworks, or any theorem from Artin's book. However, please say which result(s) you are using (for example: "By the structure theorem for modules over a PID,...") unless it is absolutely obvious.

All fields are of characteristic zero; all rings and algebras are associative and with unit, but not necessarily commutative.

Each problem is worth 15 points (so, maximal total is 90); the exam is worth 40% of the grade for the class.

1. Let $R = \mathbb{Q}[x]/I$, where I is the ideal generated by polynomials

$$p_1 = x^4 + x^3 + 2x^2 + 4x + 2$$
$$p_2 = x^5 - x^4 + 2x^3 - 2x$$

Is R a field? an integral domain?

Solution: Since $\mathbb{Q}[x]$ is a PID, the ideal I is actually generated by one polynomial, the greatest common divisor of p_1, p_2 . Explicit calculation shows $\gcd(p_1, p_2) = x^3 + 2x + 2$. By Eisenstein criterion, this polynomial is irreducible; hence, I is a maximal ideal, and R is a field.

2. Let $\pi: \mathbb{R}^n \rightarrow \mathbb{R}^n$ be the operator of orthogonal projection on the subspace $V_0 = \{v \in \mathbb{R}^n \mid \sum v_i = 0\}$:

$$\pi(v) = v - \frac{\sum v_i}{n} \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$$

- (a) Let $P = \pi(\mathbb{Z}^n) \subset V_0$. Show that P is a free abelian group of rank $n - 1$ and construct a basis of P .
- (b) Let $Q = V_0 \cap \mathbb{Z}^n$. Show that Q is a free abelian group of rank $n - 1$ and construct a basis of Q .
- (c) Describe the quotient group P/Q .

Solution: (1) One possible basis: $\omega_i = \pi(e_1), \dots, \pi(e_{n-1})$ (note that $\pi(e_n) = -\pi(e_1 + \dots + e_{n-1})$); everything else is obvious.

(2) One possible basis $\alpha_i = e_i - e_{i+1}$; everything else is obvious.

(3) The answer is $P/Q = \mathbb{Z}_n$. There are several ways to do it. Long way is writing explicitly the matrix expressing α_i in terms of ω_i and then diagonalizing it. A shorter, but more difficult to guess, way is to note that for $x \in P$, it may not be true that all x_i are integer, but $x_i - x_j$ is always an integer. Moreover, for $x \in P$, we have $x \in Q \iff x_i \in \mathbb{Z} \iff x_1 \in \mathbb{Z}$. Thus, the map $x \mapsto nx_1$ maps P to \mathbb{Z} and Q to $n\mathbb{Z}$.

3. Let G be a finite group and V, W – finite-dimensional $\mathbb{C}[G]$ -modules. Show that $\dim \text{Hom}(V, W) = \dim \text{Hom}(W, V)$ (here Hom stands for homomorphisms as $\mathbb{C}[G]$ -modules).

Solution: Every finite-dimensional $\mathbb{C}[G]$ -module is semisimple, so $V = \bigoplus V_i, W = \bigoplus W_j, V_i, W_j$ – simple modules. Thus, $\text{Hom}(V, W) = \bigoplus_{i,j} \text{Hom}(V_i, W_j)$; similarly, $\text{Hom}(W, V) = \bigoplus_{i,j} \text{Hom}(W_j, V_i)$. But $\text{Hom}(V_i, W_j)$ is either zero (if they are not isomorphic) or one-dimensional (if they are isomorphic); in both cases, $\dim \text{Hom}(V_i, W_j) = \dim \text{Hom}(W_j, V_i)$.

4. (In solving this problem, you can use without proof the fact that the ring $\mathbb{Z}[\sqrt{-2}]$ is a PID.) Show that an integer number $X = m^2 p_1 \dots p_k$, where p_i are distinct prime integers, can be presented in the form

$$X = a^2 + 2b^2, \quad a, b \in \mathbb{Z}$$

iff each of p_i can be presented in this form.

Solution: Note that X can be presented in this form iff $X = z\bar{z}$ for some $z \in \mathbb{Z}[\sqrt{-2}]$ (take $z = a + b\sqrt{-2}$).

If each of p_i can be presented in this form, then $p_i = \pi_i \bar{\pi}_i$ for some $\pi_i \in \mathbb{Z}[\sqrt{-2}]$. Then $X = m^2 \pi_1 \bar{\pi}_1 \dots \pi_k \bar{\pi}_k = z\bar{z}$, where $z = m\pi_1 \dots \pi_k$.

Conversely, assume that X can be presented in such form: $X = z\bar{z}$. Since $\mathbb{Z}[\sqrt{-2}]$ is a PID, it is also a unique factorization domain. Let us factor z into product of prime elements in $\mathbb{Z}[\sqrt{-2}]$: $z = \pi_1 \dots \pi_l$ (without loss of generality, we may assume that none of p_i is a unit). This gives a factorization for X :

$$X = \prod_{i=1}^l (\pi_i \bar{\pi}_i).$$

In particular, this implies that if one of $p_i \in \mathbb{Z}$, then it appears in the factorization even number of times.

Assume now that one of p_i can not be presented in the form $z\bar{z}$. Arguing as for the ring $\mathbb{Z}[i]$, we see that this implies that p_i is irreducible in $\mathbb{Z}[\sqrt{-2}]$; it follows from formula $X = m^2 p_1 \dots p_k$ that p_i appears odd number of times in the factorization of X into primes in $\mathbb{Z}[\sqrt{-2}]$. This contradicts the previous factorization.

5. Describe the Galois group of the polynomial $p(x) = (x^3 - 3)(x^2 - 2)$

- (a) Over \mathbb{Q}
- (b) Over $\mathbb{Q}(\zeta), \zeta^2 + \zeta + 1 = 0$.

Solution: First note that the Galois group of $x^3 - 3$ over \mathbb{Q} is S_3 , and over $\mathbb{Q}(\zeta)$ it is $A_3 \simeq \mathbb{Z}_3$ (absolutely identical to Galois group of $x^3 - 2$, many times discussed in class and in homeworks).

(a) The Galois group of p must permute the roots of p , that is, 3 cubic roots of 3 and $\pm\sqrt{2}$. Since it can not mix roots of different irreducible polynomials, it must map roots of $x^3 - 3$ to themselves and roots of $x^2 - 2$ to themselves; in other words, it must be a subgroup in $S_3 \times \mathbb{Z}_2$.

On the other hand, it can be shown that the polynomial $x^2 - 2$ is irreducible over $\mathbb{Q}(\zeta, \sqrt[3]{3})$, so the degree of the splitting field of p over \mathbb{Q} is 12. Thus, $G = S_3 \times \mathbb{Z}_2$.

(b) Similar arguments show that $G = A_3 \times \mathbb{Z}_2 = \mathbb{Z}_3 \times \mathbb{Z}_2$.

6. Let $\zeta = e^{2\pi i/5}, \mathbb{K} = \mathbb{Q}(\zeta + \zeta^{-1})$.

- (a) Consider the chain of extensions $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{Q}(\zeta)$. Show that $[\mathbb{K} : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{K}] = 2$
- (b) Write the irreducible polynomial of $\zeta + \zeta^{-1}$ over \mathbb{Q} .
- (c) Write $\cos 72^\circ, e^{2\pi i/5}$ in terms of radicals.

Solution: (a) As was discussed in class, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$ and the Galois group is \mathbb{Z}_4 . We can choose a generator to be $\tau : \zeta \mapsto \zeta^2$, so that $\tau^2(\zeta) = \zeta^4 = \zeta^{-1}$. The subgroup fixing \mathbb{K} is exactly $1, \tau^2$, which has index 2; thus, $[\mathbb{K} : \mathbb{Q}] = 2$. Since $[\mathbb{Q}(\zeta) : \mathbb{K}][\mathbb{K} : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 4$, we have $[\mathbb{Q}(\zeta) : \mathbb{K}] = 2$.

(b) General result gives $p = \prod(x - \beta)$ where the product is over all elements in the G -orbit of $\zeta + \zeta^{-1}$. In our case, the orbit consists of $\zeta + \zeta^{-1}, \tau(\zeta + \zeta^{-1}) = \zeta^2 + \zeta^{-2}$, so

$$p = (x - (\zeta + \zeta^{-1}))(x - (\zeta^2 + \zeta^{-2})) = x^2 + x - 1,$$

(where we used $\zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} = -1$).

(c) It follows from (b) that

$$\zeta + \zeta^{-1} = \frac{-1 + \sqrt{5}}{2}.$$

Thus, $\cos 72^\circ = \frac{\zeta + \zeta^{-1}}{2} = \frac{-1 + \sqrt{5}}{4}$.

To get ζ , note that $\zeta^2 - \zeta X + 1 = 0$, where $X = \zeta + \zeta^{-1}$; thus,

$$\zeta = \frac{X + \sqrt{X^2 - 4}}{2} = \frac{\frac{-1 + \sqrt{5}}{2} + \sqrt{\left(\frac{-1 + \sqrt{5}}{2}\right)^2 - 4}}{2}$$