Modern Algebra II, fall 2020, Instructor M.Khovanov

Homework 5, due Wednesday October 14.

1. (20 points) Starting with the axioms of a vector space V over a field F prove
(a) $a\underline{0} = \underline{0}$, where $a \in F$ and $\underline{0}$ is the zero vector in V (that is, $\underline{0} + v = v$ for all $v \in V$).
(b) $0v = \underline{0}$, for $v \in V$ and the zero element 0 of F.
(c) $av = \underline{0}$ iff $a = 0$ or $v = \underline{0}$ (where $a \in F$ and $v \in V$).
(d) $av = aw$ iff $a = 0$ or $v = w$, for $a \in F$ and $v, w \in V$.
Here we denote the zero element of F by 0 and the zero vector of V by $\underline{0}$ to distinguish the two.

2. (10 points) Suppose a ring R contains a field $\mathbb{F}$ as a subring. Check that R is naturally an $\mathbb{F}$-vector space. Next, suppose I is an ideal of R. Prove that I is an $\mathbb{F}$-vector subspace of R. Note that the implication does not work the other way, most vector subspaces of R are not ideals in R. Can you give an example of $\mathbb{F}$ and R as above and an F-subspace V of R which is not an ideal in R?

3. (10 points) Find irreducible polynomials $f(x)$ and $g(x)$ over $\mathbb{F}_3$ of degrees 2 and 3, respectively, and use them to define fields with 9 and 27 elements, respectively. Call these fields $\mathbb{F}_9$ and $\mathbb{F}_{27}$. Explain why $\mathbb{F}_9$ is not isomorphic to a subfield of $\mathbb{F}_{27}$. What can you say about multiplicative groups $\mathbb{F}_9^*$ and $\mathbb{F}_{27}^*$?

4. (20 points) (a) Consider the field $F = \mathbb{F}_2[\alpha]/(\alpha^3 + \alpha + 1)$. From the theorem proved in class we know that $B = (1, \alpha, \alpha^2)$ is a basis of F over $\mathbb{F}_2$. Take $\beta = \alpha + 1$. Write down powers $1, \beta, \beta^2$ in the basis B and check that they are linearly independent over $\mathbb{F}_2$. Then compute β^3 and find a linear dependence between $1, \beta, \beta^2, \beta^3$. Write this linear dependence between powers of β as the equation $g(\beta) = 0$, where g is a degree 3 polynomial with coefficients in $\mathbb{F}_2$. Your polynomial $g(x)$ should be different from the polynomial $f(x) = x^3 + x + 1$ that we use to define F.
(b) Check that f and g in (a) are the only two monic irreducible degree 3 polynomials over $\mathbb{F}_2$. Use observations in (a) to conclude that the field $F = \mathbb{F}_2[\alpha]/(f(\alpha))$ is isomorphic to the field $\mathbb{F}_2[\beta]/(g(\beta))$, even though the monic polynomials f, g are different.

5. (20 points) (a) Take the field $\mathbb{F}_8 = \mathbb{F}_2[\alpha]/(\alpha^3 + \alpha + 1)$. Write down how the Frobenius endomorphism Fr (also denoted σ_2) acts on each element of $\mathbb{F}_8$. (Recall that $\sigma_2(a) = a^2$ for all $a \in \mathbb{F}_8$.) Check that σ_2 is bijective and conclude that it is an automorphism of the field $\mathbb{F}_8$.
(b) Recall and write down the details of the proof of the theorem, mentioned in class, that the Frobenius endomorphism σ_p is bijective on any finite field F of characteristic p (that is, F that contain $\mathbb{F}_p$). Conclude that σ_p is an automorphism of F. (When F has characteristic p but is not finite, σ_p may not be an automorphism; σ_p is always injective but not always surjective.)

6. (optional, need to be familiar with countable vs. uncountable sets). (a) Suppose F is a field with countably many elements (for instance, $\mathbb{F}_p$ or $\mathbb{Q}$). Show that a finite-dimensional vector space V over F is countable (you can use standard theorems and arguments from the set theory, such as the diagonalization construction). Even more is true: suppose that V has an infinite but countable basis $(v_1, v_2, \ldots)$ as an $\mathbb{F}$-vector space. Prove that V is countable. An example of such V is $F[x]$.
Use this result to show that any basis of $\mathbb{R}$, as a $\mathbb{Q}$-vector space, is uncountable. Try constructing such a basis explicitly (you'll find that it's quite hard to find one). In particular, $\mathbb{R}$ is a vector space over $\mathbb{Q}$ of uncountable dimension, ditto for $\mathbb{C}$.

(b, even more optional) Also show that the field $\mathbb{F}_p(x)$ of rational functions in one variable x and coefficients in $\mathbb{F}_p$ is infinite but has a countable basis over $\mathbb{F}_p$. Hint: use suitable rational functions in x to construct a countable spanning set of $\mathbb{F}_p(x)$. Or just argue that $\mathbb{F}_p(x)$ has countably many elements.