Paul Gustafson
Texas A&M University - Math 416
Instructor: Dr. Papanikolas

HW 3, due 2/14

30.21 Prove that if V is a finite-dimensional vector space over a field F, then a subset $\{\beta_1, \ldots, \beta_n\}$ of V is a basis for V over F if and only if every vector in V can be expressed uniquely as a linear combination of the β_i.

Proof. Suppose $B := (\beta_i)$ is a basis for V. Let $v \in V$. Since B spans V, there exist (a_i) such that $v = \sum_i a_i \beta_i$. To see that the (a_i) are unique, suppose (b_i) also satisfy $v = \sum_i b_i \beta_i$. Subtracting, $0 = \sum_i (a_i - b_i)\beta_i$, which implies $a_i = b_i \forall i$ by the linear independence of B.

Conversely, suppose every vector in V can be expressed uniquely as a linear combination of $B := (\beta_i)$. Then B trivially spans. Also, if $0 = \sum_i a_i \beta_i$ for some a_i, then $a_i = 0$ for all i by the uniqueness. □

30.24 Let V and V' be vector spaces over the same field F.

a. If $\{\beta_i : i \in I\}$ is a basis for V over F, show that a linear transformation $\phi : V \to V'$ is completely determined by the vectors $\phi(\beta_i) \in V'$.

   Proof. Let $v \in V$. Then $v = \sum_i v_i \beta_i$, so $\phi(v) = \sum_i v_i \phi(\beta_i)$. □

b. Let $\{\beta_i : i \in I\}$ be a basis for V, and let $\{\beta'_i : i \in I\}$ be any set of vectors, not necessarily distinct, of V'. Show that there exists exactly one linear transformation $\phi : V \to V'$ such that $\phi(\beta_i) = \beta'_i$.

   Proof. Let $v \in V$. Then $v = \sum_i v_i \beta_i$ for unique v_i. Define $\phi(v) := \sum_i v_i \beta'_i$. ϕ is obviously linear. The uniqueness follows from (a). □

30.25 Let $\phi : V \to V'$ be a linear transformation.

a. Linear transformation is to vector space as what is to groups/rings?
   Answer: Homomorphism.

b. Define the *kernel* of ϕ, and show that it is a subspace of V.

   Proof. $\ker(\phi) := \phi^{-1}(0)$. Suppose $v, w \in \ker(\phi)$, then $\phi(\alpha v + \beta w) = 0$ by linearity. □

c. Describe when ϕ is an isomorphism of V with V'.
   Answer: ϕ must be bijective linear transformation. That is, $\ker(\phi) = \{0\}$ and $\phi(V) = V'$.

30.27 Let $\phi : V \to V'$ be F-linear with V finite dimensional.

a. Show that $\phi(V)$ is a subspace.

Proof. Let $v, w \in \phi(V)$. Note that $\{\alpha v + \beta w\} = \phi(\alpha\phi^{-1}(v) + \beta\phi^{-1}(w))$. $\square$

b. Show that $\dim(\phi(V)) = \dim(V) - \dim(\ker(\phi))$.

Proof. Let $A := (\alpha_i)$ be a basis for $\ker(\phi)$. Extend it to a basis for V by adding the vectors in $B := (\beta_i)$. It is easy to check that $(\phi(\beta_i))_i$ forms a basis for $\phi(V)$. Indeed, by a previous problem on this homework, $\phi(B) = \phi(A \cup B)$ spans $\phi(V)$. Linear independence follows from the linearity of ϕ and linearly independence of B. $\square$

31.6 Find the degree and a basis for $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$.

Proof. I claim $f(x) := x^4 - 10x^2 + 1 = irr(\sqrt{2}+\sqrt{3}, \mathbb{Q})$. Note that $\sqrt{2} \pm \sqrt{3}$ and $-\sqrt{2} \pm \sqrt{3}$ are the roots of f over $\mathbb{C}$. It is easy to check that every product involving a proper subset of the linear factors of f has an irrational coefficient. For example, to see $\sqrt{2}+\sqrt{3}$ is irrational, suppose $\sqrt{2}+\sqrt{3} = r$ for $r \in \mathbb{Q}$. Square both sides to reduce to the case that $\sqrt{6}$ is irrational.

Hence, $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$ is of degree 4, and a basis is $\{1, (\sqrt{2}+\sqrt{3}), (\sqrt{2}+\sqrt{3})^2, (\sqrt{2}+\sqrt{3})^3\}$. $\square$

31.10 Find the degree and a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{6})/\mathbb{Q}(\sqrt{3})$.

Proof. The degree is 2, a basis is $\{1, \sqrt{2}\}$. This follows from the fact that $\sqrt{2} = a + b\sqrt{3}$ has no solutions over $\mathbb{Q}$ (square both sides, etc.). $\square$

31.13 Find the degree and a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{6}+\sqrt{10})/\mathbb{Q}(\sqrt{3}+\sqrt{5})$.

Proof. The degree is 2, a basis is $\{1, \sqrt{2}\}$. The proof that $\sqrt{2}$ is irreducible over $\mathbb{Q}(\sqrt{3}+\sqrt{5})$ is straightforward, but tedious case work. $\square$

31.23 Show that if E is a finite extension of a field F and $[E : F]$ is a prime number, then E is a simple extension of F and $E = F(\alpha)$ for every $\alpha \in E \setminus F$.

Proof. Let $\alpha \in E \setminus F$. Suppose $F(\alpha) \neq E$. But then we are in trouble since $[E : F] = [E : F(\alpha)][F(\alpha) : F]$ which contradicts the assumption that $[E : F]$ is prime.

$\square$

31.27 Prove in detail that $\mathbb{Q}(\sqrt{3}+\sqrt{7}) = \mathbb{Q}(\sqrt{3}, \sqrt{7})$.

Proof. It is obvious that $\mathbb{Q}(\sqrt{3}+\sqrt{7}) \subset \mathbb{Q}(\sqrt{3}, \sqrt{7})$. For the opposite inclusion, let $f := irr(\sqrt{3}+\sqrt{7}, \mathbb{Q})$. It is easy to check that the roots of f over $\mathbb{C}$ are $\sqrt{3} \pm \sqrt{7}$ and $-\sqrt{3} \pm \sqrt{7}$, and that every product of proper subsets of the linear factors of f has an irrational coefficient. Hence, $((\sqrt{3}+\sqrt{7})^i)_{i=0}^3$ forms a basis for $\mathbb{Q}(\sqrt{3}+\sqrt{7})$. Note that $(\sqrt{3}+\sqrt{7})^3 = 14\sqrt{3} + 16\sqrt{7}$. Thus, $\sqrt{3}$ and $\sqrt{7}$ are in the span of $(\sqrt{3}+\sqrt{7})^3$ and $\sqrt{3}+\sqrt{7}$. $\square$

31.30 Let E be an extension field of F. Let $\alpha \in E$ be algebraic of odd degree over F. Show that α^2 is algebraic of odd degree over F, and $F(\alpha) = F(\alpha^2)$.

Proof. We have $[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$. Note that if the first factor is 1, then we are done. If the second factor is 1, then $[F(\alpha) : F] \leq 2$ which implies $F(\alpha) = F(\alpha^2) = F$ since $[F(\alpha) : F]$ is odd.

The remaining case is that both factors are greater than 1, hence greater than 2 since their product is odd. Let $m := [F(\alpha^2) : F]$. There exists a F-linear dependence involving $1, \alpha^2, \ldots, \alpha^{2m}$. But then $[F(\alpha) : F] \leq 2m$, a contradiction.

$\square$

30.34 Show that if E is an algebraic extension of a field F and contains all zeros in $\bar{F}$ of every $f(x) \in F[x]$, then E is an algebraically closed field.

Proof. Let $g(x) \in E[x]$ with $g(x) = \sum_{i=1}^{n} a_i x^i$ with $a_n \neq 0$. Let $K = F(a_1, \ldots, a_n)$. Since each a_i is algebraic over F, K/F is a finite extension. Since g lies in $K[x]$, any root α of g must lie in a finite extension of K. By the product of degrees in towers theorem, then, α lies in a finite extension of F. In particular, there must be a finite linear dependence relation among the powers of α. That is, *alpha* is a root of a polynomial over F. $\square$