# Homework 11 Solutions

3 (a) See Homework 10. This matrix is diagonalizable if and only if $x^2+1$ factors over the field.

(b) The characteristic polynomial is $(x-3)^2(x^2+(-6-a)x+6a-3)$, and so the matrix is diagonalizable if and only if $x^2-(6+a)x+6a-3$ factors over the field. The solution to $x^2+(-6-a)x+6a-3=0$ are $x=\frac{a+6\pm\sqrt{(a+6)^2-4(6a-3)}}{2}$. The quantity under the root is $(a+6)^2-24a+12=a^2+12a+36-24a+12=a^2-12a+48$. So this matrix is diagonalizable if and only if $a^2-12a+48$ is a square.

(c) The characteristic polynomial is $x^3+(-a^2-4)x^2+(4a^2-9a-3)x+(-a^2+5a-6)$. The matrix is diagonalizable if the field contains all three roots, which can be obtained via the cubic formula.

4 (a) Subtracting the first from the second twice, gives the system $x+y+z=0$ and $y+(a-2)z=1$, so $y=1-(a-2)z$. Plugging this into the first equation gives $x+1-(a-2)z+z=0$, which gives $x+1+(2-a)z+z=0$, which is $x+1+(3-a)z=0$, and so $x=-1+(a-3)z$. Thus, the solutions to the system are $(-1+(a-3)z, 1-(a-2)z, z)$ for all $z\in R$.

(b) This is an inhomogeneous system of four equations in three unknowns. Thus, it is only solvable if the matrix $\begin{pmatrix} a & 1 & 0 & c \\ 1 & a & 0 & c \\ 1 & b & 0 & d \\ 1 & 1 & 1 & d \end{pmatrix}$ is singular. That is, one of the equation is a linear combination of the others. This will happen only if the determinant of this matrix is zero. So the system is solvable iff the elements $a,b,c,d$ satisfy $abc-ad+ac-bc-c+d$.

4 (a) Set $x=\sqrt{2}+\sqrt{3}$. Then $x^2=(\sqrt{2}+\sqrt{3})^2=2+3+2\sqrt{6}=5+2\sqrt{6}$, $x^3=(\sqrt{2}+\sqrt{3})(5+2\sqrt{6})=5\sqrt{2}+5\sqrt{3}+4\sqrt{2}+6\sqrt{3}=9\sqrt{2}+11\sqrt{3}$, and $x^4=(5+2\sqrt{6})^2=25+24+10\sqrt{6}=49+10\sqrt{6}$. So we look at $x^4-10x=-1$, and so find that $\sqrt{2}+\sqrt{3}$ satisfies $x^4-10x^2+1$.

(b) The previous part bounds the degree by 4. As it isn't in $\mathbb{Q}$, it has degree at least one. So we must merely eliminate the possibility of 2 or 3. Assume it is of degree 2. Then it satisfies an equation of the form $ax^2+bx+c=a(5+2\sqrt{6})+b(\sqrt{2}+\sqrt{3})+c=0$. The only solution to this is zero, because we must have $b = 0$, because nothing can cancel the $\sqrt{2}$, and then $a = 0$ for the $\sqrt{6}$, adn this implies $c = 0$. Similarly, for a cubic, we have $ax^3 + bx^2 + cx + d = 0$, which is $a(9\sqrt{2} + 11\sqrt{3}) + b(5 + 2\sqrt{6}) + c(\sqrt{2} + \sqrt{3}) + d = 0$. This breaks up to $9a + c = 0$, $11a + c = 0$, $5b + d = 0$ and $2b = 0$. So $b = 0$, which implies $d = 0$, and the system $9a + c = 0$ and $11a + c = 0$ tells us that $a = c = 0$.

(c) The degree of $\sqrt{2}\sqrt{3} = \sqrt{6}$ is two. It is not 1, as $\sqrt{6}$ is not rational, and it satisfies $x^2 - 6$.

8 As $b$ satisfies an equation of degree $m$ over $F$, it must satisfy the same equation over $F(a)$, and so $F(a, b)$ is of degree at most $mn$ over $F$. So $[F(a, b) : F] \leq mn$. Now, by the Corollary on 209, we have that $[F(a) : F]$ and $[F(b) : F]$ divide $[F(a, b) : F]$. So we have a number which is less than or equal to $mn$ and divisible by $m$ and $n$, which are relatively prime. The only possible such number is $mn$, and so $[F(a, b) : F] = mn$.

9 (a) As $(F, +)$ is a finite abelian group, there exists a number $n \in \mathbb{N}$ such that for all $a \in F$, $na = 0$. Let $p$ be the smallest such number. We claim that $p$ is prime. This is because if it is not, then $p = ab$, and for all $x \in F$, we have $px = abx = 0$, and so $a(bx) = 0$, which means that $a, bx$ are zero divisors, because $p$ was the smallest number such that $px = 0$ for all $x \in F$. But $F$, being a field, has no zero divisors, which gives us a contradiction, so $p$ is prime.

(b) Now, $F$ contains as a subfield $\mathbb{Z}/p\mathbb{Z}$, the field consisting of all integer multiples of the identity. Thus, $F$ is a $\mathbb{Z}_p$-vector space. As $F$ is finite, it is finite dimensional, of dimension $n$. Thus, we have an isomorphism $F \cong \mathbb{Z}_p^n$. Isomorphisms are bijections, and so we have $q = |F| = |\mathbb{Z}_p^n| = |\mathbb{Z}_p|^n = p^n$, as desired.

(c) The multiplicative group of $F$ has order $q^n - 1$, and so for all $a \in F^\times$, we have $a^{q^n - 1} = 1$. Multiplying both sides by $a$, we obtain $a^{q^n} = a$ for all $a \in F$.

(d) As $K$ is algebraic over $F$, it is a finite-dimensional $F$-vector space. So $K \cong F^m$, and so we have $|K| = q^m$. Then the same argument from the previous part establishes that $b^{q^m} = b$ in $K$.