Solutions to Test 2

1 a) $[\mathbb{Q}(\sqrt{3},\sqrt{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3},\sqrt{7}) : \mathbb{Q}(\sqrt{3})]\,[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}]$.

$= 2 \cdot 2 = 4$

$(\sqrt{7} \notin \mathbb{Q}[\sqrt{3}])$.

b) A basis for $\mathbb{Q}[\sqrt{3},\sqrt{7}]$ over $\mathbb{Q}$, from the proof of the theorem on computing the degree of finite extensions is.

$\{1, \sqrt{3}, \sqrt{7}, \sqrt{21}\}$.

2 a) $\sqrt{3}+i \in \mathbb{Q}[\sqrt{3},i]$ and $[\mathbb{Q}[\sqrt{3},i] : \mathbb{Q}] = 4$ (similar to the above)

Finite extensions are algebraic so $\sqrt{3}+i$ is algebraic over $\mathbb{Q}$.

b) $\sqrt{3}+i$ has either degree 2 or 4 over $\mathbb{Q}$. If it had degree 2 then $1, z$ and z^2 would be linearly dependent. $z^2 = 2 + 2\sqrt{3}i$ and we know that $1, i, \sqrt{3}$ and $\sqrt{3}i$ are linearly independent.

If $k_1 + k_2 z + k_3 z^2 = 0$ then $k_3 = 0$ since $\sqrt{3}i$ appears only in z^2. Then $k_2 = 0$ since $i, \sqrt{3}$ only appear there. Finally $k_1 = 0$. So the degree of z is 4.

3a) Zorn's Lemma: If $(P, <)$ is a partial order in which all chains are bounded then P has a maximal element.

b) Suppose that V is an F-vector space. Let $P = \{ I \subseteq V : I \text{ is linearly independent} \}$.

Partially order P by inclusion.

If $\mathcal{C}$ is a chain in P then let $I = \bigcup \mathcal{C}$. For any $J \in \mathcal{C}$, $J \subseteq I$ so if I is in P then I is an upper bound for $\mathcal{C}$.

Now suppose $v_1, \dots v_n \in I$. Then there are $J_1, \dots J_n \in \mathcal{C}$ s.t. $v_i \in J_i$. Since $\mathcal{C}$ is a chain, there is some i s.t. $J_j \subseteq J_i$ for all j. So $v_1, \dots v_n \in J_i$ and so are lin. indep.

So P is a partial order in which all chains are bounded. Apply Zorn's Lemma to get a maximal $I \in P$. If the span of I is not all of V then there is a $v \in V \setminus \text{span}(I)$. But then $I \cup \{v\}$ is lin. indep. ~~$\not$~~ contradicting I is maximal.

So I is lin indep and spans V so I is a basis for V.

4. If F is finite then its characteristic is p for some prime number p ($\neq 0$). The subfield generated by 1 is then isomorphic to $\mathbb{Z}_p$.

As a vector space over $\mathbb{Z}_p$, F has some finite dimension say n and then $|F| = p^n$.

5. By the HBT, I has a finite basis say $f_1 \cdots f_n$. We also have that $I = \langle S \rangle$.

So for each f_i we can find $g_1^i \cdots g_{k_i}^i \in S$ so that $f_i \in \langle g_1^i \cdots g_{k_i}^i \rangle$. If we let $S_0 = \{ g_j^i : i \leq n, j \leq k_i \}$ then S_0 is finite, $S_0 \subseteq S$ and since $f_i \in \langle S_0 \rangle$ and $I = \langle f_1 \cdots f_n \rangle$, $I = \langle S_0 \rangle$.