Answersheet 11 - Yiwei Yang 2018533218

1.

First define the polynomial $f_S(x)$ is called the minimal polynomial of S (over F).

Then consider the unique map $\phi_S : F[x] \to E$ which is the identity on F and sends x to S. As ϕ_S is a ring homomorphism, it send a polynomial $f(x)$ to $f(S)$. The image of ϕ_S contains F and S and is the smallest. Thus $F[S] \cong F[x]/\ker(\varphi_S)$. Now, S is algebraic iff ϕ_S has a non-trivial kernel and the kernel is generated by a polynomiala $f_S(x)$ of positive degree that we may simply choose to be monic. If $f_S(x) = f(x)g(x)$ is a proper factorization of $f_S(x)$, then by CRT, $F[x]/\left(f_S(x)\right) \cong F[x]/(f(x)) \times F[x]/(g(x))$. The RHS the product of non-zero rings can not be a field. Thus $f_S(x)$ is irreducible and $F[x]$ is a PID, the ideal $((f_S(x)))$ is maximal, so $F[S] \cong F[x]/\left(f_S(x)\right)$ is a field. Thus $F[S] = F(S)$.

But not for infinite S, because let $E/F, E = F(u)$, be a simple field extension. Then u is algebraic if and only if E/F is finite. In this case, $[E : F] = \deg f_u$.

Proof. If u is transcendental, then $1, u, u^2, \ldots$ are linearly independent because otherwise we would obtain a polynomial $f \in F[x], f \neq 0$, with $f(u) = 0$.

If u is algebraic and $n = \deg f_u$, then I claim that $1, u, \ldots, u^{n-1}$ is a basis of E as an F -vector space. To confirm this, observe first of all that these elements are linearly independent, by the argument from the previous paragraph: if we had a linear relation $a_0 + a_1 u + \ldots + a_{n-1} u^{n-1} = 0$ with coefficients $a_j \in F$, not all equal to zero, then we would obtain a (monic, after division by the highest non-zero coefficient) polynomial $g \in F[x], g \neq 0$, with $g(u) = 0, \deg g < n$ but this contradicts the definition of the minimal polynomial as the polynomial of smallest possible degree for which this happens.

To see that $1, u, \ldots, u^{n-1}$ span E, recall that $E = F[u]$, so any element of E is a linear combination of powers $u^j, j \geq 0$. Now from $f_u(u) = 0$, we obtain a formula of the type $u^n = b_{n-1} u^{n-1} + \ldots + b_0$. So powers u^j with $j \geq n$ may be expressed in terms of powers with smaller exponents, and by applying this repeatedly, we can completely eliminate powers u^j with $j \geq n$ from the linear combination.

2.

$\mathbb{Q}$ has characteristic 0 and is countable by a famous spiral argument.

A field K has characteristic 0 if and only if $\mathbb{Q}$ is a subfield of K
So, the way I have approached this is by first assuming that K has characteristic 0 and then we know that there is an embedding of $\mathbb{Z}$
into K and since $n.1$ is in K, then, their inverses will also be in K and
hence the subfield that we get is the one generated by 1 and this is the prime subfield of K and this is isomorphic to $\mathbb{Q}$. So K contains
$\mathbb{Q}$. But I am not sure how to progress the other way.

As $|\mathbb{Q}|$ <= $|\mathbb{Z} \times \mathbb{Z}|$ and the latter is countable, $\mathbb{Q}$ is countable.

3.

Let E/F be a field extension. Define
$A=\{a \in E: a$ is algebraic over $F\}$
Then A is a field, and $F \subseteq A \subseteq E$.
Proof. The inclusions are clear because every $a \in F$ is algebraic, with minimal polynomial $f_a=x-a$. So we must show that A is a subfield of E. Let $a, b \in A$. We must show that then $a-b$ and $ab^{-1}($ if $b \neq 0)$ are in A as well.

Now $F(a, b)/F$ is a finite extension, by the same arguments as in the previous proof (adjoin a, b separately and successively and observe that each individual extension is finite). Moreover, $a-b, ab^{-1} \in F(a, b)$, so $F(a-b) \subseteq F(a, b)$ also is a finite extension of F, and thus $a-b$ is algebraic by **1.but** (and similarly for ab^{-1}).

4.

Proof. We know from above that if $\phi: E \rightarrow L$ extends σ, then $\phi(\alpha)$ must be a root of $f_\alpha^\sigma(x)$ showing that the number of ϕ is at most the number of distinct roots of $f_\alpha(x)$. On the other hand, given a root β of f^σ in Ω, there is a unique homomorphism $F[x] \rightarrow L$ that agrees with σ on F and sends x to β (this is the freeness property of the polynomial algebra composed with the isomorphism $F[x] \cong F^\sigma[x])$. Since $K=F(\alpha) \cong F[x]/\left(f_\alpha(x)\right) \cong F^\sigma[x]\left(f_\alpha^\sigma(x)\right)$ and $f_\alpha^\sigma(\beta)=0$ (i.e. the kernel of the map $F[x] \rightarrow \Omega$ is contained in $\left(f_\alpha(x)\right)$), the universal property of quotients yields a unique homomorphism $\phi: E \rightarrow L$ agreeing with σ on F and sending α to β.