Paper Code AV-8203

M.A./M.Sc. Ist Sem 2015-16

Adv. Abst. Alg. I

Suggested Solution.

1 (i) Since a group is nilpotent if and only if it has a normal series whose factors are contained in the center of a certain group, it follows that it has a normal series whose factors are abelian groups. Also a group is solvable if and only if it has a normal series with abelian factors so the result follows.

(ii) As, for $n \geq 3$ the group S_n is a group whose center contains only the identity element of S_n it follows that for each i, $Z_i(S_n)$ contains only the identity element. Thus $\nexists$ positive integers m such that $Z_m(S_n) = S_n$ for $n \geq 3$ and so S_n is not nilpotent.

(iii) Let R and S be rings. A mapping $f: R \to S$ is said to be an antihomomorphism if $\forall\, x, y \in R$ we have

(i) $f(x+y) = f(x) + f(y)$ &

(ii) $f(xy) = f(y)\, f(x)$

(iv) For any $ab \in AB$ we have $ab = ab + a0 = a(b+0)$ and for any $ac \in AC$ we have $ac = a0 + ac = a(0+c)$ it follows that both ab and ac are in $A(B+C)$ so $AB \subseteq A(B+C)$ as well as $AC \subseteq A(B+C)$ and therefore $AB + AC \subseteq A(B+C)$. Again for any $a(b+c) \in A(B+C)$ with $a \in A$ $b \in B$ and $c \in C$

we have $a(b+c) = ab+ac \in AB+AC$ so that $A(B+C) \subseteq AB+AC$. Hence $A(B+C) = AB+AC$.

(v). A module M over a ring R is said to be faithful if for some $r \in R$ $rm = 0$ $\forall$ $m \in M$ imply that $r = 0$.

(vi). A subset B of an R-module M is called a basis for M if :

(i) M is generated by B.

(ii) B is linearly independent.

(vii) Let $f(x) \in \mathbb{Z}[x]$ be primitive polynomial. Then $f(x)$ is reducible over $\mathbb{Q}$ if and only if $f(x)$ is reducible over $\mathbb{Z}$.

(viii) By definition of splitting field, it follows that K is a finitely generated extension of F with α_i $1 \leq i \leq n$ (say) such that each α_i is algebraic over F. So it follows that K is a finite ~~ex~~ extension over F and hence is an algebraic extension of F.

(ix) Student's choice.

(x) Let F and E be fields. The distinct embeddings of F into E are linearly independent.

2 (a). A composition series of a group G is a normal series without repetition whose factor groups are all simple groups.

P.t.o.

Let G be a finite group. If $|G| = 1$ then the composition series of G has no factors and so the result is trivial. Further if G is simple $\{e\} \trianglelefteq G$ is its composition series. So now we may suppose that G is not simple and $|G| > 1$. We now prove the remaining part by induction. So let us assume that the result holds for all groups of order less than $|G|$. (The induction has started as we have shown the result for $|G| = 1$) Since $|G| < \infty$ we can find a maximal normal subgroup of G say H. Since $|G| > |H|$, H by induction hypothesis has a composition series say $\{e\} \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n = H$. But then

$$\{e\} \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n \subseteq G$$ is a composition series for G.

2 (b). Suppose G is a nilpotent group of class m and H is a subgroup of G. Let $z \in H \cap Z(G)$ then $z \in H$ and z commutes with every element of G so $z \in H$ and z commutes with every element of H. Therefore $z \in Z(H)$. Thus $H \cap Z_1(G) = H \cap Z(G) \subseteq Z(H)$. Next $\forall\ x \in Z_2(G)$ and $y \in G$ $xyx^{-1}y^{-1} \in Z_1(G)$ so $\forall\ x \in H \cap Z_2(G)$ and $y \in H$ $xyx^{-1}y^{-1} \in H \cap Z_1(G) \subseteq Z_1(H)$ so we get $H \cap Z_2(G) \subseteq Z_2(H)$. By repeating the argument we see that

$H \cap Z_i(G) \subseteq Z_i(H)$ $i = 1, 2, \ldots, m$. Hence $H = H \cap G$

$= H \cap Z_m(G) \subseteq Z_m(H)$ Thus $Z_m(H) = H$ i.e. H must be nilpotent.

Let, now, $\phi : G \longrightarrow H$ be any surjective homomorphism of G on to another group H and G be nilpotent of class m. Now $\forall\ x, y \in G$ we have

$$\phi(xyx^{-1}y^{-1}) = \phi(x)\,\phi(y)(\phi(x))^{-1}(\phi(y))^{-1}$$

so $\phi(Z(G)) \subseteq Z(H)$ Let $x \in Z_2(G)$ then $xyx^{-1}y^{-1} \in Z(G)$ $\forall\ y \in G$ but then

$$\phi(x)\,\phi(y)(\phi(x))^{-1}(\phi(y))^{-1} \in \phi(Z(G)) \subseteq Z(H).$$

As ϕ is on to it follows that $\phi(x) \in Z_2(H)$.

So $\phi(Z_2(G)) \subseteq Z_2(H)$. By repeated use of this argument we get

$$\phi(Z_i(G)) \subseteq Z_i(H) \quad 1 \le i \le m.$$

Hence $H = \phi(G) = \phi(Z_m(G)) \subseteq Z_m(H)$

i.e. $Z_m(H) = H$, so H must be nilpotent.

3 (a). (i) $\Rightarrow$ (ii) Since $0 = 0 + 0 + \cdots + 0$ with $0 \in A_i$ $1 \le i \le n$ and $0 = a_1 + \cdots + a_n$ in given it follows by definition of direct sum that for each i $1 \le i \le n$ $a_i = 0$.

(ii) $\Rightarrow$ (iii) If $x \in A_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{n} A_j$ then we have

$$x = a_1 + a_2 + \cdots + a_{i-1} + a_{i+1} + \cdots + a_n \in A_i$$

thus $0 = a_1 + \cdots + a_{i-1} + (-x) + a_{i+1} + \cdots + a_n$

so by (ii), we get $x = 0$.

(iii) $\Rightarrow$ (i) Let $a = a_1 + a_2 + \cdots + a_n$ and

$a = b_1 + b_2 + \cdots + b_n$ be two representation of $a \in \sum A_i$ with $a_i, b_i \in A_i$ $1 \le i \le n$

then $0 = (a_1 - b_1) + (a_2 - b_2) + \cdots + (a_n - b_n)$.

So $a_1 - b_1 \in A_1 \cap \sum_{j=2}^{n} A_j = \{0\}$

Thus $a_1 = b_1$. Similarly $a_2 = b_2, \ldots a_n = b_n$.

Hence $A = \sum_{i=1}^{n} A_i$ is a direct sum.

3 (b) First suppose that P is a prime ideal of R and $a, b \in R$ are such that $ab \in P$. Since $\langle a \rangle \langle b \rangle$ consists of finite sums of products of elements of the type $na + ar$ and $mb + bs$ with $n, m \in \mathbb{Z}$ and $r, s \in R$, we consider these elements only.

Now $(na + ar)(mb + bs) = nmab + nabs + mabr + abrs$

(using the fact that R is commutative) so $ab \in P$ and P is an ideal implies that $(na + ar)(mb + bs)$ [and finite sums of such like products] $\in P$. Hence $\langle a \rangle \langle b \rangle \subseteq P$. Since P is prime $\langle a \rangle \subseteq P$ or $\langle b \rangle \subseteq P$ but then $a \in P$ or $b \in P$. [$\because$ $a = 1.a + a.0$ with $1 \in \mathbb{Z}$ or $b = 1.b + b.0$ with $1 \in \mathbb{Z}$]

Conversely, let $ab \in P \Rightarrow a \in P$ or $b \in P$ with $a, b \in R$. We need to show that P is prime. Let A and B be ideals of R such that $AB \subseteq P$.

Suppose if possible $A \subseteq P$. Choose an element $a \in A$ such that $a \notin P$. Then $AB \subseteq P \Rightarrow aB \subseteq P$ so $ab \in P \ \forall\ b \in B$. But then by our hypothesis $b \in P \ \forall\ b \in B$. Hence $B \subseteq P$.

4(a). Let $S = \{ A \mid A$ is an ideal of R $A \neq R$ & $I \subseteq A \}$ then $(S, \subseteq)$ is a partially ordered set under inclusion relation. Let C be any chain in S and U denote the union of members of the chain C. We show that $U \in S$. For this first let $a, b \in U$ then $\exists$ $A, B \in C \subseteq S$ with $a \in A$ and $b \in B$ As C is a chain either $A \subseteq B$ or $B \subseteq A$ accordingly $a-b \in B$ or $a-b \in A$. Also ra and ~~ar~~ ar are ~~is~~ both in B or both in A $\forall\ r \in R$. In each of these ~~cases $a-b$, ar, $ra \in C$~~

Cases $a-b$, ar, $ra \in U$. Thus U is an ideal of R. If $U = R$ then $1 \in R = U$ imply that $1 \in X$ for some $X \in C$ and so $X = R$ which is not true. Hence $U \neq R$. Thus $U \in S$. This shows that every chain in S has an upper bound in S. So by Zorn's lemma S has a maximal element say M. We ~~claim~~ claim that M is a maximal ideal in R. Suppose if possible $M \subsetneq N$ where N is an ideal in R

If $N \neq R$ then $N \in S$ (By definition of S) and so M in not a maximal element of S, a contradiction. Hence $N = R$ and thus M in a maximal ideal in R as required.

4(b). Let $f : M \longrightarrow M/N$ be the natural epimorphism i.e. $f(m) = m + N$; $m \in M$. Let X be be an R-submodule of M/N. Define:

$$U = \{x \in M \mid f(x) \in X\}$$

We show, now, that U in an R-submodule of M. U in non-empty as $0 \in M$ and $f(0) \in X$. Suppose now that $x, y \in U$ and $r \in R$ then $f(x-y) = f(x) - f(y) \in X$ and $f(rx) = r f(x) \in X$ and $f(xr) = f(x) r \in X$ which shows that U in a left as well as right module. Also $N \subseteq U$ as $\forall\, x \in N$ $f(x) = x + N = \bar{0} \in X$.

Thus N in an R-submodule of U. Also if $x \in X$ then $\exists$ $y \in M$ such that $f(y) = x$ as f is an on to homomorphism. So by definition of U $y \in U$. Thus $X \subseteq f(U)$. However by definition of U $f(U) \subseteq X$ so we have $X = f(U)$ But also $f(U) = U/N$. Hence $X = U/N$, $N \subseteq U$.

5. An R-module M is said to be a free module if M has a basis.

Suppose if possible a finitely generated module M over a commutative ring R has two bases say B_1 and B_2 with number of elements m and n respectively and $m \neq n$. Since we know that if a module M over a ring R has a basis with n number of elements then $M \cong R^n$ we get in our case that $M \cong R^m$ and $M \cong R^n$. But then $R^m \cong R^n$.

Let $\phi : R^m \longrightarrow R^n$ be an isomorphism and suppose $m < n$. Let $\phi^{-1} = \psi$ and $\{e_1 \text{ ---- } e_m\}$ be an ordered basis of R^m while $\{f_1\ f_2 \text{ ---- } f_n\}$ be an ordered basis of R^n. Let

$$\phi(e_i) = a_{1i} f_1 + \text{---} + a_{ni} f_n \quad 1 \leq i \leq m$$

& $$\psi(f_j) = b_{1j} e_1 + \text{---} + b_{mj} f_m \quad 1 \leq j \leq n.$$

Let $A = [a_{ji}]_{n \times m}$ and $B = [b_{kj}]_{m \times n}$ be the corresponding matrices. Then

$$\psi\phi(e_i) = \sum_{k=1}^{m} \sum_{j=1}^{n} b_{kj}\, a_{ji}\, e_k \qquad 1 \leq i \leq m.$$

As e_i's are linearly independent and $\psi = \phi^{-1}$ we have $\sum_{j=1}^{n} b_{kj} a_{ji} = \delta_{ki}$.

So that

$BA = I_m$ where I_m is the $m \times m$ identity matrix. Similarly $AB = I_n$. Let $A' = [A \; 0]$ and $B' = \begin{bmatrix} B \\ 0 \end{bmatrix}$ be $n \times n$ augmented matrices ($\because m < n$ by assumption) where each of the 0 blocks is a matrix of appropriate size. Then $A'B' = I_n$ where

$$B'A' = \begin{bmatrix} I_m & 0 \\ 0 & 0 \end{bmatrix}.$$

So $\det(A'B') = \det(B'A')$

$\Rightarrow \quad 1 = 0$ a contradiction.

[As A' and B' are matrices over a commutative ring it follows that $\det(A'B') = \det(B'A')$]

If we now assume $m > n$ we get a contradiction in a similar way. Thus $m \neq n$ gives us a contradiction & so $m = n$. This proves the result.

6 (a) First let $f(x)$ be reducible so that $f(x) = f_1(x) f_2(x)$ where $f_1(x)$ and $f_2(x)$ are nonconstant polynomials each of which has degree less than 3. But this implies that either $f_1(x)$ or $f_2(x)$ must be of degree 1. Let $f_1(x) = ax + b$ with $a \neq 0$. Then $f_1(-ba^{-1}) = 0$ and hence $f(-ba^{-1}) = 0$ which proves that $-ba^{-1}$ is a root of $f(x)$.

Now suppose $f(x)$ has a root say α in F. Then $f(x) = (x-\alpha)\,q(x) + r$ where $r \in F$ (By division algorithm) Then $0 = f(\alpha) = r$ so $f(x) = (x-\alpha)\,q(x)$. As $f(x)$ has degree > 1 $q(x) \notin F$ so $f(x)$ in reducible over F.

(b) (i) Let $p(x) = p_1(x)\,p_2(x)$ (if possible) so that deg $p_1(x)$, deg $p_2(x)$ in less than deg $p(x)$. Then $0 = p(u) = p_1(u).\,p_2(u)$. This gives $p_1(u) = 0$ or $p_2(u) = 0$ i.e. u satisfies a polynomial of degree less than that of $p(x)$, a contradiction. Hence $p(x)$ is inreducible over F.

(ii) By division algorithm $g(x) = p(x)\,q(x) + r(x)$ where $r(x) = 0$ or degree of $r(x)$ $<$ degree of $p(x)$. This gives $g(u) = p(u)\,q(u) + r(u)$; i.e. $r(u) = 0$. Because $p(x)$ in of the least degree among the polynomials satisfied by u, $r(x)$ must be 0. Thus $p(x) \mid g(x)$.

(iii) Let $g(x)$ be another monic polynomial of least degree such that $g(u) = 0$. Then by (ii) $p(x) \mid g(x)$ and also $g(x) \mid p(x)$, as both are monic this gives $p(x) = g(x)$.

P. T. O.

7 (a). In order to prove ~~the~~ ~~theorem~~ we require two results which are given below :

Result 1. As given in Que 1 (viii).

Result 2. If E is an algebraic extension of a field F and $\sigma : F \to L$ is an embedding of F into an algebraically closed field L then σ can be extended to an embedding $\eta : E \to L$.

We now prove ~~the~~ theorem: Let $\bar{K}$ be an algebraic closure of K. Then $\bar{K}$ is algebraic over K and as K is algebraic over F it follows that $\bar{K}$ is algebraic over F. Hence $\bar{K} = \bar{F}$. By result 1 above we get that E is an algebraic extension of F so applying result 2 to the identity mapping $\lambda : F \to F$ $\exists$ extension of λ ~~given~~ denoted by $\sigma : \bar{E} \to \bar{K}$, which is also an embedding. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$. Set $f^{\sigma}(x) = \sigma(a_0) + \sigma(a_1) x + \cdots + \sigma(a_n) x^n$. As σ is identity on F $f^{\sigma}(x) = f(x)$. However we have a factorization $f(x) = c(x-\alpha_1) \cdots (x-\alpha_n)$ with $\alpha_i \in E$ $1 \le i \le n$ $c \in F$ of $f(x)$ in E so $f(x) = f^{\sigma}(x)$ and $c \in F$ gives

$$f(x) = c(x - \sigma(\alpha_1)) \cdots (x - \sigma(\alpha_n))$$

a unique factorization of $f(x)$ in $\bar{K}[x]$. But since $f(x)$ already has a unique factorization

given by $f(x) = c(x-\beta_1) \cdots (x-\beta_n)$ in $K[x]$ (i.e. $\beta_i \in K$ $1 \le i \le n$), it follows that the sets $\{\sigma(\alpha_1), \cdots \sigma(\alpha_n)\}$ and $\{\beta_1, \beta_2, \cdots \beta_n\}$ are equal. Thus

$$K = F(\beta_1, \cdots \beta_n) = F(\sigma(\alpha_1), \cdots \sigma(\alpha_n))$$

$$= \sigma(F(\alpha_1, \cdots, \alpha_n)) = \sigma(E)$$

Hence σ is an isomorphism of E onto K.

(b). To prove the result we require the following theorem (result):

If G is a group and $a, b \in G$ are such that $ab = ba$ and $o(a) = m$ while $o(b) = n$ then $\exists$ an element $c \in G$ such that $o(c) = $ l.c.m.(m,n)

Now let F^* denote the multiplicative group of nonzero elements of F. By a repeated application of above result $\exists$ an element $a \in F^*$ whose order l is the l.c.m of the orders of all the elements in F^*. Thus the order of each element of F^* divides l. Hence $\forall\ a \in F^*$ $a^l = 1$. Because the polynomial $x^l - 1$ has at most l roots in F, it follows that the number of elements in $F^* \le l$. However $1, \alpha, \cdots \alpha^{l-1}$ are all distinct and belong to F^*. Therefore F^* is generated by α.

Que 8. As E is a finite seperable extension of F, it follows that $E = F(\alpha)$ for some $\alpha \in E$. Let $p(x)$ be the minimal polynomial of α over F whose degree is (say) n.

Then $[E : F] = [F(\alpha) : F] = n$. ——— (1)

Also if E_0 is the fixed field of $G(E/F)$ it follows that $[E : E_0] = |G(E/F)|$ ——— (2)

[∵ We know that if H is a finite subgroup of the group of automorphisms of a field E, then $[E : E_H] = |H|$.]

(i)⇒(ii) By the result "If $\sigma : F \to L$ be an embedding of F into an algebraically closed field L and $E = F(\alpha)$ is an algebraic extension of F then σ can be extended to an embedding $\eta : E \to L$ and the number of such extensions is equal to the number of distinct roots of the minimal polynomial of α." the number of extensions of the inclusion mapping $: F \to \bar{F}$ to the embedding $: F(\alpha) \to \bar{F}$ is equal to the number of distinct roots of $p(x)$. Because E is a seperable extension of F, $\alpha \in E$ is a seperable element, so its minimal polynomial $p(x)$ over F must have distinct roots. So the number of distinct roots of $p(x)$ is equal to n.

In addition, because $E = F(\alpha)$ is a normal extension of F, any embedding $\sigma : F(\alpha) \to \bar{F}$ shall map $F(\alpha)$ onto $F(\alpha)$. Also any member

of $G(E/F)$ is an extension of the inclusion mapping $F \to \bar{F}$. Thus it follows that

$$|G(E/F)| = \text{number of distinct roots} = n \quad \text{---} \quad (3)$$

From (1) to (3) we get

$$[E:F] = n = |G(E/F)| = [E:E_0]$$

Hence $[E_0:F] = 1$ so $E_0 = F$ as desired. This proves (i) $\Rightarrow$ (ii).

(ii) $\Rightarrow$ (i) As seen earlier $E = F(\alpha)$ for some $\alpha \in E$. Let $G(E/F) = \{\sigma_1 = \text{identity}, \sigma_2, \ldots, \sigma_n\}$. Consider the polynomial $f(x) = (x-\sigma_1(\alpha))(x-\sigma_2(\alpha))\cdots(x-\sigma_n(\alpha))$. Now each $\sigma_i \in G(E/F)$ induces a natural homomorphism

$$\sigma_i^* : E[x] \to E[x] \text{ where } \sigma_i^*(a_0 + a_1 x + \cdots + a_m x^m)$$

$$= \sigma_i(a_0) + \sigma_i(a_1)x + \cdots + \sigma_i(a_m)x^m. \text{ So}$$

$$\sigma_i^*(f(x)) = (x-(\sigma_i\sigma_1)(\alpha))(x-(\sigma_i\sigma_2)(\alpha))\cdots(x-(\sigma_i\sigma_n)(\alpha))$$

But since $\sigma_i\sigma_1, \sigma_i\sigma_2, \ldots, \sigma_i\sigma_n$ are distinct members of $G(E/F)$ these F-automorphisms are only a permutation of $\sigma_1, \sigma_2, \ldots, \sigma_n$. Hence, $\sigma_i^*(f(x)) = f(x)$ $1 \le i \le n$. Now by expanding $f(x)$ we have $f(x) = x^n - c_1 x^{n-1} + c_2 x^{n-2} + \cdots + (-1)^n c_n$ with $c_i \in E$. Therefore $\sigma_i^*(f(x)) = f(x)$ implies that $\sigma_i(c_j) = c_j$ for $1 \le i \le n$ $1 \le j \le n$. This gives that c_j's are in the fixed field of $G(E/F)$. So by hypothesis $c_j \in F$, $1 \le j \le n$.

Hence, $f(x) \in F[x]$. Also, all the roots of $f(x)$ lie in E. Because $E = F(\alpha)$ and α is one of the roots of $f(x)$, E is a splitting field of ~~[illegible]~~ $f(x) \in F[x]$. This proves (ii) $\Rightarrow$ (i).

(ii) $\Rightarrow$ (iii) We know that "If E is a finite seperable extension of a field F and if $H \leq G(E/F)$, then $G(E/E_H) = H$ and $[E : E_H] = |G(E/E_H)|$"

(ii) $\Rightarrow$ (iii) is clear.

(iii) $\Rightarrow$ (ii). By equation (2) $[E : E_0] = |G(E/F)|$

Thus by (iii) we get $[E : E_0] = [E : F]$ Hence $E_0 = F$ and so (iii) $\Rightarrow$ (ii) is proved.

Hence the result.