AS - 2217

M.A / M.Sc. (First Sem.) Examn. 2013

Advance Abstract Algebra - I

Solution (Suggested)

1. (i) For xG' and yG' in G/G' we have

$$xG'yG'(xG')^{-1}(yG')^{-1} = xyx^{-1}y^{-1}G' = G'$$

as $xyx^{-1}y^{-1} \in G'$, so $xG'yG' = yG'xG'$

i.e. G/G' is abelian

(ii) A group G is said to be simple if G has no proper normal subgroup.

(iii) $\{e\} \subseteq \{e, \sigma^2\} \subseteq \{e, \sigma, \sigma^2, \sigma^3\} \subseteq D_4$ is a composition series for the octic group D_4 where $\sigma = (1,2,3,4)$

(iv) If A is any ideal in a ring R then $\forall\ a \in A$ $a = a + 0 \in A + A$ so $A \subseteq A + A$.

Also $\forall\ a + b \in A + A$ as A is an additive abelian group we have $a + b \in A$ so $A + A \subseteq A$

Thus $A + A = A$.

(v) Let

$$\cdots \xrightarrow{f_{n-1}} M_{n-1} \xrightarrow{f_n} M_n \xrightarrow{f_{n+1}} M_{n+1} \rightarrow \cdots$$

be a sequence of R-modules and R-homomorphisms then it is said to be exact if $\operatorname{Im} f_n = \operatorname{Ker} f_{n+1}$ $\forall\ n \in \mathbb{Z}$.

(vi) Student may give a suitable example.

(vii) Let E be a finite extension of a field F.

Let $u \in E$ and $[E:F] = n$. Since the set $\{1, u, u^2, \ldots, u^{n-1}, u^n\}$ is linearly dependent $\exists$ $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$ not all zero in F such that $a_0 + a_1 u + \ldots + a_n u^n = 0$. Thus u is algebraic over F. Since $u \in E$ was arbitrary it follows that E is algebraic.

(viii) Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial over a field F. The derivative of $f(x)$ is denoted by $f'(x)$ and is defined as $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$.

(ix) As we know that any irreducible polynomial $f(x)$ over a field of characteristic zero has simple roots, it follows from the definition of simple root and seperable polynomial that the result is true. [A good and complete answer includes the definition of a simple root and that of seperable polynomial.]

(X) Let $G = G(\mathbb{C}/\mathbb{R})$. For $a+ib \in \mathbb{C}$, $a, b \in \mathbb{R}$ and $\sigma \in G$ we have $\sigma(a+ib) = \sigma(a) + \sigma(i)\sigma(b)$ $= a + \sigma(i) b$. Also $i^2 = -1$ imply that $(\sigma(i))^2 = -1$ and so $\sigma(i) = \pm i$. Thus $\sigma(a+ib) = a \pm ib$ That is there are only two possible automorphisms of $\mathbb{C}$.

2(a) This is an equivalent statement of Jordan-Hölder theorem whose proof can be found in any of the text books.

(b) The proof of this statement can be given using mathematical induction. The induction begins with showing that $H \times K$ is nilpotent if H and K are nilpotent. This part also needs mathematical induction to show that $Z_m(H \times K) = Z_m(H) \times Z_m(K)$. Thus students need to show first that $Z(H \times K) = Z(H) \times Z(K)$. Then the proof of entire theorem will follow.

3(a) Let $ab \in M$ (a prime ideal). For $na + ar$ and $mb + bs$ in $\langle a \rangle$ and $\langle b \rangle$ respectively we find that $(na + ar)(mb + bs)$ in in M so $\langle a \rangle \langle b \rangle \subseteq M$. So by definition $\langle a \rangle \subseteq M$ or $\langle b \rangle \subseteq M$ i.e. $a \in M$ or $b \in M$. Conversely if $ab \in M \Rightarrow a \in M$ or $b \in M$ be true and A, B be two ideals so such that $AB \subseteq M$. Let $A \nsubseteq M$ so that $\exists\ a \in A$ such that $a \notin M$. Then $AB \subseteq M \Rightarrow aB \subseteq M$ so ~~$ab \in M$~~ $ab \in M \ \forall\ b \in B$ but then by our hypothesis $b \in M \ \forall\ b \in B$ i.e. $B \subseteq M$.

(b) A left ideal A in a ring R is called nilpotent if $A^n = \{0\}$ for some positive integer n. (1 Mark)
For second part of the question let $A^m = \{0\}$ and $B^n = \{0\}$ and $K = \max(m, n)$. Now students

may calculate and show that $(A+B)^{2k} = \{0\}$ and so the result is true. [Student may find another such integer]. (4 Marks)

4 (a) Consider the canonical map $f: M \longrightarrow M/N$ and X as a submodule of M/N. Let $U = \{x \in M \mid f(x) \in X\}$. Now students may show that U is a submodule of M containing N. Then they may show that $X = f(U) = U/N$ and thus complete the proof.

(b) Let, if possible two bases of M (a finitely generated module over a commutative ring R with $1 \neq 0$) have different number of elements say m and n. Then $M \cong R^m$ and also $M \cong R^n$. Thus $R^m \cong R^n$. Now, by defining a suitable isomorphism $\phi: R^m \longrightarrow R^n$ student may generate a contradiction for both cases $m > n$ and $n > m$. Hence, it is concluded that m and n must be equal.

5 (a) Let $f(x) \in \mathbb{Z}(x)$ be given by $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ and a prime p such that $p^2 \nmid a_0$, $p \mid a_0$, $p \mid a_1, \cdots, p \mid a_{n-1}$ and $p \nmid a_n$ then $f(x)$ is irreducible over $\mathbb{Q}$. (1 Marks)

Proof: (By contradiction). Student may let $a_0 = b_0 c_0$ and use the divisibility by p (prime) and the hypothesis $p \nmid a_n$ to generate an ~~contradiction~~.

absurdity. Therefore by the result "if $f(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$ then it is also reducible over $\mathbb{Z}$ may conclude the result.

5(b) The students are supposed to first construct an extension K (say 1) of F in which every polynomial in $F[x]$ of degree ≥ 1 has a root. This can be done by induction to generate a chain of fields $K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots$ and by taking $K = \bigcup_{n=1}^{\infty} K_n$. The students are supposed to mention the results used by them for the construction of K.

Now every polynomial in $K[x]$ has its coefficients in some subfield K_n and hence a root in $K_{n+1} \supseteq K_n$. This will then complete the proof.

6(a) Let $\bar{F}$ be the algebraic closure of F and $\alpha, \beta \in \bar{F}$ be two roots of $f(x)$ with multiplicity k and k' respectively ($\alpha \neq \beta$ clearly). Students need to show that $F[x]/\langle f(x) \rangle \cong F(\alpha)$ and also $F[x]/\langle f(x) \rangle \cong F(\beta)$ so that $F(\alpha) \cong F(\beta)$. Then they may conclude that if σ is the isomorphism then $\sigma(\alpha) = \beta$. They may now find the

ring homomorphism $\eta : \bar{F}[x] \longrightarrow \bar{F}[x]$ indeced by the extension $\sigma^* : \bar{F} \longrightarrow \overline{F(\beta)} = \bar{F}$, which is given by $\eta \cdot (a_0 + a_1 x + \cdots + a_n x^n) = \sigma^*(a_0) + \sigma^*(a_1) x + \cdots + \sigma^*(a_n) x^n$

Now $\eta(f(x)) = f(x)$. Since $\eta(x-\alpha)^{k'} = (x-\beta)^{k'}$ $(x-\beta)^{k'} \mid f(x)$ $\therefore$ $k' \geq k$. By reversing the roles of α and β, it can be similarly shown that $k \geq k'$ Hence $k = k'$. This completes the proof.

6(b) (i) $\Rightarrow$ (ii) Let $f(x) \in F[x]$ be the minimal polynomial of α over F. Let K be a subfield of E containing F, and let $g(x)$ be the minimal polynomial of α over K. Then since $g(x) \in K[x]$ & $f(\alpha) = 0$ $g(x) \mid f(x)$. If k' is the subfield of k containing F and the coefficients of the polynomial $g(x)$ then $g(x) \in k'[x]$, being irreducible over K, is also irreducible over k'. Also $F(\alpha) = E \Rightarrow K(\alpha) = k'(\alpha) = E$. Thus $[E:K]$ = degree of $g(x) = [E:k']$. Hence $K = k'$

Consider the mapping σ from the family of intermediate fields to the divisors of $f(x)$ in $E[x]$ given by $\sigma(K) = g(x)$, the minimal polynomial of α over k. Then the students may conclude that σ is 1-1. Because there are only finitely many divisors of $f(x)$ the family of intermediate fields between F and E is also finite,

(ii) $\Rightarrow$ (i) If F is a finite field E is also finite and the result follows from the theorem "The multiplicative group of non-zero elements of a finite field is cyclic". For the case when F is infinite the student need to first show that for $\alpha, \beta \in E$, $\exists\ \gamma \in E$ such that $F(\alpha, \beta) = F(\gamma)$.

Choose, now, $u \in E$ such that $[F(u) : F]$ is as large as possible. Then show $E = F(u)$ and this will prove (ii) $\Rightarrow$ (i)

(Marks Dist. 5+5)

7. Students may only state Dedekind lemma first. Using the solvability conditions for m homogeneous linear equations with n variables, where $H = \{e, = g_1, g_2, \cdots g_n\}$ and $[E : E_H] = m$ the students are supposed to generate contradiction for the case $n > m$ and then for the case $m > n$. Hence they may conclude $m = n$. Details of caclulations may be given by the student as he/she deems fit.

P.T.O

Proof : The student may select a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{C}[x]$ and let $g(x) = (x^2+1)\, f(x)\, \overline{f(x)}$ where $\overline{f(x)}$ is obtained from $f(x)$ by replacing its coefficients a_i by complex conjugate of a_i i.e. $\bar{a}_i$. Then they may show that $\nexists$ a subfield K of E containing $\mathbb{C}$ such that $[K : \mathbb{C}] = 2$.

Let $G = G(E/\mathbb{R})$ be the Galois group of $g(x)$ over $\mathbb{R}$ and $|G| = 2^m q$ where q is an odd integers. Using the H (2-sylow subgroup of G and L to be its corresponding field the student may observe that

$$E \longleftrightarrow \{e\}$$
$$L \longleftrightarrow H$$
$$\mathbb{C} \longleftrightarrow G(E/\mathbb{C})$$
$$\mathbb{R} \longleftrightarrow G(E/\mathbb{R})$$

Then $[E : L] = 2^m$ so $[L : R] = q$. Then student may not conclude that $q = 1$ & so that $[E : \mathbb{C}] = 2^{m-1}$ Assuming $m > 1$ the student is no supposed to generate a contradiction & so & conclde that $m = 1$. Then $[E : \mathbb{R}] = 2$ with $\mathbb{C} \subseteq E$ which means $E = \mathbb{C}$ as desired / claimed.

Ramadin