# QUALIFY EXAMINATION ANSWERS - ALGEBRA

## 1. Sem 2, 2000/2001

**Question 1.1.** *Let $G$ be a finite group with a unique maximal subgroup. Show that $G$ is cyclic.*

*Proof.* Let $M$ be the maximal subgroup of $G$. For any $g \in G \setminus M$. $\langle g \rangle = G$. Since otherwise $\langle g \rangle$ should contained in the maximal subgroup $M$, a contradiction. □

**Question 1.2.** *Let $A$ be a subgroup of index $n$ of a finite group $G$ and let*

$$\{ g_1A, g_2A, \cdots, g_nA \}$$

*be a set of coset representatives of $G/A$. For each $g \in G$, define*

$$f_g : G/A \to G/A$$

*by $f_g(g_iA) = gg_iA$. Prove that $f_g$ is a bijection. Define $\chi : G \to S_n$ by*

$$\chi(g) = f_g$$

*Prove that $\chi$ is a group homomorphism. Determine the kernel of $\chi$.*

*Proof.* Since $f_g \circ f_{g^{-1}} = \mathrm{id}_{G/A}$, $f_{g^{-1}} \circ f_g = \mathrm{id}_{G/A}$. $f_g$ is bijection. It's easy to see that $\chi(gh)(g_iA) = f_{gh}(g_iA) = ghg_iA = f_g \circ f_h(g_iA) = (\chi(g)\chi(h))(g_iA)$. So $\chi$ is a group homomorphism.

$\chi_g = 1$ iff $f_g = \mathrm{id}_{G/A}$ iff $gg_iA = g_iA$ for all $g_i$. $g_i$ just representative element of $g_iA$. So it's equivalent to $ghA = hA$ for all $h \in G$. So $\mathrm{Ker}\chi = \{ \mathrm{g \in G \mid h^{-1}gh \in A \forall h \in G} \}$. □

**Question 1.3.** *Let $R$ be a commutative ring with identity and let $\chi : R \to F$ be a nontrivial ring homomorphism, where $F$ is an integral domain. Prove that kernel of $\chi$ is a prime ideal.*

*Proof.* $F$ is integral domain then $\mathrm{Im}\chi$ is integral domain by the definition. So $\mathrm{Ker}\chi$ is prime. (If $ab \in \mathrm{Ker}\chi$, $\mathrm{Ker}\chi = \mathrm{ab} + \mathrm{Ker}\chi = (\mathrm{a} + \mathrm{Ker}\chi)(\mathrm{b} + \mathrm{Ker}\chi)$. So $a + \mathrm{Ker}\chi = \mathrm{Ker}\chi$ or $b + \mathrm{Ker}\chi = \mathrm{Ker}\chi$ by definition of integral domain. So either $a$ or $b$ in $\mathrm{Ker}\chi$.) □

**Question 1.4.** *Let $V$ be a vector space of finite dimension over a field $F$. Suppose that $V$ is a integral domain. Prove that $V$ is a field.*

*Proof.* Note that all right ideal of $V$ is $F$ vector subspace of $V$ ($xf = x(1_V f) \in I$ for any right ideal $I$ of $V$ and $x \in I$, $f \in F$). Since $V$ is finite dimension, $V$ is right Artinian ring. So for any $0 \neq a \in V$, exists $k \in \mathbb{N}$, $b \in V$, s.t. $a^k = a^{k+1}b($ $(a) \supset (a^2) \supset (a^3) \cdots$ terminate). Since $V$ is integral domain, $ab = 1_V$. So $V$ is a field. □

**Question 1.5.** *Let $E/F$ be a field extension and let $a, b \in E$ be algebraic over $F$. Prove that every element in $F(a, b)$ is algebraic over $F$.*

*Proof.* For any $v \in F(a, b)$, $F(v) \subset F(a, b)$. So $[F(v) : F] \leq [F(a, b) : F] = [F(a)(b) : F(a)][F(a), F] \leq [F(b) : F][F(a) : F] < \infty$. Hence $v$ is algebraic over $F$. □

## 2. Sem 1, 2001/2002

**Question 2.1.** *(a) Show that if $R$ is a commutative ring with identity, then every maximal ideal of $R$ is a prime ideal.*

*(b) Show that if $R$ is a Principal Ideal Domain, then every Prime ideal of $R$ is a maximal ideal.*

*(c) Give an example of a ring $R$ which has a prime ideal that is not maximal.*

*Proof.* (a) $I$ maximal $\Leftrightarrow R/I$ is field, So $R/I$ is integral domain $\Leftrightarrow I$ prime.

(b) (i) $I = (p)$ is prime iff $p$ is prime ($p$ nonunit and $p|ab$ gives $p|a$ or $p|b$). It's easy since $p|a \Leftrightarrow a \in (p)$.

(ii) $p$ is prime the $p$ is irreducible($r$ nonunit and $r = ab$ gives $a$ or $b$ is unit). If $p = ab$, then $p|ab$. WLOG, suppose that $p|a$ then $a = ps$. So $p = psb$, then $1 = sb$ since $R$ is integral domain. So $b$ is unit.

(iii) $r$ is irreducible iff $(r)$ is maximal in the set of all proper principle ideals. If $r$ is irreducible, $(r) \subset (s)$. Then $r = sb$. If $s$ is unit, $(s) = R$, if $b$ is unit, $s = rb^{-1}$, i.e. $(s) \subset (r)$. So $(r)$ is maximal in all proper principle ideals. If $(r)$ is maximal in all proper principle ideals, $r = ab$, $(r) \subset (a)$. Then if $(a) = R$, $a$ is unit. If $(a) = (r)$, $a = rs$. So $r = rsb$, so $sb = 1$ i.e. $b$ is unit.

In the PID, every ideal is principle, so if $I$ is prime, $I$ is maximal.

(c) See Question 6.1

□

**Question 2.2.** *(a) Let $G$ and $H$ be finite groups with relatively prime orders. Let $\theta \colon G \to H$ be a group homomorphism. What can conclude about $\theta$ why?*

*(b) Let $H$ be a subgroup of a group $G$ with index 2. Prove that $H \lhd G$.*

*(c) Give an example to show that $H$ may not be a normal subgroup of $G$ if $[G : H] = 3$.*

*Proof.* (a) $\theta$ is trivial. $\mathrm{Im}(\theta)$ is a subgroup of $H$ so $|H|$ divided by $|\mathrm{Im}(\theta)|$. By $|\mathrm{Im}(\theta)| = \frac{|\mathrm{G}|}{|\mathrm{Ker}(\theta)|}$, $|G|$ divided by $|\mathrm{Im}(\theta)|$. Hence $\mathrm{Im}(\theta)$ is trivial, since $|G|$, $|H|$ coprime.

(b) Note that if $g \notin H$, $\{ H, gH \}$ forms a partition of $G$. Also $\{ H, Hg \}$ is a partition of $G$. So $gH = Hg$ since $H = H$. (Then $gHg^{-1} = H$). So $H$ is normal in $G$.

(c) Consider $S_3$ which is a non-abelian order 6 group. It has a order 2 subgroup $H$ and order 3 subgroup $N$. Then $H \cap N = 1$, $N \lhd G$. So $H$ can not be normal in $S_3$ otherwise $S_3 = H \times N$ is abelian.

□

**Question 2.3.** *If $L$ is a field extension of $K$ such that $[L : K] = p$ where $p$ is a prime number, show that $L = K(a)$ for every $a \in L$ that is not in $K$.*

*Proof.* Note that $[L : K] = [L : K(a)][K(a), K]$, $[K(a), K] > 1$ since $a \notin K$. So $[L : K(a)]$ i.e. $L = K(a)$. □

## 3. Sem 2, 2001/2002

**Question 3.1.** *Classify all groups of order $n$ up to isomorphism.*

*(a) $n$ is the square of a prime integer.*

*(b) $n = pq$ where $p, Q$ are primes with $p > q$ and $q$ does not divide $p - 1$.*

*Proof.* (a) Suppose that $|G| = p^2$. We claim that $G$ is abelian. First, the center $Z(G)$ of $G$ is non-trivial. Consider $G$ act on itself by conjugation. If $x \in Z(G)$, the orbit length is 1. Let $S = \{ x_i \}$ be the representative set of different orbit. Then we get the class equation:

$$|G| = |Z(G)| + \sum_i [G : H_i]$$

where $H_i = C_G(x_i)$. Note that $p|[G : H_i]$. So $|Z(G) \equiv 0 \pmod p$. $|Z(G)|$ non-trivial since $e \in Z(G)$.

If $Z(G) = G$, then $G$ is abelian. If $Z(G) < G$, then $|G/Z(G)| = p$ so $G/Z(G)$ is cyclic. Let $a \in G \setminus Z(G)$ and $a + Z(G)$ is a generator of $G/Z(G)$. Then every element in $G$ can written as $a^n g$ for $n \in \mathbb{Z}$, $g \in Z(G)$. So $a^{n_1} g_1 a^{n_2} g_2 = a^{n_1} a^{n_2} g_1 g_2 = a^{n_2} g_2 a^{n_1} g_1$. Hence $G$ is abelian.

So $G$ can be $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$ by the classification of finite abelian group.

(b) Consider Sylow $q$-subgroup $Q$. The number of Sylow $q$-subgroup is $kq + 1$ and divides $pq$. Since $q \nmid p - 1$, only 1 Sylow $q$-subgroup. So $Q$ is normal in $G$. On the other hand, there is a Sylow $p$-subgroup $P$. It is normal in $G$ since $p > q$, the number of Sylow $p$-group is 1. Clearly $p \cap Q = \langle e \rangle$, $PQ = G$. $P \cong \mathbb{Z}_p$ and $Q \cong \mathbb{Z}_q$. So $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_q = \mathbb{Z}_{pq}$.

□

## 4. Sem 1, 2002/2003

**Question 4.1.** *(a) Determine whether each of the following pairs of groups are isomorphic:*

*(i)* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_8$;
*(ii)* $\mathbb{Z}$, $\mathbb{Q}$;
*(iii)* $\mathbb{R}^*$, $\mathbb{C}^*$;
*(iv)* $\mathbb{R}^*$, $\mathbb{Q}^*$;
*(v)* $\mathbb{Q}$, $\mathbb{Q} \times \mathbb{Q}$.

*(b)* $\mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \}$ *is a Euclidean domain with respect to the Euclidean distance d, where*

$$d(a + bi) = a^2 + b^2$$

*(i) Find* $\alpha, \beta \in \mathbb{Z}[i]$ *such that*

$$1 - 5i = (1 + 2i)\alpha + \beta,$$

*where* $|\beta| < 5$.

*(ii) Decide, with reasons, which of the following elements are irreducible in* $\mathbb{Z}[i]$*:*

$$1 + i, 2 + 3i, 1 + 3i.$$

*Proof.* (a) (i) No. $\mathbb{Z}_8$ have order 8 element, but all element in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ at most order 2.

(ii) No. $\mathbb{Q}$ is divisible, say any $x \in \mathbb{Q}$, $n \in \mathbb{Z}$ exists $y \in bQ$ s.t. $ny = x$. But $\mathbb{Z}$ is not divisible.

(iii) No. $\mathbb{C}^*$ have any order $n$ subgroup say $\left\langle e^{2\pi i/n} \right\rangle$. But the only finite subgroup in $\mathbb{R}^*$ is $\{ \pm 1 \}$.

(iv) No. $\mathbb{R}^*$ and $\mathbb{Q}^*$ have different cardinal number.
(v) Consider $\mathbb{Q}$ and $\mathbb{Q}\times\mathbb{Q}$ as $\mathbb{Z}$-module, If $\mathbb{Q}$ isomorphism to $\mathbb{Q}\times\mathbb{Q}$ by homomorphism $\phi$. We have exact sequence:

$$0 \to \mathbb{Q} \xrightarrow{\phi} \mathbb{Q}\times\mathbb{Q} \to 0.$$

localization by tensor product with $\mathbb{Q}$. It gives a $\mathbb{Q}$-module( $\mathbb{Q}$-vector space) exact sequence:

$$0 \to \mathbb{Q} \xrightarrow{\phi\otimes \mathrm{id}_{\mathbb{Q}}} \mathbb{Q}\times\mathbb{Q} \to 0.$$

Since $\mathbb{Q}$ have IBN, $\mathbb{Q}$ can not isomorphism to $\mathbb{Q}\times\mathbb{Q}$.

(b) (i) $1-5i = (1+2i)(-2-1i)+1$.
(ii) $N(1+i)=2$, $N(2+3i)=13$ are prime, so they are irreducible. $N(1+3i)=10$, if it is reducible, i.e. $rs = 1+3i$, $N(r)=2$, $N(s)=5$. So $r=\pm1\pm i$. Then it's clearly that $(1+i)(2+i)=1+3i$.

**Question 4.2.** *(a) If $p$ is a prime number, show that the symmetric group $S_p$ has exactly $(p-2)!$ Sylow $p$-subgroups. Deduce that $(p-1)!+1$ is divisible by $p$.*
*(b) Prove that a ring wit a prime number of elements is either a field or a zero ring (i.e. a ring in which all products are zero).*

*Proof.* (a) Clearly by combination, $S_p$ has $p!/p=(p-1)!$ order $p$ elements. Different $p$-subgroups has different non-trivial element, and such element is order $p$. So $S_p$ has $(p-1)!/(p-1)=(p-2)!$ Sylow $p$-subgroup. Then $(p-2)!\equiv 1 \mod p$. Then $(p-1)!+1\equiv -1(p-2)!+1\equiv 0 \mod p$.
(b) Clearly the addtive group of $R$ is $\mathbb{Z}_p$. Let 0 and $e$ be the identity of addtive and multiplication respectively. Then if $0=e$, $R$ is zero ring. If $0\neq e$, $e$ is a generator of the addtive group. Then it determine the ring structure of $R$ by $xy=(ne)(se)=nse$ where $x=ne, y=se$ for $n,s\in\mathbb{Z}$. So $R$ is isomorphic to $\mathbb{Z}_p$. □

## 5. Sem 2, 2002/2003

**Question 5.1.** *Let $G$ be a group of order $2p$, where $p$ is an odd prime. Prove that either $G$ is a cyclic, or $G=\{1,a,a^2,\cdots,a^{p-1},b,ab,a^2b,\cdots,a^{p-1}b\}$ where $a$ has order $p$, $b$ has order 2, and $ba=a^{-1}b$.*

*Proof.* See Question 8.2 □

**Question 5.2.** *Let $F$ be a finite field with $p^n$ elements. Prove that*
*(a) the multiplicative group $F^\times = F\setminus\{0\}$ is cyclic.*
*(b) $F$ contains a subfield with $p^m$ elements if and only if $m|n$.*

*Proof.* (a) It's the same as Question 9.5.
(b) Suppose that $K$ is a subfield of $F$ then $K^\times$ is a subgroup of $F^\times$. So $|K^\times|$ divides $F^\times$. As we know finite field with character $p$ is a extension field of $\mathbb{Z}_p$ So have $p^m$ elements. It's clearly that $p^m-1|p^n-1$ if and only if $m|n$.

On the other hand, if $m|n$, $p^m-1|p^n-1$. Let $a$ be a generator of $F^\times$, then consider

$$K=\{0\}\cup\langle a^{\frac{p^n-1}{p^m-1}}\rangle$$

Clearly $|K| = p^n$. We will prove that $K$ is a field. Consider the map

$$\begin{aligned} \phi_m \colon F &\to F \\ x &\mapsto x^{p^m} \end{aligned}$$

Note that $\phi$ is a field homomorphism since $(x+y)^{p^m} = x^{p^m} + y^{p^m}$.

It's also easy to see that every element $x$ in $K$ satisfy $\phi_m(x) = x$ (0 is trivial; it's true for other elements in $K$ since $|\langle a^{\frac{p^n-1}{p^m-1}}\rangle| = p^m - 1$.) But equation $x^{p^m} - x = 0$ have at most $p^m$ solutions. So $K$ is the set of all elements s.t. $\phi_k(x) = x$. So $K$ is a field since the set $\{ x \in F \mid \phi_k(x) = x \}$ form a field ($x+y, xy, x^{-1} \in K$ if $x, y \in K$).

□

## 6. Sem 1, 2003/2004

**Question 6.1.** *(a) Let $G$ be the additive group $\mathbb{Q}/\mathbb{Z}$. Show that any finite subgroup of $G$ is cyclic.*

*(b) For the ring $R = \mathbb{Z} \times \mathbb{Z}$, give an example for each of the following:*
  - *(i) a maximal ideal of $R$.*
  - *(ii) a prime ideal of $R$ that is not maximal.*

*Proof.* (a) Let $G$ be a finite subgroup of $G$. Let $a = \min\{ x \in [0,1) \mid \bar{x} \in G \}$. Then $G = \langle \bar{a} \rangle$. If not, there is $b \in G \setminus \langle \bar{a} \rangle$. It's easy to see that, we can find $\bar{b} = n\bar{a} + \bar{c}$, where $0 < c < a$. This contradicte to the choice of $a$.

(b) $p\mathbb{Z} \times \mathbb{Z}$ is a maximal idel of $R$ since $\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z} \cong \mathbb{Z}_p$ is a field. $0 \times \mathbb{Z}$ is prime but not maximal since $\mathbb{Z} \times \mathbb{Z}/0 \times \mathbb{Z} \cong \mathbb{Z}$ is a integral domain but not a field.

□

**Question 6.2.** *(a) Let $G$ be a finite group, and $H$ be a subgroup of index 2. Show that $x^2 \in H$ for any $x \in G$ and hence deduce that $H$ contains all elements of $G$ of odd order.*

*(b) Let $n > 3$ be an integer, and let $G$ be a subgroup of $S_n$. Assume that $G$ has an odd permutation. Show that $G$ has a normal subgroup of index 2.*

*(c) Let $A_4$ be the subgroup of even permutations in $S_4$. Show that $A_4$ has no subgroup of index 2.*

*Proof.* (a) Clearly $H$ is normal in $G$. $G/H$ is order 2. So $\pi(x^2) = \pi(x)^2 = e$ where $\pi$ is the canonical map. Then $x^2 \in H$. Suppose that $x$ have odd order, then $x^2$ is the generator of $< x >$ (A result of cyclic group, $\langle x^r \rangle = \langle x \rangle$ for any $(r, |x|) = 1$). Since $x^2 \in H$, $\langle x \rangle \subset H$. So $x \in H$.

(b) There is a natural sign map form $\operatorname{sgn} \colon S_n \to \{ \pm 1 \}$. restrict on $G$. If $G$ has odd permutation, $\operatorname{sgn}|_G$ is epimorphism. Then $\mathrm{Ker}\,\mathrm{sgn}_\mathrm{G}$ is a normal subgroup of $G$ with index 2.

(c) Note that $\langle (123) \rangle$, $\langle (124) \rangle$, $\langle (134) \rangle$ and $\langle (234) \rangle$ gives 4-distinct order 3 subgroup of $A_4$. If $A_4$ have index 2 subgroup $H$. then $|H| = 6$. But there already have 8 odd order element. They should be in $H$, a contradiction.

□

**Question 6.3.** *Recall that an element $p$ of an itegral domain $D$ is called irreducible if $p$ is a non-zero, non-unit and in any factorization $p = rs$ with $r, s \in D$, one of $r, s$ is a unit. Now let*

$$D = \mathbb{Z}[\sqrt{-7}] = \left\{\, a + b\sqrt{-7} \;\middle|\; a, b \in \mathbb{Z} \,\right\}.$$

(i) *By using the norm function $N(a + b\sqrt{-7}) = a^2 + 7b^2$, show that $2, 1 \pm \sqrt{-7}$ are irreducible elemens of $D$.*

(ii) *Is $2D$ a prime ideal? Is $D$ a unique factorization domain? Justify your answers.*

*Proof.* (i) Note that $N(rs) = N(r)N(s)$ for $r, s \in D$. Moreover $N(r) \in \mathbb{N}$ for $r \in D$. So we can determin all the units of $D$. In fact, if $u$ is a unit in $D$. $N(u)N(u^{-1}) = 1$. So $N(u) = 1$, i.e. $u = \pm 1$.

If $2 = rs$, then $N(r)N(s) = 4$. No solution of the equation $2 = a^2 + 7b^2$ for $a, b \in \mathbb{Z}$. So $N(r) = 1$ or $N(s) = 1$, i.e. $r$ or $s$ is unit.

If $1 \pm \sqrt{-7} = rs$, then $N(r)N(s) = 8$. By the same reason of above, $1 \pm \sqrt{-7}$ is irreducible.

(ii) Note that $(1 + \sqrt{-7})(1 - \sqrt{-7}) = 8 \in 2D$, but $1 \pm \sqrt{-7} \notin 2D$. So $2D$ is not prime.

Clearly $(1 + \sqrt{-7})(1 - \sqrt{-7}) = 8 = 2 * 2 * 2$. So $D$ is not a unique factorization domain.

□

**Question 6.4.** *(a) Let $R$ be a finite commutative ring with 1, such that $1 \neq 0$. Let $R^* = R \setminus \{\, 0 \,\}$ and put*

$$k = \prod_{r \in R^*} r,$$

*is a field.*

*(b) Let $p$ be a positive prime number such that $p = 4k + 1$ for some $k \in \mathbb{Z}$. Show that there exists $a \in \mathbb{Z}_p$ such that $a^2 = -1$ in $\mathbb{Z}_p$*

*Proof.* (a) Do not know!

(b) In fact $p = 4k + 1$ iff exists $a$ s.t. $a^2 = -1$ in $\mathbb{Z}_p$. Note that the multiplicty group $\mathbb{Z}_p^*$ is cyclic. $-1$ is the only order 2 element. If $p = 4k+1$ then $|\mathbb{Z}_p^*| = 4k$. So exists order 4 subgroup with generator $a$. Then $a^2 = -1$ since it is order 2.

On the other hand if exists $a^2 = -1$. Then there is a order 4 subgroup in $\mathbb{Z}_p^*$. So 4 divides $|\mathbb{Z}_p^*|$. Hence $p = 4k + 1$.

**Question 6.5.** *Show that each of the following polynomials is irreducible over $\mathbb{Q}$: you may want to consider reduction modulo a prime number.*

## 7. Sem 2, 2003/2004

**Question 7.1.** *Show that if $a$ and $b$ are elements in a group $G$, then $ab$ and $ba$ have the same order.*

*Proof.* Suppose $o(ba)$ is finite. Note that $(ab)^n = a(ba)^n a^{-1}$. If $n = o(ab)$, $(ab)^n = 1$. So $o(ab) | o(ba)$. In the same way $o(ba) | o(ab)$. It's also easy to see that $ab$ and $ba$ should both have finite order. □

**Question 7.2.** *(a) Let $H$ and $K$ be subgroups of a group $G$ with $H$ normal in $G$. Show that*

$$HK := \{ hk : h \in H, k \in K \}$$

*is a subgroup of $G$ and show that $H$ is normal in $HK$.*

*(b) Show that $(H \cap K)$ is normal in $K$ and that*

$$K/(H \cap K) \cong HK/H$$

*(c) Show that if $H$ is a normal subgroup of $G$ such that*

$$gcd(|H|, [G : H]) = 1$$

*then $H$ is the unique subgroup of $G$ of order $|H|$.*

*Proof.* $(a)$,$(b)$ are trivial. If $K$ is a order $|H|$ subgroup of $G$. Let $n = |K/(H \cap K)|$, then $n$ divides $|H|$. We have $K/(H \cap K) \cong HK/H$. So $n = \frac{|G/H|}{[G/H:HK/H]}$. So $n$ divides $[G : H]$. Hence $n = 1$. $H \cap K = K$ i.e. $K = H$ by $|K| = |H|$. □

**Question 7.3.** *(a) Show that if Ris a finite integral domain with a unit element, then $R$ is a field.*

*(b) Show that if $R$ is a finite commutative ring with a unit element, then every prime ideal of $R$ is a maximal ideal*

*Proof.* (a) $R$ is finite, so $R$ is right Artinian ring. right Artinian integral domain is field. It's the same as Question 1.4.

(b) If $P$ is a prime ideal in $R$, $R/P$ is integral domain. Then $R/P$ is field since it is finite. So $P$ is maximal in $R$.

□

**Question 7.4.** *Let $R$ is a ring with a unit element, $1_R$, in which*

$$(ab)^2 = a^2b^2$$

*for all $a, b \in R$. Prove that $R$ must be commutative.*

*Proof.* (From sci.math.) $((a+1)b)^2 = (a+1)^2b^2$ gives $(ab)^2+ab^2+bab+b^2 = a^2b^2+2ab^2+b^2$. So $bab = ab^2$. Then $(b+1)a(b+1) = a(b+1)^2$ gives $bab+ba+ab+a = ab^2+2ab+a$. Hence $ba = ab$. So $R$ commutative. □

**Question 7.5.** *(a) Let $K$ be a finite field of $p$ element, where $p$ is a prime. Let $\gcd(n, p) = 1$ and $F$ be the splitting field of $x^n - 1_K$ over $K$. Show that if $(F : K) = f$ then the $n$ divides $p^f - 1$.*

*(b) Show that $f$ is the smallest integer $m$ for which $p^m - 1$ is divisible by $n$.*

*Proof.* (a) It's clearly that $K \cong \mathbb{Z}_p$ by the uniqueness field of $p$ elements. Let $g(x) = x^n - 1 \in K[x]$. Since $\gcd(n, p) = 1$, there exists $k$ such that $kn = 1$. So $-g + kxg' = -x^n + 1 + knx^n = 1$, i.e. $g$, $g'$ coprime. So $f$ is separable in $F$. It's easy to see that the set $S$ consists all solutions of $x^n - 1$ form a multiplication subgroup of $F^\times$. Hence $n = |S|$ divides $p^f - 1$.

(b) Clearly $F$ is a finite extenstion of $K$. So $F$ is finite field of charactor $p$. Then $F$ has $p^s$ elements. If $s$ not the smallest integer $m$ for which $q^m - 1$ is divisible by $n$. Then consider $x^{q^m} - 1$ which is

## 8. Sem 1, 2004/2005

### 8.1. Ring Theory.

**Question 8.1.** *Let $R = M_n(\mathbb{R})$ be the ring of all $n \times n$ matrices over the real numbers. Find all the ideals of $R$. Justify your answers.*

*Proof.* $R$ is simple ring, so the all ideals of $R$ are 0 and itself. To prove $R$ is simple $\square$

### 8.2. Group Theory.

**Question 8.2.** *Let $p$ be a prime. Find all he groups (up to isomorphism) of order $2p$. Justify your answers.*

*Proof.* If $p = 2$, then it's order 4 group and is abelian. See Question 3.1 (a). Then $G$ can be $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$.

If $p > 2$, then consider the Sylow $p$-subgroup $P$. Clearly it's a cyclic group and suppose that it's generator is $a$. $P$ is normal in $G$ since it's the only order $p$ subgroup of $G$. Let $Q = \langle b \rangle$ be a Sylow 2-subgroup of $G$. Consider $Q$ act on $P$ by conjugation. Then $bab^{-1} = a^k$ and $a^k$ is a generator of $P$. Moreover $a = b(bab^{-1})b^{-1} = a^{k^2}$ So $k = \pm 1 \pmod p$. If $k = 1$, $G$ is abelian. Then $G$ isomorphic to $\mathbb{Z}_{2p}$. (Also see the proof of Question 3.1 (a).) If $k = 1$, then $G$ is non-abelian and isomorphic to the dihedral group $D_p$. $\square$

**Question 8.3.** *Let $p$ be a prime and let $G$ be a group of $p^3$ elements. Suppose that $G$ is not abelian. Prove that $Z(G)$ is cyclic of order $p$.*

*Proof.* In the proof of Question 3.1 (a) we see that $Z(G)$ is non-trivial. Then $|Z(G)| = p$ or $p^2$ since $G$ is not abelian. But if $|Z(G) = p^2$, $G/Z(G)$ is a cyclic group of order $p$. Also in the proof of Question 3.1 (a) we know that $G$ should be abelian, a contradiction. So $Z(G)$ is cyclic of order $p$. $\square$

### 8.3. Field Theory.

**Question 8.4.** *Let $\sigma$ be a field automorphism from $\mathbb{R}$ to $\mathbb{R}$. Prove that $\sigma(x) = x$ for all $x \in \mathbb{R}$.*

*Proof.* First $\sigma$ preserves rational number $\mathbb{Q}$. Note that $\sigma(1) = 1$. So $\sigma(x) = x$ for all $x\imath\mathbb{Z}$. Then there are equal in it's fractional field $\mathbb{Q}$ by the universal property of fractional field. ($\sigma_{\mathbb{Z}} = \mathrm{id}_{\mathbb{Z}}$ clearly can be extended uniquely to a homomorphism $\sigma_{\mathbb{Q}}$ on $\mathbb{Q}$ s.t. $\sigma_{\mathbb{Q}} \circ i = \sigma_{\mathbb{Z}}$ where $i$ is the natrual inclusion map from $\mathbb{Z}$ into $\mathbb{Q}$. Clearly $\mathrm{id}_{\mathbb{Q}}$ is a map satisfying this property. Hence $\sigma_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$.)

Next not that $\sigma$ preserves the "order" of $\mathbb{R}$. Let $a > b$ iff $a - b \in \mathbb{R}^+$. If $x \in \mathbb{R}^+$, there is $y \in \mathbb{R}$, s.t. $y^2 = x$, then $\sigma(x) = \sigma(y^2) = \sigma(y)^2 \in \mathbb{R}^+$. So $\sigma(a) > \sigma(b)$ if $a > b$. Note that there is one-one corresponding between $x \in \mathbb{R}$ and the set $\{ q \in \mathbb{Q} \mid x > q \}$. Since $\sigma$ preserves rational number $\sigma$ preserves $\{ q \in \mathbb{Q} \mid x > q \}$. So $\sigma(x) = x$ for any $x \in \mathbb{R}$. $\square$

## 9. Sem 2, 2004/2005

### 9.1. **Ring Theory.**

**Question 9.1.** *Prove that every integral domain can be embedded in a field.*

*Proof.* Localization. □

**Question 9.2.** *Let $D$ be an integral domain and let $F = \{ x \in D \mid xd = 1 \text{ for some } d \in D \}$. Suppose that $D$ is a finite dimensional vector space over $F$. Prove that $D$ is a field.*

*Proof.* I don't think $F$ is a field. If $F$ is a field, it's the same as Question 1.4. □

### 9.2. **Group Theory.**

**Question 9.3.** *Let $G$ be a nonabelian finite group generated $x$ and $y$, where $o(x) = o(y) = 2$. Prove that $G$ isomorphic to a dihedral group.*

*Proof.* I think this Question is wrong order 4 group are abelian. I think $o(x)$ may be an odd prime number. □

**Question 9.4.** *Let $G$ be a group of order 56. Suppose that $G$ has 2 or more subgroups of order 7. Prove that $G$ has a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.*

*Proof.* By Sylow's theorem $G$ has 7 different Sylow 7-subgroups. So there is unique Sylow 2-subgroups containing all element of $G$ not in Sylow 7-subgroups. Let $P$ be a Sylow 7-subgroup. $Q$ be the unique Sylow 2-subgroup. If $Q$ has a order 4 element. Consider the set $S$ of all order 4 element. Let $P$ act on $S$ by conjugation. Then it gives a homomorphism from $P$ to $Aut_{|S|}$. Note that $|S| \leq 6$. So the action is trivial. Let $a$ be a order 4 element. So $H = P \langle a \rangle$ is a subgroup of $G$. More over $H$ is cyclic group of order 28. Clearly $H$ has order 2 so $H$ is normal in $G$. By Sylow's theorem $gPg^{-1}$ givs all Sylow 7-subgroup. But, $gPg^{-1} < H$ since $P < H$ and $H$ normal. So $gPg^{-1} = P$ for all $g$. This contradict to $G$ has 2 or more subgroups of order 7. So $Q$ has no order 4 element. Then $Q \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (first $Q$ is abelian since every element is order 2, then deduce by the classifcation of finite abelian group.). □

### 9.3. **Field Theory.**

**Question 9.5.** *Let $F$ be a finite field. Prove that $F - \{ 0 \}$ under multiplication is a cyclic group.*

*Proof.* It's well know that finite multiplication group of field is cyclic. Clearly $F - \{ 0 \}$ form a group under multiplication, then it is cyclic.

We can prove this result as following. Let $G$ be a finite multiplication subgroup of field $F$. Let the primary decomposition of $G$ be $\bigoplus_{i=1}^{n} G_{p_i}$, where $n \in \mathbb{N}$ and $p_i$ are prime number and $G_{p_i} = \oplus_{j=1}^{n_i} \mathbb{Z}_{p^{\alpha_j}}$, $n_i \in bN$, $alpha_{i,j} \geq 1$. We claim that $n_i = 1$, i.e. $G_{p_i} = \mathbb{Z}_{p^{\alpha_i}}$, then $G$ is cyclic ($\mathbb{Z}_a \oplus \mathbb{Z}_b = \mathbb{Z}_{ab}$ if $\gcd(a, b) = 1$). If $n_i > 1$, for some $i$, $G$ has two distinct order $p_i$ subgroup, then there are more than $p_i$ element is $G$ satisfying the equation $x^{p_i} - 1 = 0$. Since $F$ is a field, there at most $p_i$ different solution of the equation, a contradiction. □

**Question 9.6.** *Prove that $\sqrt{2} + \sqrt{3} + \sqrt{5} + \sqrt{7}$ is irrational.*

*Proof.* Note that $Q(\sqrt{2},\sqrt{3},\sqrt{5})(\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7}) = Q(\sqrt{2},\sqrt{3},\sqrt{5})(\sqrt{7})$. $[Q(\sqrt{2},\sqrt{3},\sqrt{5})(\sqrt{7}) : Q] = 16$. $[Q(\sqrt{2},\sqrt{3},\sqrt{5}) : Q] = 8$.

So $\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7}$ is irrational since if it is rational, $Q(\sqrt{2},\sqrt{3},\sqrt{5}) = Q(\sqrt{2},\sqrt{3},\sqrt{5})(\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7})$. □

## 10. Sem 1, 2005/2006

**Question 10.1.** *Classify all groups of order 8 up to isomorphism.*

*Proof.* If $G$ is abelian, then $G$ can be $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$, $\mathbb{Z}_4\times\mathbb{Z}_2$ and $\mathbb{Z}_8$. If $G$ is non-abelian, $G$ has a order. □

**Question 10.2.** *Let $R$ be a ring with 1. A simple left $R$-module $M$ is a left $R$-module such that $|M| > 1$ and if $N$ is a submodule of $M$, then either $N = M$ or $N = \{0\}$.*

*(a) Let $I$ be a maximal left ideal of $R$. Show that $R/I$ is a simple $R$-module.*
*(b) Let $m$ be a nonzero element of a simple left $R$-module $M$. Prove that:*
- *(i) $Rm := \{ rm \mid r \in R \}$ equals $M$;*
- *(ii) $Ann(m) := \{ r \in R \mid rm = 0 \}$ is a maximal left ideal of $R$;*
- *(iii) $R/Ann(m) \cong M$ as left $R$-module.*

*Proof.* See uestion 12.1]. □

## 11. Sem 2, 2005/2006

**Question 11.1.** *(a) Prove that a group of order 12 either has a normal subgroup of order 3, or is isomorphic to $A_4$, the alternating group on 4 letters.*
*(b) Show that any simple group acting on a set of $n$ elements is isomorphic to a subgroup of $A_n$, the alternating group on $n$ letters.*

*Proof.* (a) If $|G| = 12$ and has no order 3 normal subgroup. Then the number of it's Sylow 3-subgroups is 4. Let $G$ act on the set of Sylow 3-subgroups $S$ by conjugation. It gives a homomorphism $\phi\colon G \to S_4$. The same as Question 6.2 (c) $G$ has no order 6 subgroup. So $\mathrm{Im}\phi \subset \mathrm{A}_4$. Since $G$ act on $S$ transitively. $|\mathrm{Im}\phi| \geq |\mathrm{S}| = 4$. So $|\mathrm{Ker}\phi| \leq 3$. Since $G$ have no order 3 subgroup, $|\mathrm{Ker}\phi| \neq 3$. Since $A_4$ have no order 6 subgroup, $|\mathrm{Ker}\phi| \neq 2$. So $\phi$ is monomorphism, then isomorphism from $G$ to $A_4$.
(b) See Question 14.1

□

**Question 11.2.** *Let $R$ be a ring, not necessarily commutative and not necessarily containing the multiplicative identity. Prove that if $R[X]$ is a principal ideal domain, then $R$ is a field.*

*Proof.* First we can embed $R$ in $R[X]$. Since $R[X]$ is integral domain (commutative, no zero divisor), $R$ is integral domain. Consider the evaluation $\phi\colon R[X] \to R$ by $f \mapsto f(0)$. $\phi$ is sujective. Since $R$ is integral domain, $\mathrm{Ker}\phi$ is prime ideal in $R[X]$, then it is maximal ideal by Question 2.1 (b). So $R$ is a field. □

## 12. Sem 1, 2007/2008

**Question 12.1.** *Prove that a simple group of order* 60 *is isomorphic to* $A_5$.

*Proof.* Note that, if there is a action of $G$ on set $S$ with $|S| = n$, then there is a injective from $G$ to $A_n$. (See Question 11.1 (b)) Since $|G| = 60$, $|A_n| \geq |G|$ i.e. $n \geq 5$. $60 = 3 \times 4 \times 5$. Consider 2-Sylow group. There is two approachs.

(a) If there are two 2-Sylow subgroup $P$,$Q$ with non-trivial intersection. Clearly $H = P \cap Q$ is order 2. Choose $e \neq x \in H$. Then $P \cap Pq \subset C_G(x)$(order 4 group are all abelian), where $q \in Q \setminus H$. So $|C_G(x)| \geq 8$. Cearly $C_G(x) \neq G$, if so $C(G)$ is a non-trivial normal subgroup of $G$. So $|C_G(x)| \leq 12$, by looking the left action of $G$ on $G/C_G(x)$ ($[G : C_G(x)] \geq 5$). Now $|C_G(x)|$ divides 60 and $|P|$ divids $C_G(x)(P < C_G(x))$. So $|C_G(x)| = 12$. Hence it gives a isomorphism from $G$ to $A_5$ by looking the left action of $G$ on $G/C_G(x)$.

    If all 2-Sylow subgroup have no non-trivial intersection, fix a 2-Sylow subgroup $P$. Consider the normalizer $N_G(P)$. We will prove that $N_G(P) \neq P$. If so, the only possible is $|N_G(P)| = 12$, then $G \cong A_5$.

    Suppose that $N_G(P) = P$, then $|N_G(P)| = 4$. So there is fifteen differen 2-Sylow subgroup of $G$ since $N_G(P)$ is the stabilizer of the action of $G$ on the set $S$ of all 2-Sylow subgroups and $G$ act on $S$ transitively. Note that $G$ is simple, so there is six different 5-Sylow subgroups of $G$. Clearly the interesection of different 5-Sylow subgroups is trivial. Also the interrsection of 5-Sylow subgroup and 2-Sylow subgroup is trivial since $\gcd(4, 5) = 1$. Then there at least $1+(4-1)*15+(5-1)*6 = 70 > 60$ differenet element in $G$, a contradiction.

(b) The number of Sylow-2 subgroup can be $3, 5, 15$. Now consider $G$ act on Sylow-2 by conjugation.
    (i) 3 is impossible.
    (ii) If it has 5 Sylow-2 subgroup, it gives a isomorphism $G$ to $A_5$ since $|A_5| = 60$.
    (iii) 15 is impossible in the proof of (a).

□

## 13. Sem 2, 2007/2008

**Question 13.1.** *Let $R$ be a commutative ring with* 1.

*(a) Let $I$ be an ideal of $R$. Explain briefly what is meant to say that (i) $I$ is prime, (ii) $I$ is maximal.*

*(b) Prove or disprove each of the following statements:*
   *(i) If $I$ is a maximal ideal of $R$, then $I$ is prime.*
   *(ii) If $I$ is a nonzero prime ideal of $R$, then $I$ is maximal.*

*Proof.* See Question 6.1 □

**Question 13.2.** *Let $p$ and $q$ be a prime integers with $p \leq q$.*

*(a) Show that any group of order $pq$ has a normal subgroup of order $q$.*

*(b) Hence, or otherwise, classify all groups of order $pq$ up to isomorphism.*

*Proof.* (a) Suppose that $|G| = pq$. Sylow thorem there $kq + 1|pq$ Sylow $q$-subgroup. By $p \leq q$, there only one Sylow $q$-subgroup, then it is normal.

(b) Let $Q$ be a Sylow $q$-subgroup in $G$. Let $P$ be a Sylwo $p$-subgroup of $G$.
 (i) If $p \nmid q$, i.e. no $kp+1=q$ then $P$ is normal in $G$. So $G \cong \mathbb{Z}_p \times \mathbb{Z}_q = \mathbb{Z}_{pq}$.
 (ii) IF $p \mid q$. Let $P = \langle a \rangle$, $Q = \langle b \rangle$. Consider $P$ act on $Q$ by conjugation. Then $aba^{-1} = a^s$ should be a generator of $Q$. So $G = \langle a, b | a^p = 1, b^q = 1, aba^{-1} = a^s \rangle$ where $a^s$ is a generator of $Q$, i.e. $\gcd(s,q) = 1$.

□

**Question 13.3.** *Let $R$ be a ring with 1, and let $M$ be a left $R$-module. Prove that the following statements are equivalent:*
*(a) $M$ is nonzero, and if $N$ is a submodule of $M$, then $N = 0$ or $N = M$.*
*(b) For every $m \in M \setminus \{ 0 \}$, $M = \{ rm \mid r \in R \}$.*
*(c) There exists a maximal left ideal $I$ of $R$ such that $M \cong R/I$ as left $R$-modules.*

*Proof.* $(a) \Rightarrow (b)$**:** Clearly $N = \{ rm \mid r \in R \}$ is a submodule of $M$. $0 \neq m \in N$. So $N \neq 0$. Hence $N = M$.
$(b) \Rightarrow (c)$**:** There is a natural homomorphism $\phi$ from left $R$-module $R$ to $M$ by $\phi(r) = rm$. $I = \mathrm{Ker}\phi$ have to be maximal. If not $I$ is contained in some maximal left ideal $J$ since $R$ have 1. Then $J/I$ is a proper nontrivial submodule of $R/I$, but $R/I \cong M$, a contradiction.
$(c) \Rightarrow (a)$**:** Clearly by the one-one corresponding between left ideals of $R$ which contains $I$ and submodule of $R/I$.

□

## 14. Sem 1, 2008/2009

**Question 14.1.** *(a) Let $G$ be a finite simple group, and suppose that $H$ is proper subgroup of $G$ of index $k$. Show that there exists an injective group homomorphism from $G$ to the alternating group $A_k$ of degree $k$.*
*(b) Show that a group of order 120 is not simple.*

*Proof.* (a) Consider $G$ act on the set of left cosets $\{ gH \mid g \in G \}$ by left multiplication, i.e. $x \cdot gH = (xg)H$. It gives a map $\phi$ from $G \to S_k$ since $\# \{ gH \mid g \in H \} = k$. Clearly $\phi$ is nontrival since $H$ is proper subgroup of $G$ ($\exists g$ s.t. $gH \neq H$). So $\phi$ is monomorphism since $G$ is simple ($\mathrm{Ker}\phi$ is normal in $G$). Moreover $\mathrm{Im}\phi \subset \mathrm{A_n}$. If not $\mathrm{sgn}\phi \colon G \to \{ \pm 1 \}$ is epimorphism. Then $G$ have a nontrivial index 2 normal subgroup $\mathrm{Ker}\,\mathrm{sgn}\phi(|G| > 2)$.
(b) If $|G| = 120 = 8 \times 5 \times 3$ and $G$ is simple. By Sylow's theorem, $G$ has 6 Sylow 5-subgroup. Consider $G$ act on the 6 subgroup by conjugation. It gives a embedding of $G$into $A_6$. Clearly $G$ has index 3 in $A_6$. By considering $A_6$ act on the cosets of $G$, it gives a homomorphism from $A_6$ to $S_3$. But it impossible since $A_6$ is simple.

□

**Question 14.2.** *(a) Let $R$ and $S$ be integral domains with $R \subseteq S$. Prove or disprove the following:*
 *(i) If $R$ is a Euclidean domain, then $S$ is a unique factorisation domain.*
 *(ii) If $S$ is a Euclidean domain, then $R$ is a unique factorisation domain.*
*(b) Let $\phi \colon T \to U$ be a surjective ring homomorphism between two integral domains $T$ and $U$. Prove or disprove the following:*

*(i) If $T$ is a principal ideal domain, then $U$ is a principal ideal domain.*
*(ii) If $T$ is a unique factorisation domain, then $U$ is a unique factorisation domain.*

*Proof.* (a) a
(b) (i) For any ideal $I \subset U$, $\phi^{-1}(I)$ is a ideal in $T$. Then $\phi^{-1}(I) = (r)$ for some $r$. Then $I = (\phi(r))$.
(ii) Not true! A example on wikipedia. $F[X, Y, Z, W]$ is UFD for any field $F$. But $F[X, Y, Z, W]/(XY - ZW)$ is not UFD.

□

**Question 14.3.** *Let $K$ be the splitting field of $X^4 - 2$ over the field $\mathbb{Q}$ of rational numbers.*

*(a) Show that there exist field automorphisms $\tau$ and $\sigma$ of $K$ satisfying the following properties.*
- *$\tau$ has order 2;*
- *$\sigma$ has order 4;*
- *$\tau \circ \sigma = \sigma^{-1} \circ \tau$.*

*(b) Hence, or otherwise, find all intermediate fields between $\mathbb{Q}$ and $K$.*

*Proof.* □

**Question 14.4.** *Let $R$ be a ring with multiplicative identity, and let $M$ be a finitely generated left $R$-module.*

*(a) Let $B$ be a non-empty finite subset of $M$. Show that $M$ is a free $R$-moudle with basis $B$ if and only if every function from $B$ to any left $R$-module $N$ can be uniquely extended to a left $R$-module homomorphism from $M$ to $N$.*
*(b) Suppose further that $R$ is a principal ideal domain. Prove that $M$ is a free $R$-module if and only if $M$ is a projective $R$-moudule.*

*Proof.* □