QUALIFY EXAMINATION ANSWERS - ALGEBRA

1. Sem2, 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. $\square$

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

$$f_g \colon G/A \to G/A$$

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

$$\chi(g) = f_g$$

Prove that χ is a group homomorphism. Determine the kernel of χ.

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 bijective. 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 χ 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 $\mathrm{Ker}\chi = \{ \mathrm{g \in G \mid h^{-1}gh \in A \forall h \in G} \}$. $\square$

Question 1.3. *Let R be a commutative ring with identity and let $\chi \colon R \to F$ be a nontrivial ring homomorphism, where F is an integral domain. Prove that kernel of χ 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 $ab \in \mathrm{Ker}\chi$, $\mathrm{Ker}\chi = \mathrm{ab + Ker}\chi = (\mathrm{a + Ker}\chi)(\mathrm{b + Ker}\chi)$. 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 $\mathrm{Ker}\chi$.) $\square$

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 ($xf = x(1_Vf) \in I$ 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. $\square$

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. $\square$

2. Sem1, 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 domian. 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. Whtat can conclude about θ why?*

(b) Let H be a subgroup of a group G with index 2. Prive 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) θ 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. Sem2, 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 $|G| = p^2$. By Sylow's theorem G has a order p subgroup P. It's easy to see that $C_G(P)$

□

4. Sem1, 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 $\langle e^{2\pi i/n} \rangle$. 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 ϕ. 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) a

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) a

(b) b

$\square$

5. Sem 2, 2002/2003

6. Sem 1, 2003/2004

Question 6.1. *(a) Let G be the additive grou $\mathbb{Q}/\mathbb{Z}$. 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.*

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 π 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 natrual sign map form $\mathrm{sgn}\colon S_n \to \{ \pm 1 \}$. restric on G. If G has odd permutation, $\mathrm{sgn}|_G$ 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.

$\square$

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. $\square$

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) g

□

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. □

8. Sem 1, 2004/2005

9. Sem 2, 2004/2005

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

10. Sem 1, 2005/2006

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 ϕ is monomorphism, then isomorphisom 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 $f \mapsto f(0)$. ϕ is surjective. Since R is integral domain, Kerϕ 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

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 ϕ from $G \to S_k$ since $\#\{ gH \mid g \in H \} = k$. Clearly ϕ is nontrival since H is proper subgroup of G ($\exists g$ s.t. $gH \neq H$). So ϕ is monomorphism since G is simple (Kerϕ is normal in G). Moreover Im$\phi \subset \mathrm{A_n}$. If not sgn$\phi\colon G \to \{ \pm 1 \}$ is epimorphism. Then G have a nontrivial index 2 normal subgroup Ker sgn$\phi(|G| > 2)$.

(b) If $|G| = 120 = 8 \times 5 \times 3$ and G is simple. By Sylow's theorem, $|G|$ has a order 8 subgroup H, it's normalizer $N(H)$ can not be G since G is simple. If the index of $N(H)$ is 5 or 3 for any cases it's impossible since $60 = |A_5|, 6 = |A_3| < 120 = |G|$. But by (a) G can be embedded into A_5 or A_3, a contradiction. If the index of $N(H)$ is 15, then there is 15 different 2-Sylow subgroup of G.

□

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)

□