FALL 2018

Qualifying Exam - MA 553

In answering any part of a question, you may assume the results in previous parts, even if you have not solved them. Be sure to provide all details of your work.

.....

1. Prove that there is no simple group of order $7^2 \cdot k$ which has a subgroup of index 10. (20 points)

Solution: Suppose G is a simple group. Let P be a subgroup of index 10 in G. Then the acton of a simple group G on G/P by left multiplication defines the nontrivial action homomorphism $\phi : G \to S_{10}$.

Since group G is simple the normal subgroup $ker(\phi)$ is trivial and ϕ is an injective homomorphism. Thus G is isomorphic to a subgroup $\phi(G)$ of S_{10}. Consequently $|G| = 7^2 \cdot k$ divides $|S_{10}| = 10! = 7 \cdot s$, where 7 does not divide s. This is a contradiction.

2. Assume that G is a group of order $17 \cdot 15$.

   (a) Show that G contains a normal cyclic subgroup P of order 17. (10 points)

   (b) Show that G/P is cyclic. (10 points)

   (c) Show that $P \subset Z(G)$ (10 points)

   (d) Show that G is abelian. (10 points)

   Solution: (a) By the Sylow theorem the number of the Sylow 17-subgroups n_{17} satisfies the conditions $n_{17}|15$, so $n_{17} = 1, 3, 5, 15$, and $n_{17} \equiv 1(\text{mod } 17)$. So $n_{17} = 1$ and consequently there is a unique Sylow 17-subgroup P which is normal in G. Moreover P is a subgroup of order 17. In particular $P \simeq \mathbb{Z}_{17}$.

   (b) Firs note that $|G/P| = |G|/|P| = 15 = 3 \cdot 5$.

   Then for the Sylow subgroups in G/P we have:

   $n_3 = 1, 5$, $n_3 \equiv 1(\text{mod } 3)$. So $n_3 = 1$.

   $n_5 = 1, 3,$, $n_5 \equiv 1(\text{mod } 5)$, and $n_5 = 1$. So there is a unique Sylow normal 3-subgroup $P_3 \simeq \mathbb{Z}_3$ and a unique Sylow normal 5-subgroup $P_5 \simeq \mathbb{Z}_3$. Since $P_3 \cdot P_5 = G/P$, and $P_3 \cap P_5 = 1$, and both P_3, P_5 are normal we conclude that

$$G/P = P_3 \times P_5 \simeq \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{15}$$

   is cyclic.

   (c) Since $P \simeq \mathbb{Z}_{17}$, its automorphism group

$$Aut(P) \simeq Aut(\mathbb{Z}_{17}) \simeq \mathbb{Z}_{17}^* \simeq \mathbb{Z}_{16}.$$

   Since P is normal G acts on P by conjugation defining the automorphisms of P. This determines the action homomorphism

$$\phi : G \to Aut(P) \simeq \mathbb{Z}_{16}.$$

   Since P is abelian the action of P on itself by conjugation is trivial. So $\phi(P) = 1$, and ϕ factors through

$$\overline{\phi} : G/P \to Aut(P) \simeq \mathbb{Z}_{16}.$$

Since $|G/P| = 15$, we have $\phi(G) = \overline{\phi}(G/P)$ divides $|G/P| = 15$ and $|Aut(P)| = 16$, hence it divides $gcd(15, 16) = 1$, and $\phi(G) = 1$. Thus the action of G on P by conjugation is trivial, and $P \subset Z(G)$.

(d) Since $P \subset Z(G)$ there is a natural surjective homomorphsim $G/P \to G/Z(G)$. The group $G/Z(G)$ is the image of the cyclic group G/P so it is cyclic. Consequently, by a theorem, G is abelian.

3. (a) Determine the number of the elements of order 2 in the Alternating group A_4. (10 points)

   (b) Describe the Sylow 2-subgroups in A_4. (10 points)

   (c) Describe the Sylow 2-subgroups in A_5 and find their number. (10 points)

Solution:

(a) The elements of order 2 in A_4 have the cycle type 2-2. There are exactly $4 \cdot 3 \cdot 2/8 = 3$ elements of that form

(b) The Sylow 2-subgroup in A_4 contains 4 elements since $|A_4| = 12 = 3 \cdot 4$. The Klein subgroup V_4 in A_4 consists of all the 3 elements of order 2 of the form 2-2:

$$(12)(34), (13)(24), (14)(23)$$

and 1. Thus it is a unique normal subgroup Sylow 2 subgoup in A_4.

(c) The group A_5 has 60 elements and its Sylow 2-subgroup is of order 4 The group A_4 is a subgroup of A_5 and contains V_4. So V_4 is a subgroup of A_5 and since it contains 4 -elements it is a Sylow 2 -subgroup. Since all Sylow 2 -subgroups are conjugate we conclude that all Sylow 2-subgroups are isomorphic to $V_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Moreover each Sylow 2-subgroup is determined by a unique fixed element in $\{1, 2, 3, 4, 5\}$. So there are 5 Sylow 2- subgroups in A_5.

4. Let R be a non-zero commutative ring with 1. Let I be an ideal of R such that $1 + a$ is a unit in R for all $a \in I$.

   (a) Show that I is proper. (10 points)

   (b) Show that I is contained in every maximal ideal of R. (10 points)

Solution: (a) Suppose $I = R$. Then $-1 \in I$, and $1 + (-1) = 0$ is a unit, by the assumption, which is impossible.

(b) Suppose I is not contained in a maximal ideal M. Then there is a noninvertible element $a \in I$ which is not in M. So, by maximality of M we have $(a) + M = R$, and thus there exists $c \in R$, $d \in M$ such that $ca + d = 1$. But by the assumption $d = 1 - ca \in M$ is a unit in R. A contradiction since a proper ideal contains no units.

5. Prove that

   (a) the natural homomorphism $\mathbb{Z} \to \mathbb{Z}[i]/(6+i), \quad a \mapsto a + (6+i)$ is surjective. (10 points)

   (b) $\mathbb{Z}[i]/(6+i) \simeq \mathbb{Z}_{37}$. (10 points)

Solution: (a) For any $a + bi + (6+i) \in \mathbb{Z}[i]/(6+i)$ we have

$$a + bi + (6+i) = a - 6b + (6+i)$$

as $a + bi - (a - 6b) = b(6+i)$. So

$$\phi(a - 6b) = a + bi + (6+i).$$

(b) $ker(\phi) = \{a \in \mathbb{Z} \mid (6+i)|a\}$.

If $6 + i|a$ then $N(6+i)|N(a)$, so $37|a^2$, and thus $37|a$. Conversely if $37|a$ then $6 + i|a$, as

$$37 = (6+i)(6-i),$$

and $a \in ker(\phi)$. So $ker(\phi) = 37\mathbb{Z}$, and, by the first isomorphism theorem,

$$\mathbb{Z}[i]/(6+i) \simeq \mathbb{Z}/37\mathbb{Z} = \mathbb{Z}_{17}.$$

6. Find a simpler description of the ring. $\mathbb{Z}[x]/(x^2-3, x+4)$. (10 points)

Solution: Consider the surjective homomorphism $\mathbb{Z}[x] \to \mathbb{Z}$. $f(x) \mapsto f(-4)$. Its kernel is given by

$$ker(\phi) = \{f \in \mathbb{Z}[x] \mid f(-4) = 0\}.$$

Since $x+4$ is monic there is a division with remainder

$$f(x) = q(x)(x+4) + r,$$

where r is constant. Thus $r = f(-4)$ so $f(-4) = 0$ implies that $(x+4)|f(x)$ and vice versa, and

$$ker(\phi) = (x+4)$$

Thus the induced homomrphism $\phi : \mathbb{Z}[x]/(x+4) \to \mathbb{Z}$ is an isomorphism. Consequently

$$\mathbb{Z}[x]/(x^2-3, x+4) \simeq \mathbb{Z}/(\phi(x^2-3)) = \mathbb{Z}/(13) = \mathbb{Z}_{13}.$$

7. Consider the polynomial $f(x) = x^4 + 2$ over $\mathbb{Q}$.

   (a) Express all roots of $f(x)$ in terms of radicals. (10 points)

   (b) Show that the degree of the splitting field $L = \mathbb{Q}_f$ over $\mathbb{Q}$ is 8. (10 points)

   (c) Determine the Galois group of the splitting field $L = \mathbb{Q}_f$ over $\mathbb{Q}$. (10 pts)

   (d) Find all the intermediate fields $\mathbb{Q} \subset F \subset L$ such that $[F : \mathbb{Q}] = 2$. (10 points)

Solution: (a) The roots of $x^4 + 2$ are of the form $\sqrt[4]{2}\epsilon$, where $\epsilon^4 = -1$. In particular ϵ is an 8-th root of unity so it has a form

$$\epsilon = \epsilon_8^k = cos(k \cdot 2\pi/8) + sin(k \cdot 2\pi/8),$$

where $k \in \mathbb{Z}_8^*$ and so $k = 1, 3, 5, 7$. In paricular $\epsilon = \sqrt{2}/2(\pm 1 \pm i)$, and the roots of $x^4 + 2$ are

$$\sqrt[4]{2}\sqrt{2}/2(\pm 1 \pm i) = \sqrt[4]{8}/2(\pm 1 \pm i)$$

(b) The sum of the roots

$$\sqrt[4]{8}/2(1 + i) + \sqrt[4]{8}/2(1 - i) = \sqrt[4]{8}$$

is in L. Likewise the elements $(1 + i) = 2(\sqrt[4]{8}/2(1 + i))/\sqrt[4]{8}$, and $\sqrt[4]{2} = 2/\sqrt[4]{8}$ are in L. So $\mathbb{Q}(\sqrt[4]{2}, i) \subseteq L$. On the other hand the roots $\sqrt[4]{2}\sqrt{2}/2(\pm 1 \pm i)$ generate L and are in $\mathbb{Q}(\sqrt[4]{2}, i)$. So $L = \mathbb{Q}(\sqrt[4]{2}, i)$.

Note that $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ since $\sqrt[4]{2}$ is a root of the polynomial $x^4 - 2$ which is irreducible over $\mathbb{Q}$, by Eisenstein criterion for $p = 2$. On the other hand i is a root of x^2+1 which has no roots in real field $\mathbb{Q}(\sqrt[4]{2})$, so it is irreducible over $\mathbb{Q}(\sqrt[4]{2})$. So $[L : \mathbb{Q}(\sqrt[4]{2}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2}] = 2$, and

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{2}] \cdot [\mathbb{Q}(\sqrt[4]{2}] : \mathbb{Q}] = 2 \cdot 4 = 8$$

(c) The polynomial $f(x) = x^4 + 2$ is irreducible, by Eisenstein criterion for $p = 2$. By (b) its Galois group has order 8. Then, by the classification of the Galois groups of irreducible polynomials, we conclude that $Gal(L/K) \simeq D_8$.

(d) Write

$$Gal(L/K) \simeq D_8 = \langle r, s \mid r^4 = s^2 = 1, rs = sr^3 \rangle.$$

There are exactly 3 subgroups of index 2 in $Gal(L/K) \simeq D_8$:

$$H_1 = \{1, r, r^2, r^3\}, H_2 = \{1, r^2, s, sr^2\}, H_3 = \{1, r^2, sr, sr^3\}.$$

They correspond, by Galois Theory, to 3 different intermediate fields F such that $\mathbb{Q} \subset F \subset L$ with $[F : \mathbb{Q}] = 2$, namely:

$$\mathbb{Q}(i),\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{2}i)$$

8. Let K be the splitting field of the polynomial

$$g(x) = (x^4 + x^2 + x)(x^3 + 1)(x^3 + x^2 + 1)$$

over F_2.

(a) Describe K and find $[K : F_2]$. (10 points)

(b) Find the Galois group $Gal(K/F_2)$ and its generator(s).(10 points).

Solution: (a) We can write $g(x)$ as the product of irreducible polynomials

$$g(x) = x(x^3 + x + 1)(x + 1)(x^2 + x + 1)(x^3 + x^2 + 1).$$

All the nonlinear polynomials in the above decomposition are irreducible over F_2 since they do not have roots in F_2 . So K is the splitting field of the product of irreducible polynomials of degree 2, and 3. Thus it is of the form $K = F_{2^6}$. Consequently $[K : F_2] = 6$.

(b) The Galois field

$$Gal(K/F_2) = Gal(F_{2^6}/F_2) \simeq \mathbb{Z}_6$$

is generated by the Frobenius autmorphism σ_2: $x \mapsto x^2$.