Problems on Abstract Algebra (Group theory, Rings, Fields, and Galois theory)

Dawit Gezahegn Tadesse (davogezu@yahoo.com)
African University of Science and Technology(AUST)
Abuja,Nigeria

Reviewer
Professor Tatiana-Gateva Ivanova
Bulgarian Academy of Sciences
Sofia, Bulgaria

March 2009

preface

The first chapter is the solutions to my first test during Algebra I.I hope many readers who have an idea about Abstract Algebra particularly, Group theory, in his/her undergraduate studies will not get them difficult.The second chapter is the extension of group theory mainly the applications of the Sylow theorems and the beginnings of Rings and Fields.The third chapter includes Group theory,Rings,Fields,and Ideals.In this chapter readers will get very exciting problems on each topic.

The fourth chapter is the beginning of Algebra II more particularily,it is all about the problems and solutions on Field extensions.The last chapter consists of the problems and solutions in Field extensions and Galois theory.In most of African universities curriclulum,the last two chapters are given at graduate level.

As much as possible,in very few of the problems,I have included two ways(approaches) of solving them.

The problems are which I took them as tests and exams while I was in my Algebra I and Algebra II classes.They were given by my course professor Prof.Tatiana-Gateva Ivanova. Most of the solutions are solutions I presented during the exams.I communicated with Prof.Ivanova and she really encouraged me to do this work which also includes giving me the Latex versions of her questions.My deep appreciation and respect go to her.My thanks also goes to Dr.Boubou Cisse who helped me giving my exam papers back.

We used 'Algebra,Micheal Artin' as a text book for both Algebra I and Algebra II and most of the problems are at the end of each respective chapters in the book.I really advice the readers to read the book before start solving the problems.Please before going to the solutions try to solve them by yourselves and then can check up your solutions.To make the material more student oriented I left some problems as an exercise after the similar problem has been solved.I hope the readers will benifit from solving them similarily than merely reading the solutions.

I really wel come suggestions and corrections.Finally I would like to thank Dr.Bashir Ali and Mr.Bewketu Teshale(currently a postgraduate student in South Africa) who helped me a lot in the typesetting of the document.

Contents

CHAPTER 1

Algebra I Test I

1) *(10 points)*

a) Let G be a cyclic group of order 6. How many of its elements generate G?

b) Answer the same question for the cyclic groups of order 5, 10 and 8.

Solution

a) Suppose that $G = \langle a \rangle$ for some $a \in G$,then $G = \{1, a, a^2, a^3, a^4, a^5\}$ since the order $o(G) = 6 \Rightarrow a^6 = 1$.Now finding the generators of G amounts to finding the elements of G of order 6, however this is possible iff the power of a is coprime with 6 i.e.iff $\gcd(a, 6) = 1$ where gcd refers to the greatest common divisor.Here the only generators of G are a and a^5 $\therefore$ the number of generators of a cyclic group of order 6 is just 2.

b) Suppose that $G = \langle a \rangle$ so that $G = \{1, a, a^2, a^3, a^4\}$ we can easily see here that a, a^2, a^3, a^4 are the generators so we have 4 total generators.(Note that if the order of a group is $p-$prime then the number of generators is $p - 1$.) Similarly,suppose that $G = \{1, a, a^2, ..., a^9\}$ then the generators here are a, a^3, a^7, a^9 and hence the number of generators is 4.

We leave to the reader to show ,similarly, that the number of generators of a cyclic group of order 8 is 4.

Another Approach:

In number theory, the totient $\varphi(n)$ of a positive integer n is defined to be the number of positive integers less than or equal to n that are coprime to n. The value of $\varphi(n)$ can be computed using the fundamental theorem of arithmetic: if $n = p_1^{k_1} \cdots p_r^{k_r}$ where the p_j are distinct primes, then $\varphi(n) = (p_1 - 1)p_1^{k_1 - 1} \cdots (p_r - 1)p_r^{k_r - 1}$. For example

$\varphi(6) = 2$(which is the number of generators) because $6 = 2^1.3^1$ so in this case, $p_1 = 2, p_2 = 3, k_1 = 1, k_2 = 1$. Similarly the reader can easily calculate $\varphi(5), \varphi(10), \varphi(8)$.

2) *(10 points)*

a) Find all subgroups of the symmetric group S_3.

b) Which of them are normal?

Solution

a) As a set $S_3 = \{1, (12), (23), (13), (123), (132)\}$,by the Lagrange theorem the subgroups of S_3 should have orders of $1, 2, 3, 6$. But the order of any cycle is equal with its length(for example,the order of (12) is 2).The only subgroup of S_3 with order 1 is $\{1\}$,the subgroups of S_3 with order 2 are:$\{1, (12)\}, \{1, (23)\}, \{1, (13)\}$,the only subgroup of S_3 with order 3 is $\{1, (123), (132)\}$,and the only subgroup of S_3 with order 6 is S_3 itself.So we have proved that the total number of subgroups of S_3 is 6 and they are:$H_0 = \{1\}, H_1 = \{1, (12)\}, H_2 = \{1, (23)\}, H_3 = \{1, (13)\}, H_4 = \{1, (123), (132)\}$, and $H_5 = S_3$.

b) H_0 is is normal because $\forall g \in S_3, g1g^{-1} = 1 \in H_0$, H_5 is normal in itself,and $\forall g \in S_3, gh_4g^{-1} \in H_4$,where $h_4 \in H_4$.

$\therefore$ the normal subgroups of S_3 are $\{1\}, \{1, (123), (132)\}$, and S_3.

3) *(10 points)*

a) Prove that every subgroup of index 2 is normal

b) Give an example of a subgroup of index 3 which is not normal.

Solution

a) Let G be a group and H be a subgroup of index 2.H partitions G into 2 left cosets H and aH, and similarly H partitions G into 2 right cosets, H, Ha for some $a \in G$. If $a \in H$ then $aH = H = Ha$ since H is a subgroup of G. If $a \in GH$ then $aH = GH = Ha$. Thus, $aH = Ha$ for all $a \in G$, and hence H is normal in G.

b) Let $G = S_3$ and $H = \{1, (12)\}$ a subgroup of index 3. Then $(123)H = \{(123), (13)\}$ and $H(123) = \{(123), (12)\}$, thus $(123)H \neq H(123)$ and H is not normal.

4) *(10 points)*

Prove that a group in which every element except the identity has order 2 is abelian.

Proof. Let G be a group such that for elements $a \neq 1$ we have $a^2 = 1$. Then we get $a = a^{-1}$. From closurity $ab \in G$ for $a, b \in G$. Then $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ (the second equality follows from the definition for the inverse of product of two elements and the third one using the fact that $a = a^{-1}, \forall a \in G$). We have proved that for any two elements $a, b \in G, ab = ba$ which means that G is abelian. □

5) Classify the groups of order 4 (10 points).

Solution

Let us prove the general case:Every group of order p^2 is one of the following types:

i) a cyclic group of order p^2;

ii) a product of two cyclic groups of order p.

Proof. Since the order of an element divides p^2,there are two cases to consider:

Case 1. G contains an element of order p^2 and is therefore a cyclic group. Therefore,$G \simeq C_p$.

Case 2. Every element x of G except the identity has order p.Let x, y be two elements different from 1,and let H_1, H_2 be the cyclic groups of order p generated by x and y respectively.We may choose y so that it is not a power of x.Then since $y \notin H_1, H_1 \cap H_2$ is smaller than H_2,which has order p.So $H_1 \cap H_2 = \{1\}$.Also,the subgroups H_i are normal because G is abelian.Since $y \notin H_1$,the group H_1H_2 is strictly larger than H_1,and its order divides p^2.Thus $H_1H_2 = G$Then from product groups,$G \simeq H_1 \times H_2$.Therefore,$G \simeq C_p \times C_p$.
Here $4 = 2^2 \therefore$ every group G of order 4 is isomorphic to C_4 or $C_2 \times C_2$.

□

6) *(10 points)* Let p be a prime number. Classify the groups of order p.

Solution

Let G be a group of order p,and let $1 \neq a \in G$.But by Lagrange theorem,$|a|||G| = p \Rightarrow |a| = p$ hence that this element generates the whole group $G \Rightarrow G = \langle a \rangle$

$\therefore G \simeq C_p$.

7) *(10 points)*

Classify the groups of order 6 by analyzing the following three cases:

a) G contains an element of order 6.

b) G contains an element of order 3 but none of order 6.

c) All elements of G have order 1 or 2.

Solution

a) If $|G| = 6$ and G contains an element g of order 6 then $G = \langle g \rangle$.

b) If $|G| = 6$ and G contains an element g of order 3 but no element of order 6, then $H = \{1, g, g^2\} = \langle g \rangle$ is a subgroup of G and thus partitions G into 2 right cosets, H and $Hb = \{b, gb, g^2b\}$ where $b \notin H$. The order of b has to divide 6, the order of G. So $|b| = 1, 2$, or 3. Since $b \notin H, |b| \neq 1$, so $|b| = 2$ or 3. If $|b| = 3$ then $b^2 \neq 1$. Moreover,

one sees that $b^2 \neq g$, for if $b^2 = g$ then $(b^2)^2 = g^2$ and $b^4 = b^3.b = g \Rightarrow b = g$, contradicting the assumption that $b \notin H$. Equally, straightforward arguments yields that $b^2 \neq g^2, b, gb, g^2b$. Thus, $|b| \neq 3$, and $|b| = 2$. Next, since H has index 2 then $Hb = bH$, and $\{b, gb, g^2b\} = \{b, bg, bg^2\}$. Again we look at the various cases: If $gb = bg$, then $(gb)^2 = g^2b^2 = g^2; (gb)^3 = b.(gb)^4 = g; (gb)^5 = g^2b$. Hence $|gb| = 6$, which contradicts the assumption that there was only one element of order 6. So $gb = bg^2$ and we have that $G = \{1, g, g^2, b, gb, g^2b\}$ with $|g| = 3, |b| = 2$ and $gb = bg^2$; Hence $G \simeq S_3$.

(c) If all elements have order 1 and 2, then G would be of the form $\{1, g_1, g_2, g_3, g_4, g_5\}$ with $|g_i^2|$ =1 for all $1 \leq i \leq 5$. Let $H = \langle g \rangle = \{1, g_1\}$. Then $[G : H] = \dfrac{6}{2} = 3$. Thus we should have 3 distinct left cosets. But the 5 cosets: $g_iH = \{g_i, g_ig_1\}$ for $1 \leq i \leq 5$ are distinct for $g_i \neq g_j$ for all $i \neq j$. Since H partitions G and $g_iH \neq g_jH$ we must have $g_iH \cap g_jH = \varnothing$. But then $|G| = 6.2 = 12$, contradicting our hypothesis that $|G| = 6$.

8) *(15 points)*

Prove that a group of order 30 can have atmost 7 subgroups of order 5.

Solution

Let G be a group of order 30 i.e it contains 30 elements.Suppose that H_i is a subgroup of G with order 5.But we know that a group having prime order is cyclic$\Rightarrow$ $H_i = \langle a^i \rangle$ for some $a^i \in G$.Using the fact that two distinict groups of prime order intersect at 1, 7 subgroups is possible as we will have a total of $7.4 + 1 = 29 \leq 30$ elements.If we suppose we are able to have greater than 7 subgroups,say 8 we would get the total number of distinict elements in G as $8.4 + 1 = 33 > 30$ which is not possible.

$\therefore$ the maximum possible number of subgroups of order 5 in a group of order 30 is 7.

9) *(20 points)*

a) Describe the set $Hom(\mathbb{Z}^+, \mathbb{Z}^+)$ of all homomorphisms $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$. Which of them are injective? which are surjective, which are authomorphisms?

b) Use the results of (a) to determine the group of automorphisms $Aut(\mathbb{Z}^+)$.

Solution

a) Let $z \in Z$ we have two cases:

i) If $z \in Z_+-$set of non-negative integers.
Since 1 is the generator for z under addition

$$z = 1 + 1 + ... + 1(ztimes)$$

since f is a homomorphism;
$f(z) = f(1 + 1 + ... + 1) = f(1) + f(1) + ... + f(1) = zf(1)$
Let $f(1) = a \in Z$ then it follows that $f(z) = az$

ii) If $z \in Z_-$−set of negative integers
-1 is also a generator for Z under addition:

$$z = -1 - 1 - ... - 1 = (-1) + (-1) + ... + (-1)(-ztimes)$$

As from the hyopthesis, f is a homomorphism;
$f(z) = f(-1 - 1... - 1) = f(-1) + f(-1) + ... + f(-1) = zf(-1)$
But $f(1) = a \Rightarrow f(-1) = -a \Rightarrow f(z) = -az$.
$\therefore$ we have proved that any homomorphism $f : Z^+ \to Z^+$ is of the form $f(z) = az$ where $a = f(1)$
Suppose that $f(z_1) = f(z_2) \Rightarrow az_1 = az_2 \Rightarrow z_1 = z_2$ when $a \neq 0 \Rightarrow f(z) = az$ is injective when $a \neq 0$.
When $a = \pm 1, f(z) = az = \pm z$ and f is surjective.
$\therefore Hom(\mathbb{Z}^+, \mathbb{Z}^+) = \{f : Z^+ \to Z^+ : f(z) = az, z \in Z, a = f(1)\}$

b) $Aut(\mathbb{Z}^+) = \{f : Z^+ \to Z^+, f(z) = z, f(z) = -z\} = \langle f(z) = -z\rangle$
$\therefore Aut(\mathbb{Z}^+) \simeq C_2$.

10) *(20 points)*

The Sylow theorem implies the following

Fact. Every group of order 2p, p is a prime number contains a subgroup of order p.

Classify the groups G of order 10 by analyzing the following cases:

a) G is abelian.

b) G is not abelian.

Solution

Know $10 = 2.5$ by the above fact there exists H a subgroup of G such that $\mid H \mid = 5$.But every group of prime order is cyclic which means $H = \langle a\rangle$ for some $a \in G$ and $a^5 = 1$.Therefore by Lagrange theorem, $[G : H] = 2$ but from the fact in the question (2) above H is normal in G i.e $H \triangleleft G$.Let $b \in G/H$,then the left cosets of G and H are H, and bH.$G = H \cup bH$ (it is a disjoint union)$\Rightarrow a \neq b$.As a set

$$G = \{1, a, a^2, a^3, a^4, b, ba, ba^2, ba^3, ba^4\} \tag{1.1}$$

We need to know a formula for multiplication in G. It will be enough to know that $ab \in bH = Hb$ presented as an element in (1.1) i.e $ab = ba^j, 1 \leq j \leq 4$.Here we alredy know that $a^5 = 1$ we need to determine the order of b :The group generated by b is a subgroup of G and hence by Lagrange theorem $o(b)|o(G) = 10$(where o refers to order).Convince yourself that the order of b can not be 5 meaning the only possibilities are $o(b) = 2 \vee o(b) = 10$.Infact, we have:consider $K = \langle b\rangle \cap \langle a\rangle < \langle a\rangle = H$ then $|K|||H| = 5$ as $a \neq b$ we get

a) If G is abelian,$ab = ba$ then we have two subcases for the order of b: (i) $o(b) = 2 \Rightarrow c = ab$ has an order of $2.5 = 10$ then $G = \langle c\rangle \simeq C_{10}$ (ii) $o(b) = 10 \Rightarrow G = \langle b\rangle \simeq C_{10}$

b) If G is not abelian,the only possible case is that $o(b) = 2$(if it were $o(b) = 10$ then the group would be abelian)$\Rightarrow ab = ab^j$ for $1 < j \leq 4$

Claim:j=4

Proof. $bab = a^j \Rightarrow a = ba^jb = (bab)(bab)...(bab) = (bab)^j = (a^j)^j \Rightarrow 1 = a^{j^2-1} = a^{j-1}j + 1$.But $|a| = 5 \Rightarrow 5|(j-1)(j+1)$.Since $0 \neq j-1 \leq 4, j+1 \leq 5$, then $5|(j-1) \vee 5|(j+1)$ but the only possible case this to happen is that $j + 1 = 5 \Rightarrow j = 4$

$\therefore G = \langle a, b|a^5 = 1, b^2 = 1, bab = a^4\rangle \simeq D_5$ □

CHAPTER 2

Algebra I Test II

1) *(25 points)*

Let p be a prime number, $p > 2$. Classify groups of order $2p$.

Hint. Prove that a group of order $2p$ is either cyclic or is isomorphic to the Dihedral group D_p

Solution

We will make use of the following fact:Every group of order $2p$, where $p > 2$ is a pime number,contains a subgroup of order p.

Let G be a group of order $2p$. The above fact implies that there exists an element $a \in G$, of order p. Then the cyclic group $H = \langle a \rangle$ has index 2 in G, and therefore is a normal subgroup.Furthermore,G is a disjoint union of two cosets

$$G = H \cup Hb, b \in G \backslash H$$

So there is an equality of sets:

$$G = \{1, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b\} \tag{2.1}$$

We claim that $b^2 = 1$. Note first that b^2 is not in bH, since $b^2 = ba^i, 1 \leq i \leq 4$ would imply $b = a^i \in H$, which gives $bH = H$, a contradiction.It follows then that

$$b^2 \in H \cap \langle b \rangle. \tag{2.2}$$

But the intersection $H \cap \langle b \rangle$ is a subgroup of H, which is different from H, so its order divides the order of H, p, and therefore

$$H \cap \langle b \rangle = \{1\}. \tag{2.3}$$

It follows from (2) and (3) that $b^2 = 1$.

Two cases are possible:

a) G is abelian.Then $ab = ba$, and the element $c = ab$ is of order $2p$, therefore $G = \langle c \rangle \simeq C_{2p}$. (We have used the fact that if a, b are elements of a group of order m, n, respectively where m, are coprime,and $ab = ba$,then the order of $c = ab$ is the prodect of m and n.) The proof goes like this:
(i) $(ab)^{mn} = (ab)(ab)...(ab) = (a)^{mn}(b)^{mn} = (a^m)^n(b^n)^m = 1$ the second equality follows from the fact that $ab = ba$.So we have proved that $(ab)^{mn} = 1$.
(ii)Suppose that $(ab)^k = 1$ since $ab = ba$ we have $a^k b^k = 1 \Rightarrow a^k = b^{-k}$ since a,and b are coprime orders,if they intersect,the intersection is 1 implying that $a^k = b^{-k} = 1$ which implies that $m \mid k$ and $n \mid k$ and hence,from Number Theory, $mn \mid k$.
From (i) and (ii) one can conclude that the order of ab is mn.

b) G is not abelian. We will show that in this case G is isomorphic to the dihedral group D_p. G is described as a set by (2.1), but we need to find out a relation between a and b which will determine the multiplication in G. it will be enough to express explicitly ba as an element of the set on the right hand side of (2.1). Clearly,$ba \in bH = Hb$, and $ba \neq b$.Hence

$$ba = a^i b, for some i, 1 \leq i \leq p-1 \tag{2.4}$$

We multiply on b (on the right) the two sides of (4), and since $b^2 = 1$ we obtain

$$bab = a^j, for some j, 1 \leq j \leq p-1 \tag{2.5}$$

Note first that $1 < i$. Indeed if $j = 1$,we get $ba = ab$, and as we have shown above,the element $c = ab$ has order $2p$, which is impossible,since G is not abelian. Now we use (5) to deduce

$$a = ba^i b = (bab)(bab)...(bab) = (bab)^j = (a^j)^j = a^{j^2}, where 2 \leq j \leq p-1 \tag{2.6}$$

This implies

$$1 = a^{j^2-1},$$

and therefore the order p of a divides the integer $(j-1)(j+1)$. But $2 \leq j \leq p-1$, so $1 \leq j-1 \leq p-2$ and it is not divisible by p. It follows then(see the fact below) that p divides $j+1$, where $3 \leq j+1 \leq p$. Clearly this implies $j+1 = p$, so $j = p-1$. We have shown that if G is not abelian,it is generated by a, and b and the following relations are satisfied:

$$a^p = 1, b^2 = 1, bab = a^{p-1}.$$

This implies that G is isomorphic to the Dihedral group

$$D_p = \langle a, b; a^p = 1, b^2 = 1, bab = a^{p-1} \rangle \tag{2.7}$$

(Prove the isomorphism).

In this argument we used the following **fact** from Number Theory:

Suppose p is a prime number,$m, n-$ positive integers,and suppose p divides the product mn, but does not divide m. Then p divides n.To prove the fact we need the following lemmas from Number Theory:

Lemma 1:For any integers m, n, l, we have that

$$gcd(ml, nl) = gcd(m, n)l$$

Lemma 2:Suppose $m, n, l \in Z$ are such that $l \mid n$ and $l \mid m$.Then $l \mid gcd(m, n)$. where gcd refers to the greatest common divisor.

Proof of the fact:$p \nmid m$ implies that gcd(p, m)=1,since only 1 and p divide p.By the above Lemma 1 gcd$(pn, mn) = n$.Since $p \mid pn$ and,by hypothesis,$p \mid mn$,it follows from Lemma 2 that

$$p \mid gcd(pn, mn) = n$$

2) a) *(5 points) Give the definition of a Sylow p-subgroup of a group. Formulate the Sylow theorem.*

b) *(10 points)*

Let G be a group, and let p be a prime, which divides the order of G. Prove that if G has a unique Sylow subgroup H then H is a normal subgroup of G.

Solution

a) Definition:Let p be a prime.A group G, in which every element $x \in G$ is of order some positive powe of p is called a $p-$group.Clearly,every group of order a positive power of p is a $p-$group.A maximal $p-$group H in a group G is called a Sylow $p-$subgroup.(Note that a maximal subgroup H of a group G is a proper subgroup, such that no proper subgroup K contains H strictly.)

The following are the three famous Sylow theorems which were first proposed and proven by the Norwegian Mathematician Ludwig Sylow :

Theorem 1. *For any prime factor p with multiplicity n of the order of a finite group G, there exists a Sylow $p-$subgroup of G, of order p^n.*

The following weaker version of theorem 1 was first proved by Cauchy.

Corollary: Given a finite group G and a prime number p dividing the order of G, then there exists an element of order p in G.

Theorem 2. *Given a finite group G and a prime number p, all Sylow $p-$subgroups of G are conjugate (and therefore isomorphic) to each other, i.e. if H and K are Sylow $p-$subgroups of G, then there exists an element g in G with $g^{-1}Hg = K$.*

Theorem 3. *Let p be a prime factor with multiplicity n of the order of a finite group G, so that the order of G can be written as $p^n m$, where $n > 0$ and p does not divide m. Let n_p be the number of Sylow $p-$subgroups of G. Then the following hold:*

** n_p divides m, which is the index of the Sylow $p-$subgroup in G.*

** $n_p \equiv 1 mod p$.*

** $n_p = |G : N_G(P)|$, where P is any Sylow $p-$subgroup of G and N_G denotes the normalizer.*

b) From the above Sylow theorem 2 we have that for every $x \in G$ the conjugate group xKx^{-1} is a Sylow $p-$subgroup.It follows from the hypothesis that $xKx^{-1} = K$, and therefore K is normal.

3) *(25 points)*

Let p, q be prime numbers, $p < q$. Show that a group G of order pq can not be simple.

(Give the definition of a simple group first).

Solution

Definition(simple group) A group $G \neq \{1\}$ is called a simple group if it contains no proper normal subgroup(no normal group other than $\{1\}$ and G).

Note that there is only one sylow subgroup H of order q. Indeed,by the Sylow theorem 3 above,the number s_q of the Sylow $q-$subgroups divides p and equals $1(\text{mod}q)$,so $s_q = rq+1$ for some nonnegative integer r.This implies that $s_q = 1, s_q = q+1, s_q = 2q+1, ...$ but the only such s_q which can divide p is 1.This implies that $s_q = 1$,so the Sylow $q-$subgroup H is unique and therefore it is normal in G. Now we have got a proper normal subgroup H of G meaning that the group G having order pq where p, q are primes and $p < q$ can not be simple.

4) *(30 points)*

Classify groups of order 33.

Solution

We have $33 = 3.11$

Note first that there is only one Sylow subgroup H of order 11.Indeed,by the Sylow theorem 3 above,the number $s_1 1$ of the Sylow $11-$subgroups divides 3 and equals $1\text{mod}(11)$,so $s_{11} = q.11 + 1$ for some $q \geq 0$.This imples that $s_{11} = 1$,so the Sylow $11-$subgroup H is unique and therefore it is normal in G.Clearly,as a group of prime order $11, H$ is cyclic,$H = \langle a \rangle$,where $a^{11} = 1$ for some $a \in G$.

Next we study the number s_3 of the Sylow $3-$subgroups of G.By the Sylow theorem,$s_3|11$ thus the only possibilites are $s_3 = 1$, or $s_3 = 11$.Furthermore we have

$$s_3 = q.3 + 1,$$

from which we have $s_3 = 1, s_3 = 4, s_3 = 7, s_3 = 10, s_3 = 13, ...$ which shows that the case $s_3 = 11$ is impossible and the sylow $3-$subgroup K in G is also unique,and therefore,K is

normal.Clearly,as a group of prime order 3,K is cyclic,so $K = \langle b \rangle$,where $b^3 = 1$ for some $b \in G$.It follows from Lagrange's theorem that

$$H \cap K = \{1\} \tag{2.8}$$

The proof of (2.8) goes:

Let $H \cap K = A$ by the Lagrange theorem the order of A divides both the orders of H and K, as the orders of H and K are coprimes, we have the order of A equals 1.Hence $A = H \cap K = \{1\}$.

And we prove that $ab = ba$ as follows:

$a(ba^{-1}b^{-1}) \in H$ because $a \in H$ and H is normal group and hence closurity.Similarily $(aba^{-1})b^{-1} \in K \Rightarrow aba^{-1}b^{-1} \in H \cap K$ which means that $aba^{-1}b^{-1} = 1$ implying that $ab = ba$.The elements a and b commute and have orders 11 and 3,respectively,which are coprime numbers,therefore their product $c = ab$ has order $3.11 = 33$, or equivalently,the cyclic group $\langle c \rangle$ has order 33 which by hypothesis is the order of G,so $G = \langle c \rangle$.

This gives

$$G \simeq C_{33}$$

We have shown the following

Each group of order 33 **is isomorphic to** C_{33}

(5) *(35 points)*

Prove that the set $\mathbb{H}$ consisting of all complex matrices of the shape

$$A = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \in \mathbb{C}^{2\times 2}$$

is a division ring which is not commutative (i.e. $\mathbb{H}$ is not a field). The division ring $\mathbb{H}$ is called *the algebra of quaternions.*

Clearly,$\mathbb{H}$ is also a subspace of $\mathbb{C}^{n\times n}$. Find the dimension $dim_{\mathbb{C}}\mathbb{H}$

Solution

Let us recall the following definition:A non empty subset $S \subset R$ is a *subring* of R if it is closed under the operations summation,subtraction, and multiplication,and $1 \in S$ i.e.$1 \in S$ and,$a, b \in S \Rightarrow a + b \in S, a - b \in S, ab \in S$.

Take $a = 1$ and $b = 0$ then

$$A = \begin{bmatrix} 1 & 0 \\ -\bar{0} & \bar{1} \end{bmatrix} = I_{2\times 2}$$

which implies that $1 = I_{2\times 2} \in \mathbb{H}$. Let $A_1 = \begin{bmatrix} a_1 & b_1 \\ -\bar{b_1} & \bar{a_1} \end{bmatrix} \in \mathbb{H}$ and $A_2 = \begin{bmatrix} a_2 & b_2 \\ -\bar{b_2} & \bar{a_2} \end{bmatrix} \in \mathbb{H}$.It is very clear that $A_1 + A_2, A_1 - A_2, A_1A_2 \in \mathbb{H}$.Then from the definition of subring, $\mathbb{H}$ is a subring of $\mathbb{C}^{2\times 2}$ and hence it is a ring by itself.Let $A = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \Rightarrow a$

or $b \neq 0$.Since we have $\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \frac{1}{a^2+b^2} \begin{bmatrix} \bar{a} & -b \\ \bar{b} & a \end{bmatrix} = I_{2\times 2}$,every non zero element $A = \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$ of $\mathbb{H}$ has an inverse $A^{-1} = \frac{1}{a^2+b^2} \begin{bmatrix} \bar{a} & -b \\ \bar{b} & a \end{bmatrix} \in \mathbb{H}$.Hence $\mathbb{H}$ is a division ring. To show that it is not commutative,take $A = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \in \mathbb{H}$ and $B = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \in \mathbb{H}$,but it is not difficult to see that $AB \neq BA$.Hence noncommutativity follows. $dim_{\mathbb{C}}\mathbb{H} = 2$

CHAPTER 3

Algebra I Final exam

I. Group theory.

1. *(10 points)*

   Let $\mathbb{R}^\times$ be the multiplicative group of the nonzero real numbers, and let $P < \mathbb{R}^\times$ be the subgroup of positive real numbers. Identify the quotient group $\mathbb{R}^\times/P$

   Solution

   Let $\mathbb{R}^\times$, as given,the quotient group $\mathbb{R}^\times/P$ is the set of all cosets of P in $\mathbb{R}^\times$.Hence,

   $$\mathbb{R}^\times/P = P \cup P^- = \langle P^- \rangle$$

   where P^- is a set of negative real numbers.

   $\therefore \mathbb{R}^\times/P \simeq C_2$.

2. *(15 points)*

   Classify groups of order 95.

   Solution

   $95 = 5.19$

   From Sylow theorem,$S_5|19$ and $S_5 = 1 + 5r, r \geq 0$,where S_5 is the number of the Sylow 5-subgroups of G.As 19 is a prime,$S_5 = 1, 19$.However,the possible values of $S_5 = 1, 6, 11, 16, 21, \Rightarrow S_5 = 1 \Rightarrow$ The Sylow $5-$subgroup H is unique and normal.Since its order is prime it is cyclic$\Rightarrow H = \langle a \rangle, a \in G$.

   Similarily,$S_{19}|5$ and $S_{19} = 1 + 19r', r' \geq 0$.The only psssible value is $S_{19} = 1$,hence the Sylow 19-subgroup,K,is unique and then normal.Sine the order of K is prime,$K = \langle b \rangle$

for some $b \in G$.but observe that $a \neq b$.As two distinict cyclic groups intersect at 1,

$$H \cap K = \{1\} \tag{3.1}$$

Consider now $aba^{-1}b^{-1}$,

$$aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in H, \tag{3.2}$$

similarily,

$$aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in K \tag{3.3}$$

In the above equations (3.2) and (3.3)) we used the fact that every cyclic group is normal. From the equations (3.1),(3.2) and (3.3) one can conclude that $aba^{-1}b^{-1} = 1$ which by rearranging it means $ab = ba$.

Let $c = ab \Rightarrow |c| = 5.19 = 95 \Rightarrow$c generates G and hence G is cyclic $\Rightarrow G \simeq C_{95}$.

$\therefore$ any group of order 95 is cyclic.

3. *(20 points)*

Show that a group G of order 110 can not be simple.

Solution

Know $110 = 2.5.11$

Consider the Sylow $11-$subgroup,

By the Sylow theorem,

$S_{11}|10$ and $S_{11} = 1 + 11r, r \geq 0$, where S_{11} is the number of the Sylow 11-subgroup.As easily seen,the only psssibility is $S_{11} = 1$ which means that the Sylow 11-subgroup is normal.However, the Sylow 11-subgroup is a proper subgroup of G.We have proved here that there exists a proper normal subgroup of G which means that G can not be simple.

II. Rings, fields, ideals

4. *(20 points)*

a) Describe the group of units of the ring $\mathbb{Z}_n$, where n is an arbitrary positive integer

b) Prove that $\mathbb{Z}_p$ is a field if and only if p is a prime integer?

Solution

a) The groups of units of the ring $\mathbb{Z}_n, \mathbb{Z}_n^{\times} = \{k : 1 \leq k < n : gcd(n, k) = 1\}$

b) Suppose $\mathbb{Z}_p$ is a field,assume in contrary that,p is not prime which implies that $\exists s,t, 1 < s,t < p$ such that $p = st \Rightarrow \bar{p} = \bar{s}\bar{t}$ but $\bar{p} = 0$ in $\mathbb{Z}_p \Rightarrow \bar{s}\bar{t} = 0$,since $s,t \neq 0$ this means that $\mathbb{Z}_p$ has a zero divisor which is not possible in a field that is a contradiction.Hence,p is a prime.

In the other way around, suppose that p is a prime.(Here $\mathbb{Z}_p$ is a comutative ring) Let $0 \neq a \in \mathbb{Z}_p \Rightarrow 1 \leq a < p, \Rightarrow \gcd(a,p)$=1.But from our usual friend Number Theory,$\exists u, v \in \mathbb{Z}$ such that $1 = up + va \Rightarrow \bar{1} = \bar{u}\bar{p} + \bar{v}\bar{a}$ since $\bar{p} = 0$ in $\mathbb{Z}_p$ we have $\bar{v}\bar{a} = 1 \Rightarrow \bar{a}$ has an inverse in $\mathbb{Z}_p$.Since $\bar{a}$ is arbitrariliy non zero element of $\mathbb{Z}_p, \mathbb{Z}_p$ is a field.

5. *(25 points in total)*

a) *(10 points)*
Find the group of units $R^\times$, of the ring $R = \mathbb{Z}_{10}$.
Using direct computations show that $\mathbb{Z}_{10}^\times$, is a cyclic group and find an element $a \in \mathbb{Z}_{10}^\times$ which generates it.

b) *(15 points)*
Find the set S of all ideals in $\mathbb{Z}_{10}$. How many ideals contains S? Write down explicitly the elements of each ideal. Which are the maximal ideals in $\mathbb{Z}_{10}$?

Solution

a) From the above question(4) the groups of units of $\mathbb{Z}_{10}^\times = \{k : 1 \leq < 10, gcd(10,k) = 1\} \Rightarrow \mathbb{Z}_{10}^\times = \{1,3,7,9\}$.The order of the groups is 4.As a very simple exercise,show that this set is a group under multiplication $mod10$.Clearly,$\langle 3\rangle = \langle 7\rangle = \mathbb{Z}_{10}^\times$,then it is even a cyclic group generated by $a = 3$ or $a = 7$.

b) We know as a set $\mathbb{Z}_{10} = \{0,1,2,3,4,5,6,7,8,9\}$.The ideals of $\mathbb{Z}_{10}$ should be a subgroup of $\mathbb{Z}_{10}$ under addition $mod10$.However we have the following:
$(0) = \{0\}$
$(1) = (3) = (7) = (9) = \{0,1,2...,9\} = \mathbb{Z}_{10}$
$(2) = (4) = (6) = (8)\{0,2,4,6,8\}$
$(5) = \{0,5\}$
All the above form a subgroup of $\mathbb{Z}_{10}$ under addition $mod10$.Hence the set of ideals $S = \{(0),(2),(5),\mathbb{Z}_{10}\}$.
Note that a maximal ideal is an ideal which is not contained in any other proper ideal of the ring Or Given a ring R and a proper ideal I of R (that is $I \neq R$), I is called a maximal ideal of R if there exists no other proper ideal J of R so that $I \subset J$.Therefore the maximal ideals of $\mathbb{Z}_{10}$ are (2) and (5).

6. *(35 points in total)*

Let $C \subset \mathbb{R}^{2\times 2}$ be the set of all real matrices of the shape

$$A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in \mathbb{R}^{2\times 2}$$

a) *(15 points)*
Show that C is a field. (Prove first that C is a subring of the ring $\mathbb{R}^{2\times 2}$).

b) *(5 points)*
Show that C is a subspace of the space of matrices $\mathbb{R}^{2\times 2}$, find the dimension $dim_{\mathbb{R}}C$ and a basis of C (as an $\mathbb{R}$-space). (The result of this problem can be used for the solution of (c)).

c) *(15 points)*
Show that the field C is isomorphic to the field of complex numbers $\mathbb{C}$.

Solution

a) Let

$$A_1 = \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} \in C$$

and

$$A_2 = \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} \in C$$

then

$$A_1 + A_2 = \begin{bmatrix} a_1 + a_2 & b_1 + b - 2 \\ -(b_1 + b_2) & a_1 + a_2 \end{bmatrix} \in C$$

$$A_1 - A_2 = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ -(b_1 - b_2) & a_1 - a_2 \end{bmatrix} \in C$$

and

$$A_1A_2 = \begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -(a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{bmatrix} \in C$$

Furthermore,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in C$$

and hence C is a subring of $\mathbb{R}^{2\times 2}$.
$A_2A_1 = \begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -(a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{bmatrix} = A_1A_2$ which means the ring is a commutative one.Finally,for any $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \neq A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in C, A^{-1} = \begin{bmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ -\frac{-b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{bmatrix} \in C$,meaning that every non zero matrix in C is invertible.Hence,C is a field.

b) Let the matrices A_1 and A_2 are as given in (a).We showed that $A_1A_2 \in C$,let $r \in \mathbb{R}$ be a scalar.Then $rA \in C$ for any martix A in C.And C is a subspace of $\mathbb{R}^{2\times 2}$.
The set $\{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\}$ is a basis of C, over the vector space $\mathbb{R}$
$\therefore dim_{\mathbb{R}}C = 2$.

c) Let us define a function $\varphi : C \to \mathbb{C}$ by $\varphi(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}) = a + bi$.Th issue is to show that φ is an isomorphism:
Claim:

(1) φ is a homomorphism
(2) φ is bijective

Proof. (1) $\varphi(A_1 + A_2) = \varphi(\begin{bmatrix} a_1 + a_2 & b_1 + b - 2 \\ -(b_1 + b_2) & a_1 + a_2 \end{bmatrix}) = (a_1 + a_2) + i(b_1 + b_2)$,the last equality follows from the definition of φ.Using our complex analysis and substituting one gets $\varphi(A_1 + A_2) = \varphi(A_1) + \varphi(A_2$.
Similarily,$\varphi(A_1A_2) = \varphi(\begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -(a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{bmatrix}) = \varphi(A_1)\varphi(A_2)$.The identity element in C is the identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and the identity element in $\mathbb{C}$ is 1.In fact,we have $\varphi(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}) = 1 + 0i = 1$ i.e identity carried to identity.From all these three properties,φ is a homomorphism.

(2) Suppose that $\varphi(A_1) = \varphi(A_2) \Rightarrow a_1 + ib_1 = a_2 + ib_2$,using our friend complex analysis we finally have $a_1 = a_2$ and $b_1 = b_2 \Rightarrow A_1 = A_2 \Rightarrow \varphi$ is injective.In the other side,take $x + iy, x, y \in \mathbb{R}$,then $\begin{bmatrix} x & y \\ -y & x \end{bmatrix} \in C$ such that $\varphi(\begin{bmatrix} x & y \\ -y & x \end{bmatrix}) = x + iy$.Hence,$\varphi$ is surjective.And then from (1) and (2) φ is an isomorphism.
$\therefore C$ is isomorphic to $\mathbb{C}$.

□

CHAPTER 4

Algebra II Test I

1. *(1) (10 points)*

   Let F be a field. Find all elements $a \in F$, such that $a = a^{-1}$.

   Solution

   multiplying both sides of the equation $a = a^{-1}$ by a we get that $aa = 1$ where 1 is the multiplicative identity element in the field F this is possible as every field contains a multiplicative identity element$\Longleftrightarrow a^2 = 1 \Longleftrightarrow a^2 - 1 = 0 \Longleftrightarrow (a-1)(a+1) = 0$ but a field is an integral domain which implies that $a-1 = 0 \vee a+1 = 0 \Longleftrightarrow a = 1 \vee a = -1$.

   But both 1 and -1 are in $F \Rightarrow$ the possible values of a are -1 and 1 if the characterstic $charF = 2$. However when $charF = 2$ there exist only one element with $a^2 = 1$,namely $a = 1$.(because in this case we have $-1 = 1$.)

2. *(20 points)*

   Let $K = Q(\alpha)$,where α is a root of the irreducible polynomial $f(x) = x^5 + 2x^4 + 4x^3 + 6x + 2 \in Q[x]$. Determine α^{-1} explicitly.

   Solution

   α is a root$\Leftrightarrow \alpha^5 + 2\alpha^4 + 4\alpha^3 + 6\alpha + 2 = 0 \Leftrightarrow \alpha^5 + 2\alpha^4 + 4\alpha^3 + 6\alpha = -2 \Leftrightarrow \alpha(\alpha^4 + 2\alpha^3 + 4\alpha^2 + 6) = -2 \Leftrightarrow -1/2\alpha(\alpha^4 + 2\alpha^3 + 4\alpha^2 + 6) = 1$=the multiplicative identity element in K.

   which leads us to conclude that $\alpha^{-1} = -1/2(\alpha^4 + 2\alpha^3 + 4\alpha^2 + 6)$.

3. *(10 points)*

   Let F be a field and let α be an element which generates a field extension of degree 7. Prove that α^3 generates the same extension.

Solution

Let $K_1 = F(\alpha)$ and $K_2 = F(\alpha^3)$ then K_1 and K_2 are the field extensions generated by α and α^3 respectively.We are given that $[K_1 : F]$ = the degree of the irreducible polynomial of α over F=7. The main issue here is to prove that $K_1 = K_2$.We know that K_2 is an intermediate extension i.e $F \subset K_2 \subset K_1$ using the following important equation for such finite extension fields:$[K_1 : F] = [K_1 : K_2][K_2 : F] = 7$ as 7 is prime(the only divisors of 7 are 1 and 7 itself)one have either $[K_1 : K_2] = 1$ or $[K_1 : K_2] = 7$ but the second case is not posible if it was possible we would get that $[K_2 : F] = 1$which means $K_2 = F$ which is not true(the reader is invited to justify why they are not equal).Therefore we have proved that $[K_1 : K_2] = 1$ implying that $K_1 = K_2$.

$\therefore$the field extension generated by α^3 is the same with the one generated by α.

Remark: this fact is not necessarily true for degrees which are not prime.

4. *(20 points 6+7+8)*

Define $\zeta_n = e^{(2\pi)i/n}$. Find the irreducible polynomials over Q of (a) ζ_4, (b) ζ_6 (c) ζ_9

Solution

Definition:In algebra, the nth cyclotomic polynomial, for any positive integer n, is the monic polynomial

$$\phi_n(X) = \prod(X - \omega)$$

where the product is over all primitive nth roots of unity ω, i.e. all the complex numbers of order n.

Note that the irreducible polynomial of ζ_n over the field Q is the nth cyclotomic polynomial Φ_n. But for any positive integer n

we have $X^n - 1 = \Pi\Phi_d(X)$ where the product runs through d the divisors of n.

(a) So we have $X^4 - 1 = (X - 1)(X + 1)(X^2 + 1) = \Phi_1\Phi_2\Phi_4$.But $\Phi_1 = X - 1$ and $\Phi_2 = X + 1$which gives $\Phi_4 = X^2 + 1$.
$\therefore$ the irreducible polynomial over Q of ζ_4 is $\Phi_2 = X^2 + 1$.

(b) Also $X^6 - 1 = (X^3 - 1)(X^3 + 1) = (X^3 - 1)(X + 1)(X^2 - X + 1) = \Phi_1\Phi_2\Phi_3\Phi_6$ but $X^3 - 1 = \Phi_1\Phi_3$ and $X + 1 = \Phi_2$ which
gives us that $\Phi_6 = X^2 - X + 1$.
$\therefore$the irreducible polynomial over Q of ζ_6 is $\Phi_6 = X^2 - X + 1$.

(c) Similarily, the reader is invited to show that the irreducible polynomial over Q of ζ_9 is $\Phi_9 = X^6 + X^3 + 1$.

5. *(5) (10 points)*

Identify the groups F_4^+ and $F_4^\times$.

Solution

Let K be the field F_4.There is a unique irreducible polynomial $f(x)$ of degree 2 in $F_2[x]$,namely $f(x) = x^2 + x + 1$,and the field K is obtained by adjoining a root α of $f(x)$ to $F = F_2 : K \simeq F[x]/(x^2+x+1)$. Since the order of K is $4 = 2^2$,the elements of K are the roots of the polynomial $x^4 - x$ .Therefore as a set $K = F_4 = \{0, 1, \alpha, 1+\alpha\}$.The element $1 + \alpha$ is the second root of the polynomial $f(x)$ in K.Computation in K is made by using the relations $1 + 1 = 0$ and $\alpha^2 + \alpha + 1 = 0$.

We can easily see that $F_4^+ = \langle 1, 1 + \alpha\rangle$ = the group generated by the elements 1 and $1 + \alpha$ because $1 + 1 = 0$ and $1 + 1 + \alpha = \alpha$.Therefore $F_4^+ \simeq C_2$X C_2.

However as a set $F_4^\times = \{1, \alpha, 1+\alpha\}$ and $F_4^\times$ is generated by α because $\alpha^2 = -(\alpha+1) = \alpha + 1$ and $\alpha^3 = \alpha^2 + \alpha = 1 + 2\alpha = 1 \Rightarrow F_4^\times \simeq \langle\alpha\rangle$.Therefore we will finally have $F_4^\times \simeq C_3$=the cyclic group of order 3.

6. *(6) (15 points)*

Let $F = F_p$, be the prime field of order p, p is a prime. Suppose V is an F-vector space of dimension 4. How many elements contains V ? Motivate your answer.

Solution

The number of elements of V is p^4 but before we move to the proof first we need to prove one important fact:

Propostion:The number of words of length n, in a k distinict letters is exactly k^n. The proof goes with the Principle of Mathematical Induction (PMI) applied to n as follows.

(i) For $n = 1$, the number of words of length 1 in k distinict letters is obviously k

(ii) Assume the proposition is true for $n =, m$ and we should prove that it is true for $n = m + 1$

But from (ii) we have the number of words of length m in k distinict letters is k^m, now to get the number of words of length $m + 1$ in these k distinict letters, we have k choices to the word of length of m implying that we will have a total of $k^m k = k^{m+1}$ total number of words and hence the theorem follows from PMI. Suppose that $\{a_1, a_2, a_3, a_4\}$ is a basis of V over the field F.Let $v \in V$ implying that $v = \alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3 + \alpha_4 a_4$ for some $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in F$. The number of elements of V is the total number of words of length 4 in p letters which is, from the above fact,p^4.

7. *(25 points)*

Determine the irreducible polynomials of degree 2 over the field F_3.

Solution

We know as a set that $F_3 = \{0, 1, 2\}$.Let us assume that the required irreducible polynomial is monic(i.e the coefficient of its highest degree is 1).So the polynomial has a shape of $f(x) = x^2 + ax + b$.Note that a polynomial in F_3 is reducible iff it has roots in F_3.We have nine different cases for the values of a and b:

a=0, b=0 $\Rightarrow f(x) = x^2$ has 0 as a double root which means it is reducible

a=0, b=1 $\Rightarrow f(x) = x^2 + 1$ has no root in F_3 which implies it is irreducible

a=0, b=2 $\Rightarrow f(x) = x^2 + 2$ has 1 and 2 as roots implying it is reducible

a=1, b=0 $\Rightarrow f(x) = x^2 + x$ has 0 and 2 as roots meaning it is reducible

a=1, b=1 $\Rightarrow f(x) = x^2 + x + 1$ has 1 as a double root and it is reducible

a=1, b=2 $\Rightarrow f(x) = x^2 + x + 2$ has no root therefore it is irreducible

a=2, b=0 $\Rightarrow f(x) = x^2 + 2x$ has 0 and 1 as roots which means it is reducible

a=2, b=1 $\Rightarrow f(x) = x^2 + 2x + 1$ has 2 as a double root meaning it is reducible

a=2, b=2 $\Rightarrow f(x) = x^2 + 2x + 2$ has no root which implies that it is irreducible

$\therefore$we have the following three irreducible polynomials of degree 2 over the field F_3: $x^2 + 1, x^2 + x + 2$,and $x^2 + 2x + 2$.

8. *(Bonus problem) (45 points 20 +25)*

Determine the irreducible polynomial over $Q(\zeta_3)$ of (a) ζ_6, (b) ζ_9

Solution

(a) We know that the irreducible polynomial of ζ_6 over the field Q is $\zeta_6 = X^2 - X + 1$ and the irreducible polynomial of ζ_3 over the field Q is $\zeta_3 = X^2 + X + 1$.The roots of $\zeta_6 = X^2 - X + 1$ are $X_{1,2} = (1 \pm \sqrt{3})/2$ and that of $\zeta_3 = X^2 + X + 1$ are $X_{3,4} = (-1 \pm i\sqrt{3})/2$. As $[Q(\zeta_3) : Q] = [Q(\zeta_6)] = 2$=the degrees of the irreducible polynomials, one then can easily verify that $Q(\zeta_3) = Q(\zeta_6) = Q(i\sqrt{3})$. Furthermore,$\zeta_6 - \zeta_3 = 1 = X_{1,2} - X_{3,4}$ which means that $\zeta_6 = 1 + \zeta_3$ and then we get $f(X) = X - (1 + \zeta_3)$ as the irreducible polynomial over $Q(\zeta_3)$ of ζ_6.

(b) We know from the above question $4(c)$ that the irreducible polynomial of ζ_9 over Q is $\Phi_9 = X^6 + X^3 + 1$ this means we have $[Q(\zeta_9) : Q] = 6 = [Q(\zeta_3) : Q][Q(\zeta_9) : Q(\zeta_3)] \Rightarrow [Q(\zeta_9) : Q(\zeta_3)] = 3$ because $[Q(\zeta_3) : Q] = 2$. Clearly we have $\zeta_9^3 = \zeta_3$ therefore we can see that $f(X) = X^3 - \zeta_3$ is the irreducible polynomial of ζ_9 over the field $Q(\zeta_3)$.

CHAPTER 5

Algebra II Final Exam

1. *(15 points)* Express the symmetric polynomial

   $$f(u_1,u_2,u_3,u_4) = u_1^3u_2+u_1^3u_3+u_1^3u_4+u_2^3u_3+u_2^3u_4+u_3^3u_4+u_1u_2^3+u_1u_3^3+u_1u_4^3+u_2u_3^3+u_2u_4^3+u_3u_4^3$$

   as a polynomial in the elementary symmetric functions $\sigma_i, 1 \leq i \leq 4$, or equivalently, as a polynomial in the power sums

   $$S_k = u_1^k + u_2^k + u_3^k + u_4^k, \quad k = 1,2,3,4.$$

   Solution

   It is not difficult to see that $S_1S_3 = f + \Sigma u_1^4 \Rightarrow S_1S_3 = f + S_4$.

   Therefore we finally have $f = S_1S_3 - S_4$.

2. *(25 points)*

   Determine the Galois group of the polynomial $f(x) = x^3 - 2$.

   Let K be the splitting field of f over $\mathbb{Q}$. Describe the set of all intermediate fields L, $\mathbb{Q} < L < K$ and the Galois correspondence.

   Solution

   Let K be the splitting field of f over $\mathbb{Q}$ i.e an extension field of Q generated by the roots of f where the roots of f are $\alpha, \zeta\alpha$, and $\zeta^2\alpha$ where $\alpha =$ cubic root of 2 and ζ the third primitive root of unity.

   Writing the given polynomial $f(x) = x^3 - 2$ in the depressed cubic form: $f(x) = x^3 + px+q$ we get $p = 0$ and $q = -2$.Then determine the discriminant $D = -4p^3-27q^2$ which is $D = -27*4$ and it is clear that the square root of D is not in the field $F = Q$. Using

the criterion for cubic equations one gets that the galois group $G(K/Q) \simeq S_3 =$ the permutation group of order 6. And $S_3 = \{1, (12), (13), (23), (123), (132)\}$ has the following four proper subgroups : $\{1, (12)\}, \{1, (13)\}, \{1, (23)\}$, and $\{1, (123), (132)\}$.Therefore by The Main Theorem of Galois Theory we should have four intermediate fields corresponding to these proper subgroups.Observe that the splitting field $K = \mathbb{Q}(\alpha, \zeta)$ which corresponds to the whole group S_3, and $\mathbb{Q}(\alpha), \mathbb{Q}(\zeta\alpha), \mathbb{Q}(\zeta^2\alpha), \mathbb{Q}(\zeta)$ are the four splitting fields corresponding to the proper subgroups
$\{1, (12)\}, \{1, (13)\}, \{1, (123), (132)\}, \{1, (23)\}$ respectively.

OR(another approach towards the solution)

(Hint: The solutions of f are $\alpha, \zeta\alpha$, and $\zeta^2\alpha$ where $\alpha =$ cubic root of 2 and ζ the third primitive root of unity.So we have six different automorphisms sending a root of f to a root of f.)

3. *(30 points)*

Let

$$f(x) = x^4 + 4x^2 + 2 \in \mathbb{Q}[x]$$

$F = \mathbb{Q}$ and K be the splitting field of the polynomial f over $\mathbb{Q}$.

a) Find the Galois group $G(f) = G(K/F)$.

b) Describe explicitly the intermediate fields $\mathbb{Q} < L < K$ and the Galois correspondence between the set of subgroups of $G(f)$ and the set of intermediate fields.

c) Present K as a simple extension $K = \mathbb{Q}(\beta)$. What is the irreducible polynomial of β in $\mathbb{Q}[x]$?

Solution

a) Here $(i) 2 \mid 2, 2 \mid 0, 2 \mid 4, (ii) 2 \nmid 1$, and $(iii) 2^2 \nmid 2 \Rightarrow f(x)$ is irreducible by the Eisenstein's criterion .Write the polynomial $f(x) = x^4 + 4x^2 + 2$ in the depressed quartic form $f(x) = x^4 + px^2 + qx + r$ we get that $p = 4, q = 0$, and $r = 2$.Then the resolvant polynomial $w(x) = x^3 - 2px^2 + (p^2 - 4r)x + q^2$ is $w(x) = x^3 - 8x^2 + 8x$. Let θ_1, θ_2, and θ_3 be the roots of $w(x)$, clearly $\theta_1 = 0 \in Q$ but as the polynomial $w_1(x) = x^2 - 8x + 8$ is irreducible over Q we have $\theta_2, \theta_3 \notin Q$. By the criterion for quartic equations we get that $G(f) \simeq C_4$ or $G(f) \simeq D_4$. To determine the correct isomorphism we will check whether $D' = (\theta_2 - \theta_3)\sqrt{\theta_2\theta_3}$ is in Q or not.As θ_2 and θ_3 are the roots of $w_1(x) = x^2 - 8x + 8, \theta_2 - \theta_3 = D(w_1(x)) = 4\sqrt{2}$ and $\theta_2\theta_3 = 8$ which means that $D' = 16 \in Q$.(D is discriminant)

$\therefore G(f) \simeq C_4$.

Note that if we don't know whether polynomial $f(x)$ is irreducible directly then we should check if the roots are in Q or it can be written as a product of two irreducible monic quadratic equations (i.e check whether it can be written as $f(x) = (x^2 + ax + b)(x^2 + cx + d)$ for some a, b, c, and $d \in Q$.)

b) Put $x^2 = y$ then $x^4 + 4x^2 + 2 = 0 \Rightarrow y^2 + 4y + 2 = 0$ using the the quadratic formula from our high school Math we get $y = -2 + \sqrt{2}$ or $y = -2 - \sqrt{2}$ then solve for x.

Remember here that we have $D = 2\sqrt{2}$. If we let $\alpha_1, \alpha_2, \alpha_3$, and α_4 the roots of f we have $\alpha_1 = i\sqrt{2-\sqrt{2}}, \alpha_2 = i\sqrt{2+\sqrt{2}}, \alpha_3 = -i\sqrt{2-\sqrt{2}}, \alpha_4 = -i\sqrt{2+\sqrt{2}}$. C_4 contains the 4 elements generated by (1234) i.e.$C_4 \simeq \{1, (13)(24), (1234), (1432)\}$.The only proper subgroup of C_4 is $\{1, (13)(24)\}$ so by the Main Theorem of Galois Theory we should have exactly one intermediate field L corresponding to this proper subgroup.Observe that the the splitting field $K = \mathbb{Q}(\alpha_1, \alpha_2) = Q(\alpha_1) = Q(\alpha_2)$ and the intermediate field $L = \mathbb{Q}(i\sqrt{2})$.

c) From b) above we have $K = \mathbb{Q}(\beta) = \mathbb{Q}(i\sqrt{2-\sqrt{2}})$ and the irreducible polynomial of β in $\mathbb{Q}[x]$ is $f(x) = x^4 + 4x^2 + 2$.

4. *(20 points)*

Determine the irreducible polynomial over $\mathbb{Q}(\zeta_3)$ of ζ_6.

Solution

Please refer the last question in the previous chapter 4.

5. *(10 points)*

Show that if F is a finite field with characteristic p, then its cardinality is $\mid F \mid = p^m$, for some integer $m \geq 1$.

Solution

Let F be a finite field. Write its additive identity as 0 and its multiplicative identity as 1. The characteristic of F is a prime number p as the characteristic of a finite ring is positive and must be prime or else the ring would have zero divisors(Remember that a field has no zero divisors). The p distinct elements $0, 1, 2, , p1$ (where 2 means $1 + 1$, etc.) form a subfield of F that is isomorphic to Z/pZ.F is a vector space over Z/pZ, and it must have finite dimension over Z/pZ. Call the dimension m, so each element of F is specified uniquely by m coordinates in Z/pZ. There are p possibilities for each coordinate, with no dependencies among different coordinates, so the number of elements in F is p^m.

Another approach towards the proof:

When F is a finite field and a and b are any two nonzero elements of F, the function $f(x) = (b/a)x$ on F is an additive automorphism which sends a to b. (It certainly is not multiplicative too, in general!) So F is, under addition, a finite abelian group in which any two nonidentity elements are linked by an automorphism. Let's show that for any nontrivial finite abelian group A where any two nonzero elements are linked by an automorphism of A, the size of A must be a prime power. Let p be a prime factor of the size of A. By Cauchy's theorem, there is an element a of A of order p. Since we are assuming for every nonzero b in A there is an automorphism f of A such that $f(a) = b, b$ must have order p as well. Hence all nonzero elements in A have order p. If q were any prime dividing the size of A, by Cauchy's theorem there is an element in A of order q, and since we have shown all nonzero elements have order p it follows that $q = p$. Thus p is the only prime factor of the size of A, so A has order equal to a power of p.

6. *(50 points= 2+ 3 + 5 + 20+ 20)*

   a) Show that the polynomial $f(x) = x^2 + 1$ is irreducible in $\mathbb{F}_3[x]$.

   b) Let α be a root of f in some extension $K > \mathbb{F}_3$. Find a basis B for the simple extension $F = \mathbb{F}_3(\alpha)$ considered as a vector space over $\mathbb{F}_3$. Find the cardinality of F.

   c) Using the results of (a) and (b) write down explicitly the elements of the field $F = \mathbb{F}_{3^2}$ (in terms of the found basis B).

   d) Identify the multiplicative group $F^\times$. Find explicitly a generator β for $F^\times$ and present all elements of $F^\times$ as powers of β.

   e) What is the order $\mid F^+ \mid$, of F considered as a group with respect to the operation $+$. Give explicitly the order of each element of F^+. Identify the group F^+.

Solution

a) We know that as a set $F_3 = \{0, 1, 2\}$ but $f(0) = 1 \neq 0, f(1) = 2 \neq 0$, and $f(2) = 2 \neq 0$. As f does not have a root in F_3, $f(x) = x^2 + 1$ is irreducible in $\mathbb{F}_3[x]$.

b) Using the proposition: Let α be an algebraic element over F, and let $f(x)$ be its irreducible polynomial.Suppose $f(x)$ has degree n. Then $(1, \alpha, ..., \alpha^{n-1})$ is a basis for $F[\alpha]$ as a vector space over F.Therefore $B = (1, \alpha)$ is a basis for the simple extension $F = \mathbb{F}_3(\alpha)$ considered as a vector space over $\mathbb{F}_3$. Let $y \in F = \mathbb{F}_3(\alpha)$ then $y = x_1 + x_2\alpha =$ a linear combination of the elements of the basis B where x_1 and $x_2 \in \mathbb{F}_3$.Noting again the following important fact,:The number of words of length k in m letters is m^k,that the cardinality of F is $3^2 = 9$.

c) Use different values for x_1 and x_2 in the linear combination $y = x_1 + x_2\alpha$: as follows:
$x_1 = 0, x_2 = 0 \Rightarrow y = 0$
$x_1 = 0, x_2 = 1 \Rightarrow y = \alpha$
$x_1 = 0, x_2 = 2 \Rightarrow y = 2\alpha$
$x_1 = 1, x_2 = 0 \Rightarrow y = 1$
$x_1 = 1, x_2 = 1 \Rightarrow y = 1 + \alpha$
$x_1 = 1, x_2 = 2 \Rightarrow y = 1 + 2\alpha$
$x_1 = 2, x_2 = 0 \Rightarrow y = 2$
$x_1 = 2, x_2 = 1 \Rightarrow y = 2 + \alpha$
$x_1 = 2, x_2 = 2 \Rightarrow y = 2 + 2\alpha$
Therefore as a set we have $F = \{0, 1, 2, \alpha, 2\alpha, 1 + \alpha, 1 + 2\alpha, 2 + \alpha, 2 + 2\alpha\}$.

d) Here will see that $F^\times \simeq C_8 =$ the cyclic group of order 8 and computations are made using the relations $1 + 2 = 0$ and $\alpha^2 + 1 = 0$.As a set $F^\times = \{1, 2, \alpha, 2\alpha, 1 + \alpha, 1 + 2\alpha, 2 + \alpha, 2 + 2\alpha\}$. Put $\beta = 1 + \alpha$ then we have:
$\beta^1 = (1 + \alpha)^1 = 1 + \alpha$
$\beta^2 = (1 + \alpha)^2 = \alpha^2 + 2\alpha + 1 = 2\alpha$
$\beta^3 = (1 + \alpha)^3 = 2\alpha(1 + \alpha) = 2(\alpha^2 + \alpha) = 2(-1 + \alpha) = 2(2 + \alpha) = 1 + 2\alpha$

$\beta^4 = (1+\alpha)^4 = (1+\alpha)(1+2\alpha) = (1+3\alpha+2\alpha^2) = 1+0-2 = 2$
$\beta^5 = (1+\alpha)^5 = 2(1+\alpha) = 2+2\alpha$
$\beta^6 = (1+\alpha)^6 = (1+\alpha)(2+2\alpha) = 2(1+2\alpha+\alpha^2) = \alpha$
$\beta^7 = (1+\alpha)^7 = \alpha(1+\alpha) = \alpha+\alpha^2 = 2+\alpha$
$\beta^8 = (1+\alpha)(2+\alpha) = 2+3\alpha+\alpha^2 = 2+0-1 = 1$

Therefore one can see that $\beta = 1+\alpha$ generates $F^\times$ and have $F^\times = \langle(1+\alpha)\rangle \simeq C_8$.

e) As a set F^+ contains 9 elements implying that the order $\mid F^+ \mid$, of F considered as a group with respect to the operation $+$ is 9. The characteristic of $F = \mathbb{F}_3(\alpha)$ is 3 because $\forall a \in F = \mathbb{F}_3(\alpha)\backslash\{0\}$ we have $a+a+a = 3a = 0$, and 3 is the smallest such natural number implying that the order of each element except 0 is 3 but the order of 0 is 1.

The group $F^+ \simeq C_3 X C_3$.

A short History of Évariste Galois

Évariste Galois (French pronunciation: [evaist alwa]; October 25, 1811 May 31, 1832) was a French mathematician born in Bourg-la-Reine. While still in his teens, he was able to determine a necessary and sufficient condition for a polynomial to be solvable by radicals, thereby solving a long-standing problem. His work laid the foundations for Galois theory, a major branch of abstract algebra, and the subfield of Galois connections. He was the first to use the word "group" (French: groupe) as a technical term in mathematics to represent a group of permutations. A radical Republican during the monarchy of Louis Philippe in France, he died from wounds suffered in a duel under shadowy circumstances at the age of twenty.

Early life

Galois was born on October 25, 1811, to Nicolas-Gabriel Galois and Adéla´ide-Marie (born Demante). His father was a Republican and was head of Bourg-la-Reine's liberal party, and became mayor of the village after Louis XVIII returned to the throne in 1814. His mother, the daughter of a jurist, was a fluent reader of Latin and classical literature and she was for the first twelve years of her son's life responsible for his education. At the age of 10, Galois was offered a place at the college of Reims, but his mother preferred to keep him at home. In October 1823, he entered the Lycée Louis-le-Grand, and despite some turmoil in the school at the beginning of the term (where about a hundred students were expelled), Galois managed to perform well for the first two years, obtaining the first prize in Latin. He soon became bored with his studies, and it was at this time, at the age of 14, that he began to take a serious interest in mathematics. He found a copy of Adrien Marie Legendre's Éléments de Géométrie, which it is said that he read "like a novel" and mastered at the first reading. At the age of 15, he was reading the original papers of Joseph Louis Lagrange and Niels Henrik Abel, work intended for professional mathematicians, and yet his classwork remained uninspired, and his teachers accused him of affecting ambition and originality in a negative way.

Budding mathematician

In 1828, he attempted the entrance exam to École Polytechnique, without the usual preparation in mathematics, and failed for lack of explanations on the oral examination. In that same year, he entered the École préparatoire, a far inferior institution for mathematical studies at that time, where he found some professors sympathetic to him. In the following year, Galois' first paper, on continued fractions was published, and while it was competent it held no suggestion of genius. Nevertheless, it was at around the same time that he began making fundamental discoveries in the theory of polynomial equations, and he submitted two papers on this topic to the Academy of Sciences. Augustin Louis Cauchy refereed these papers, but refused to accept them for publication for reasons that still remain unclear. In spite of many claims to the contrary, it appears that Cauchy had recognized the importance of Galois' work, and that he merely suggested combining the two papers into one in order to enter it in the competition for the Academy's Grand Prize in Mathematics. Cauchy, a highly eminent mathematician of the time considered Galois' work to be a likely winner (see below). On July 28, 1829, Galois' father committed suicide after a bitter political dispute with the village priest. A couple of days later, Galois took his second, and final attempt at entering Polytechnique, and failed yet again. It is undisputed that Galois was more than qualified; however, accounts differ on why he failed. The legend holds that he thought the exercise proposed to him by the examiner to be of no interest, and, in exasperation, he threw the rag used to clean up chalk marks on the blackboard at the examiner's head. More plausible accounts state that Galois made too many logical leaps and baffled the incompetent examiner, evoking irascible rage in Galois. The recent death of his father may have also influenced his behavior.

Having been denied admission to Polytechnique, Galois took the Baccalaureate examinations in order to enter the Ecole Normale. He passed, receiving his degree on December 29 1829. His examiner in mathematics reported: "This pupil is sometimes obscure in expressing his ideas, but he is intelligent and shows a remarkable spirit of research."

His memoir on equation theory would be submitted several times but was never published in his lifetime, due to various events. As previously mentioned, his first attempt was refused by Cauchy, but he tried again in February 1830 after following Cauchy's suggestions and submitted it to the Academy's secretary Fourier, to be considered for the Grand Prix of the Academy. Unfortunately, Fourier died soon after, and the memoir was lost. The prize would be awarded that year to Abel posthumously and also to Jacobi. Despite the lost memoir, Galois published three papers that year, two of which laid the foundations for Galois theory, and the third, an important one on number theory, where the concept of a finite field is first articulated.

Contributions to Mathematics

Tu prieras publiquement Jacobi ou Gauss de donner leur avis, non sur la vérité, mais sur l'importance des théorémes.

Aprs cela, il y aura, j'espere, des gens qui trouveront leur profit é déchiffrer tout ce gâchis.

(Ask Jacobi or Gauss publicly to give their opinion, not as to the truth, but as to the

importance of these theorems. Later there will be, I hope, some people who will find it to their advantage to decipher all this mess.) Évariste Galois, Lettre de Galois é M. Auguste Chevalier

Unsurprisingly, Galois' collected works amount to only some 60 pages, however within them are many important ideas that have had far-reaching consequences for nearly all branches of mathematics. It was indeed, much to the advantage of later mathematicians to decipher the mess that was Galois' work. His work has been compared to that of Niels Henrik Abel, yet another mathematician who died tragically at a very young age, and much of their work has had significant overlap.

Algebra

While many mathematicians before Galois gave consideration to what are now known as groups, it was Galois who was the first to use the word 'group' (in French groupe) in the technical sense it is understood today, making him among the key founders of the branch of algebra known as group theory. He developed the concept that is today known as a normal subgroup. He called the decomposition of a group into its left and right cosets a 'proper decomposition', if the left and right cosets coincide, which is what today is known as a normal subgroup. He also introduced the concept of a finite field (also known as a Galois field in his honor), in essentially the same form as it is understood today.

Galois Theory

Main article: Galois theory

Galois' most significant contribution to mathematics by far is his development of Galois theory. He realized that the algebraic solution to a polynomial equation is related to the structure of a group of permutations associated with the roots of the polynomial, the Galois group of the polynomial. He found that an equation could be solvable in radicals if one can find a series of normal subgroups of its Galois group which are abelian, or its Galois group is solvable. This proved to be a fertile approach, which later mathematicians adapted to many other fields of mathematics besides the theory of equations which Galois originally applied it to.

This short history is taken from Wikipedia, the free encyclopedia.

References

[A.G90] Joseph A.Gallian. *Contemporary Abstract Algebra,2nd edition.* D.C.Heath and Company, 1990.

[Art91] Micheal Artin. *Algebra.* Upper Saddle River, 1991.

[I.N75] I.N.herstein. *Topics in Algebra, 2nd edition.* Wiley, New York, 1975.

[Lip91] Seymour Lipschutz. *Schaumu's outline of Theory and problems of Linear Algebra.* Mc GRAW-Hill, New York, 1991.

[LR04] Frank Ayres Lloyd R.Jaisingh. *Schaumu's outline, Abstract Algebra, 2nd edition.* Mc GRAW-Hill, New York, 2004.

[MBP06] G. Marchesi M. Beck and D. Pixton. *A First course in Complex Analysis.* Mc GRAW-Hill, 2002- 2006.

[Rom08] Steven Roman. *Advanced Linear Algebra, 3rd edition.* Springer, New York, 2008.

[Ste07] William Stein. *Elementary Number Theory,A Computational Approach.* Mc GRAW-Hill, March 2007.