MATH 631
Midterm Part I

Name : SOLUTIONS

November 14, 2018

Instructions: This exam is closed book and closed notes, and one hour in length. Part II is on Friday. You may use **only** your brain and blank scratch paper in writing solutions.

Questions involving quick computational answers will be clearly indicated. You do not need to show work for these. For more theoretical questions, you should prove results from first principles and not simply quote statements from the book. Your proofs will be graded not only on correctness, but points will be awarded/taken away for poor writing and exposition. Blank paper is supplied for scratch work, but final responses should be written in the space provided. Do your best!

1. (6 pts.) Answer briefly.

(a) Give an example of a finite ring of characteristic zero, if possible. Otherwise explain why no such ring exists.

Impossible. If $|R| = n$, then $n \cdot 1 = 0$ so the characteristic of $R \leq n$.

(b) Give the definition of a nilpotent element in a ring R. Then prove that the set of nilpotent elements in $M_2(\mathbb{Q})$ is **not** an ideal.

Suppose $x \in R$. If there exists $n \in \mathbb{Z}^+$ such that $x^n = 0$, then x is nilpotent.

Both $x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ are nilpotent with $n=2$. However,

their sum is $x+y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ which is a unit!

2. (6 pts.) Suppose G is a non-cyclic group of order $205 = 5 \cdot 41$. Give, with proof, the number of elements of order 5 in G. By the Sylow Theorems, $n_{41} = 1$. Thus, there is a unique normal subgroup of prime $p = 41$ order $\mathbb{Z}_{41}$. The subgroup contains 40 elements of order 41. If $n_5 = 1$, then G would necessarily be cyclic since if the unique Sylow 5-subgroup is $\langle x \rangle$ and $\mathbb{Z}_{41} = \langle y \rangle$, then $|xy| = 205$ since $|xy| \neq 1, 5, 41$ and G is cyclic. Thus, G has $205 - 40 - 1 = 164$ elements of order 5

3. (6 pts.) Find **ALL** solutions x in the integers to the simultaneous congruences.

$$x \equiv 7 \mod 11$$
$$x \equiv 2 \mod 5$$

$1 = 1 \cdot 11 - 2 \cdot 5$

$\Rightarrow \quad x = 7 \cdot (-10) \quad + 2 \cdot 11 \quad + \quad 55k \quad k \in \mathbb{Z}$

$= -48 + 55k$

$= 7 + 55k$!

4. (12 pts.) Suppose G is a group, $H \leq G$, and $\mathrm{Aut}(H)$ the group of automorphisms of H.

(a) Using the First Isomorphism theorem, give a **full** proof of the following statement. The quotient group $N_G(H)/C_G(H) \cong A \leq \mathrm{Aut}(H)$.

Let $N = N_G(H)$ act on H by conjugation; that is, if $n \in N$, $n \cdot h = nhn^{-1}$ $\forall h \in H$. Since $n \in N$, this is a well-defined group action and each n induces an automorphism $\varphi_n \in \mathrm{Aut}(H)$. This group action induces a group homomorphism $\varphi : N \to \mathrm{Aut}(H)$ given by $\varphi(n) = \varphi_n$. Let $A = \mathrm{Im}(\varphi)$ and note that $A \leq \mathrm{Aut}(H)$. Moreover, the kernel of φ is $C = \{n \in N \mid n \cdot h = h \ \forall h \in H\} = \{n \in N \mid nhn^{-1} = h \ \forall h \in H\}$

$$= \{n \in N \mid nh = hn \ \forall h \in H\} = C_G(H)!$$

By the First Isomorphism Theorem,

$$N/C \cong A. \ \square!$$

(b) Suppose now that P is a Sylow p-subgroup of S_p for a prime p. Prove that

$$N_{S_p}(P)/C_{S_p}(P) \cong \mathrm{Aut}(P).$$

Let P be a Sylow p-subgroup of S_p. Note that P is cyclic generated by a p-cycle. By part a) using $N = N_{S_p}(P)$ and $C = C_{S_p}(P)$, we have $N/C \cong A \leq \mathrm{Aut}(P)$ for some subgroup $A \leq \mathrm{Aut}(P)$. Moreover, since P is cyclic, $|\mathrm{Aut}(P)| = p-1$. If $p=2$, then $S_p \cong C_2$ and the result is trivial, so assume p is odd.

Let $\mathrm{Syl}_p(S_p)$ be the collection of Sylow p-subgroups of S_p. Then $n_p = |\mathrm{Syl}_p(G)|$ can be computed directly: Each $H \in \mathrm{Syl}_p(S_p)$ is cyclic, generated by a p-cycle, and contains exactly $p-1$ p-cycles. The number of p-cycles in S_p is $(p-1)!$. Thus, $n_p = (p-1)!/p-1 = (p-2)!$. If S_p acts on $\mathrm{Syl}_p(S_p)$ by conjugation, the Orbit-Stabilizer Theorem yields $n_p = (p-2)! = |\mathcal{O}_P| = [S_p : N]$ from which we compute $|N| = p(p-1)$. Moreover, $C = P$ and so $|C| = p$. Finally, $|N/C| = p(p-1)/p$ so that the cardinality $|A| = p-1$. That is, $A = \mathrm{Aut}(P)$.

Lemma: If p is a prime and $P = \langle (1 \cdots p) \rangle$ is a Sylow-p-subgroup of S_p, then $C_{S_p}(P) = P$.

Proof. Let $\tau = (1\ 2 \cdots p)$ and $\sigma \in S_p$. Under conjugation, $\sigma \cdot \tau = \sigma \tau \sigma^{-1} = (\sigma(1)\ \sigma(2)\ \cdots\ \sigma(p)) = (1\ 2\ \cdots\ p)$ if, and only if, there is some integer j with $\sigma(i) = i + j \mod p$. Thus, $\sigma = \tau^j$. □

Note on grading: I tried to be very generous here. You did not need as complete a proof as I gave.

5. (10 pts.) Prove **one** of the following statements. Circle the statement you want graded.

(a) Every nonzero prime ideal in a PID is a maximal ideal.

OR

(b) In a PID every nonzero element is a prime if, and only if, it is irreducible.

(a) Suppose P is a non-zero prime ideal in a PID R. Then there exists a generator $x \in P$ with $P = (x)$. Suppose that $J \subseteq R$ is an ideal, $J = (y)$ for $y \in R$, and $P = (x) \subseteq (y) \subseteq R$.

Since $x \in (y)$, there exists an element $r \in R$ with $x = yr$. Since P is prime and $yr = x \in P$, either $y \in P$ or $r \in P$. In the first case, when $y \in P$, then $(y) \subseteq (x) = P$ and $(x) = (y)$. In the second case, when $r \in P = (x)$, there exists some $s \in R$ with $r = sx$. Thus,

$x = yr = ysx \Rightarrow 1 = ys$ by the cancellation law in domains since $x \neq 0$.

Thus, y is a unit in R and $(y) = J = R$. Thus, P is a maximal ideal. $\square$

(b) In a PID R, show $x \in R$, $x \neq 0$, then x is prime $\Leftrightarrow$ x is irreducible.

$\Rightarrow$) Suppose x is prime and $x = ab$ for $a, b \in R$. Then $x \mid ab$ and since x is prime, x divides one of the factors, without loss of generality $x \mid a$. Then there exists $r \in R$ with $a = xr$ and thus, $x = ab = xrb \Rightarrow 1 = rb$ in a domain. It follows that b is a unit of R and that p is irreducible.

$\Leftarrow$) Suppose now that $p \in R$ is irreducible. We will show that (p) is a maximal ideal. To this end, suppose $(p) \subseteq (m) \subseteq R$. Then $p = mx$ for some $x \in R$. Since p is irreducible, either m is a unit in which case $(m) = R$ or x is a unit in which case $(p) = (m)$. Since (p) is therefore a maximal ideal, it is also a prime ideal and therefore p is a prime element of R.

6. (10 pts.) Suppose R is a commutative ring with 1 and for each $x \in R$, there is a positive integer $n > 1$ so that $x^n = x$. Prove that every nonzero prime ideal is maximal.

Let $P \subseteq R$ be a non-zero prime ideal and form the quotient ring R/P.

It suffices to show that R/P is a field, since this establishes that P is a maximal ideal. Since P is prime, R/P is an integral domain and it remains to show every non-zero element of R/P is a unit.

To this end, suppose $x \notin P$ and consider $x + P \in R/P$. By hypothesis, there is some integer $n > 1$ such that $x^n = x$. From this, we find

$$(*) \quad x^n + P = (x+P)(x^{n-1} + P) = (x+P) = (x+P)(1+P)$$

Moreover, since R/P is an integral domain by the cancellation law, $(*)$ implies $(x^{n-1} + P) = (1+P)$ in R/P. As a result,

$$(x+P)(x^{n-2} + P) = (1+P) \text{ in } R/P$$

and $x+P$ is a unit. $\square$

MATH 631
Midterm Part II

Name : SOLUTIONS

November 16, 2018

Instructions: This exam is closed book and closed notes, and one hour in length. You may use **only** your brain and blank scratch paper in writing solutions.

Questions involving quick computational answers will be clearly indicated. You do not need to show work for these. For more theoretical questions, you should prove results from first principles and not simply quote statements from the book. Your proofs will be graded not only on correctness, but points will be awarded/taken away for poor writing and exposition. Blank paper is supplied for scratch work, but final responses should be written in the space provided. Do your best!

7. (5 pts.) Recall that an *integral domain* or a *domain* is a commutative ring with 1 that has no zero divisors.

   Suppose that R is a commutative ring with 1. Give, with proof, a necessary and sufficient condition on ideals of R so that R is an integral domain.

   Answer: A ring R that is commutative with multiplicative identity 1 is an integral domain if, and only if (0) is a prime ideal.

   Proof:

   The principal ideal (0) is prime : for all $ab \in (0)$ either $a \in (0)$ or $b \in (0)$

   This holds if, and only if, $ab = 0 \Rightarrow a = 0$ or $b = 0$ i.e.

   if, and only if, R is an integral domain.

8. (5 pts.) Find, with brief justification, all ring homomorphisms from $\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$.

   φ is determined by the image of 1, i.e. by $\varphi(1) = a$. We must find all $a \in \mathbb{Z}/12\mathbb{Z}$ such that φ is a ring homomorphism. Moreover, $\varphi(1) = \varphi(1^2) = \varphi(1)^2 = \varphi(1) \Rightarrow a = a^2$ in $\mathbb{Z}/12\mathbb{Z}$, that is, a is an idempotent. $a \equiv a^2 \mod 12$

   Testing:

a	0	1	2	3	4	5	6	7	8	9	10	11
a^2	0	1	4	9	4	1	0	1	4	9	4	1
	↑	↑			↑					↑		

   Thus, $a = 0, 1, 4, 9$ give rise to well-defined ring homomorphisms.

9. (10 pts.) Suppose that A is an Abelian group of order $1323 = 3^3 \cdot 7^2$. Give the isomorphism classes for A in the table below. In the left hand column, give the elementary divisor decomposition and in the right hand column, give the invariant factor decomposition. **Groups on the same row should be isomorphic.** You do not need to show your work.

Elementary Divisor decomposition	Invariant Factor decomposition
$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_7$	$\mathbb{Z}_3 \times \mathbb{Z}_{21} \times \mathbb{Z}_{21}$
$\mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_7 \times \mathbb{Z}_7$	$\mathbb{Z}_{21} \times \mathbb{Z}_{63}$
$\mathbb{Z}_{27} \times \mathbb{Z}_7 \times \mathbb{Z}_7$	$\mathbb{Z}_7 \times \mathbb{Z}_{189}$
$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{49}$	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{147}$
$\mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_{49}$	$\mathbb{Z}_3 \times \mathbb{Z}_{441}$
$\mathbb{Z}_{27} \times \mathbb{Z}_{49}$	$\mathbb{Z}_{1323}$

10. (10 pts.) Consider the ring of Gaussian integers $\mathbb{Z}[i]$.

(a) (6 pts.) Prove that if $\alpha = a + bi$ for $a, b \in \mathbb{Z}$ is a Gaussian integer with $N(\alpha) = p$ for p a prime of $\mathbb{Z}$, then α is irreducible.

Suppose $\alpha = a+bi$ $a, b \in \mathbb{Z}$ and $N(\alpha) = p$ for p prime in $\mathbb{Z}$.

If $\alpha = \beta\gamma$ for $\beta, \gamma \in \mathbb{Z}[i]$, then $N(\alpha) = p = N(\gamma\beta) = N(\gamma)N(\beta)$ since N is multiplicative. Since p is prime, either $N(\gamma) = 1$ or $N(\beta) = 1$. Without loss of generality, assume $N(\gamma) = 1$. Then γ is a unit in $\mathbb{Z}[i]$ and we conclude α is an irreducible element of $\mathbb{Z}[i]$.

(b) (4 pts.) Give an example of a prime number $p \in \mathbb{Z}$ such that p is irreducible in $\mathbb{Z}[i]$. Justify your answer by stating an appropriate result.

Choose any $p \equiv 3 \mod 4$. For example, $p = 3$ (or 7 or 19)

Then p is <u>not</u> the sum of the squares of two integers so $\nexists\, \alpha \in \mathbb{Z}[i]$ with $N(\alpha) = 3$. Thus, if $3 = \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}[i]$, the norm of, without loss of generality, say α is 1, $N(\alpha) = 1$. Thus, 3 is irreducible in $\mathbb{Z}[i]$.

11. (10 pts.) Let G be a finite group of order 22, $|G| = 22$. Prove that G is either cyclic or isomorphic to the dihedral group D_{22}.

Proof: By Sylow's Theorem, the number of Sylow 2-subgroups $n_2 = 1$ or 11, and the number of Sylow 11-subgroups is $n_{11} = 1$. Since there is only one Sylow 11-subgroup P_{11}, it is a normal subgroup. Moreover, since $|P_{11}| = 11$ a prime, P_{11} is cyclic. Let y be a generator of P_{11}. Let $x \in G$ be a generator of a Sylow 2-subgroup of G. Then $|x| = 2$.

Conjugating y by x, we find $xyx^{-1} = y^i \in \langle y \rangle = P_{11}$.

Conjugating by x a second time, we find

$$x(xyx^{-1})x^{-1} = xy^ix^{-1}$$
$$\Rightarrow \quad x^2yx^{-2} = (xyx^{-1})^i$$
$$\Rightarrow \quad y = (y^i)^i. \quad \text{That is,} \quad y = y^{i^2} \quad (*).$$

It follows that $i^2 \equiv 1 \mod 11$ or, equivalently, $11 \mid i^2 - 1 = (i+1)(i-1)$.

Since 11 is prime, $11 \mid i+1$ or $11 \mid i-1$.

Suppose first that $11 \mid i-1$. Then $i \equiv 1 \mod 11$ and $xyx^{-1} = y$. That is, x and y commute. Moreover, since $P_{11} \trianglelefteq G$, $\langle x \rangle P_{11}$ is a subgroup of G with $|\langle x \rangle P_{11}| = \dfrac{2 \cdot 11}{|\langle x \rangle \cap \langle y \rangle|} = 22$ since $\langle x \rangle \cap \langle y \rangle = \{1\}$. Thus, ", $G = \langle x, y \rangle = \langle x \rangle P_{11}$ and G is Abelian since x and y commute. Since $(2, 11) = 1$, the element xy has order 22. Thus, G is cyclic.

Suppose now that $11 \mid i+1$ or, equivalently, that $i \equiv -1 \mod 11$. Then $xyx^{-1} = y^{-1}$ and $G = \langle x, y \mid |x| = 2, |y| = 11, xyx^{-1} = y^{-1} \rangle$ is a presentation for D_{22}. □

12. (10 pts.) Let D be a square-free integer, and consider the quadratic number field $\mathbb{Q}(\sqrt{D})$ and its subring of integers $\mathcal{O}$. Let $N : \mathbb{Q}(\sqrt{D}) \to \mathbb{Z}$ denote the field norm map which is multiplicative. The restriction of N to the ring of integers $\mathcal{O}$ will also denoted by N.

(a) (3 pts.) Prove that an element $\alpha \in \mathcal{O}$ is a unit if, and only if, $N(\alpha) = \pm 1$.

For $\alpha \in \mathcal{O}$, $\alpha = a + b\sqrt{D}$, $a, b \in \mathbb{Z}$, the norm is $N(\alpha) = a^2 - Db^2 \in \mathbb{Z}$.

For the equivalence above, if $\alpha \in \mathcal{O}$ is a unit with inverse $\alpha^{-1} \in \mathcal{O}$, then:

$1 = N(1) = N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1})$. Since both $N(\alpha), N(\alpha^{-1}) \in \mathbb{Z}$, $N(\alpha) = 1$ or -1.

Now assume $N(\alpha) = \pm 1$, then if $\beta = \frac{a - b\sqrt{D}}{N(\alpha)}$ we have $N(\alpha) = 1 = (a + b\sqrt{D})\frac{(a - b\sqrt{D})}{N(\alpha)}$

and $\beta = \frac{a - b\sqrt{D}}{N(\alpha)} = \alpha^{-1}$. □

(b) (3 pts.) When $D = -3$, the ring of integers is $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-3}}{2}\right)$. Find a unit in $\mathcal{O} \setminus \mathbb{Z}$.

For $\alpha \in \mathbb{Q}(\sqrt{D})$, the field norm is $N(\alpha) = q_1^2 + 3q_2^2$ where $\alpha = q_1 + q_2\sqrt{D}$ $q_1, q_2 \in \mathbb{Q}$.

Taking $\alpha = \frac{1}{2}(1 + \sqrt{-3}) \in \mathcal{O}$, the norm is $N\left(\frac{1}{2} + \frac{\sqrt{-3}}{2}\right) = \left(\frac{1}{2}\right)^2 + 3\left(\frac{1}{2}\right)^2 = 1$.

Thus, $\alpha \in \mathcal{O}^*$!

(c) (4 pts.) Let $D = -5$. Give, with proof, an example of an element $x = a + b\sqrt{-5}$ for $a, b \in Z$ such that x is irreducible, but x is not prime in $\mathbb{Z}[\sqrt{-5}]$.

Any of $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ would work. Let take $x = 3$.

Claim: $x = 3$ is irreducible:

Suppose $3 = \alpha\beta$ for $\alpha, \beta \in \mathcal{O} = \mathbb{Z}[\sqrt{-5}]$. Then $N(3) = 9 = N(\alpha)N(\beta)$ but there does not exist any $\gamma \in \mathcal{O}$ with $N(\gamma) = 3$ (i.e. $3 = a^2 + 5b^2$ has no integer solutions (a, b)). Thus, $N(\alpha)$ or $N(\beta) = 1$. Without loss of generality, assume $N(\beta) = 1$.

Then β is a unit and α is irreducible.

Similarly, there does not exist any integer solutions to $2 = a^2 + 5b^2$ and therefore 2 is irreducible. From these observations coupled with $N(1 \pm \sqrt{-5}) = 6 = 2 \cdot 3$, we see that $1 \pm \sqrt{-5}$ irreducible.

Finally, note that $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Thus, $2 \mid 6 = 2 \cdot 3$ but $2 \nmid (1+\sqrt{-5}), (1-\sqrt{-5})$

so 2 can not be prime in $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$.