Johns Hopkins University, Department of Mathematics
110.402 Abstract Algebra - Spring 2014
Midterm Exam–Solution

Instructions: This exam has 5 pages. No calculators, books or notes allowed. **You must answer the first 2 questions, and then answer one of question 3 or 4.** Do not answer both. No extra points will be rewarded. Place an "X" through the question you are not going to answer. Be sure to show all work for all problems. No credit will be given for answers without work shown.
If you do not have enough room in the space provided you may use additional paper provided by the instructor. Be sure to clearly label each problem and attach them to the exam.

You have 50 MINUTES.

Academic Honesty Certification

I certify that I have taken this exam with out the aid of unauthorized people or objects.

Signature: ______________________________ Date: ____________________

Name: ______________________________

Problem	Score
1	
2	
3 or 4	
Total	

1. (30 points) Consider the ring $R = \mathbb{Z}[\sqrt{3}] := \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$.

a) Which of the following elements of R are units?

$$5 + 3\sqrt{3}, \quad 2 - \sqrt{3}, \quad 1 + \sqrt{3}, \quad 7 + 4\sqrt{3}.$$

b) Does the following equality of ideals hold in R?

$$(5 + 3\sqrt{3}) = (1 + \sqrt{3}).$$

Motivate the answer.

c) Is $(3 + \sqrt{3})$ a prime ideal in R? Motivate the answer.

d) Find, if exists, the G.C.D.$(1 + 3\sqrt{3},\ 5 + \sqrt{3})$ (up-to associates).
[G.C.D.= greatest common divisor].

e) Determine a maximal ideal $\mathfrak{M} \subset \mathbb{Z}[X]$ such that $X^2 - 3 \in \mathfrak{M}$.

<u>Solution</u>: a) We apply the norm map $N : R \to \mathbb{Z}$ to test which elements in the list have norm ± 1, where $N(a + b\sqrt{3}) := (a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2$.
$N(5 + 3\sqrt{3}) = -2$, $N(2 - \sqrt{3}) = 1$, $N(1 + \sqrt{3}) = -2$, $N(7 + 4\sqrt{3}) = 1$. We conclude that the second and fourth elements in the list are units, the others are not.

b) Yes, the equality holds since the elements $5 + 3\sqrt{3}$ and $1 + \sqrt{3}$ are associates. More precisely:

$$1 + \sqrt{3} = (2 - \sqrt{3})(5 + 3\sqrt{3})$$

and we know from a) that $2 - \sqrt{3} \in R^\times$.

c) No, $(3 + \sqrt{3})$ is not a prime ideal in R. $N(3 + \sqrt{3}) = 6$. We know that if π is a prime element in R, then $(\pi) \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, hence $(\pi) \cap \mathbb{Z} = p\mathbb{Z}$, for some prime number $p \in \mathbb{Z}$. Then the inclusion $p \in (\pi)$ shows that $p = \pi\pi'$ in R, and so $p^2 = N(p) = N(\pi)N(\pi')$. Since π is not a unit in R, $N(\pi) \neq \pm 1$, and it follows that $p|N(\pi)|p^2$ in $\mathbb{Z}$. Since 6 is neither a prime nor the square of a prime in $\mathbb{Z}$, $(3 + \sqrt{3})$ cannot be a prime ideal in R.

d) R is an Euclidean domain, thus the GCD of any pair of elements in R exists and it is unique up-to associates. One notices that $N(1+3\sqrt{3}) = -2{\cdot}13$ and $N(5+\sqrt{3}) = 2{\cdot}11$. Thus $\mathrm{GCD}(1+3\sqrt{3}, 5+\sqrt{3}) = a + b\sqrt{3}$ with $N(a + b\sqrt{3}) = a^2 - 3b^2 = \pm 2$. We know from a) that $N(5 + 3\sqrt{3}) = -2$. Thus, up-to associates, $5 + 3\sqrt{3} = GCD(1 + 3\sqrt{3}, 5 + \sqrt{3})$.

e) A possible example of maximal ideal $\mathfrak{M} \subset \mathbb{Z}[X]$ such that $X^2 - 3 \in \mathfrak{M}$ is $\mathfrak{M} = (X + 1, X^2 - 3)$. In fact, by applying the third isomorphism theorem we find that $\mathbb{Z}[X]/\mathfrak{M} \simeq \mathbb{Z}/2\mathbb{Z}$ is a field. Alternatively, we can choose $\mathfrak{M} = (X^2 - 3, p)$, where $p \in \mathbb{Z}$ is a prime number such that $X^2 - 3 \in (\mathbb{Z}/p\mathbb{Z})[X]$ is an irreducible polynomial, e.g. $p = 5$.

2. [30 points] Consider the ring $R = \mathbb{Z}[X]/(X^4 + 3X^3 + 1)$.

a) Is $(\bar{2})$ a maximal ideal in R? Explain. $(\bar{2} = 2 + (X^4 + 3X^3 + 1) \in R)$

b) Is R an integral domain? Is R a field? Explain.

c) Does R have any further unit besides ±1? If yes, give an example of such unit.

Solution: a) Yes, it is so. In fact, by applying the thrid isomorphism theorem we find $R/(\bar{2}) \simeq \mathbb{Z}[X]/(2, X^4 + 3X^3 + 1) \simeq (\mathbb{Z}/2\mathbb{Z})[X]/(X^4 + X^3 + 1)$ and this latter ring is a field since $q(X) = X^4 + X^3 + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$ is an irreducible polynomial. In fact $q(\bar{1}) \neq 0$ and $q(X)$ is not the product of the unique irreducible polynomial $X^2 + X + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$.

(b) R is an integral domain but is not a field. R is not a field since by a) $(\bar{0}) \neq (\bar{2}) \subset R$ is a maximal ideal of R. To show that R is an integral domain it suffices to prove (since $\mathbb{Z}[X]$ is UFD) that $X^4 + 3X^3 + 1$ is an irredubible polynomial in $\mathbb{Z}[X]$. By applying the modular irreducibility test with $p = 2$, we find from a) that $X^4 + 3X^3 + 1$ is irreducible in $\mathbb{Q}[X]$, thus has no proper factorization in $\mathbb{Z}[X]$ and in fact not even an improper factorization is possible for $X^4 + 3X^3 + 1 \in \mathbb{Z}[X]$. Thus $X^4 + 3X^3 + 1$ is irreducible in $\mathbb{Z}[X]$.

(c) Yes, an example of a unit in R is: $X^3 + 3X^2 + (X^4 + 3X^3 + 1)$: in fact the equation $X^4 + 3X^3 + 1 = X(X^3 + 3X^2) + 1$ holds in $\mathbb{Z}[X]$. This implies that both $X + (X^4 + 3X^3 + 1)$ and $X^3 + 3X^2 + (X^4 + 3X^3 + 1)$ are units in R.

3. (20 points) (**ANSWER THIS QUESTION OR 4.**)

Let R be a commutative ring with identity and let $I \subset R$ be a proper ideal. Prove or disprove:

$$R/I \text{ free } R\text{-module} \Longrightarrow I = (0)$$

Solution: The statement is true. In fact, since I is a proper ideal, R/I has non-zero elements. Suppose R/I is a free R-module, then R/I has a non-empty R-basis, and this basis contains at least one linearly independent element $x + I$, $x \in R \setminus I$. Let $i \in I$. Then $i(x + I) = ix + I = I$ since I is an ideal and $ix \in I$. I is the zero element in R/I and since $x + I$ is R-linearly independent we must have $i = 0$. Therefore $I = (0)$.

4. (20 points) (**ANSWER THIS QUESTION OR 3.**)

Prove or disprove (X = indeterminate):

(a) $\mathbb{C}$ and $\mathbb{R} \oplus \mathbb{R}$ are isomorphic as $\mathbb{Z}$-modules and as rings.

(b) $\mathbb{Q}[X]/(X^2 - X - 1)$ and $\mathbb{Q}[X]/(X^2 - 1)$ are isomorphic as rings and as $\mathbb{Q}$-vector spaces.

Solution: (a) $\mathbb{C}$ and $\mathbb{R} \oplus \mathbb{R}$ are isomorphic as abelian groups (*i.e.* as $\mathbb{Z}$-modules) in fact $\varphi : \mathbb{C} \to \mathbb{R} \oplus \mathbb{R}$, $\varphi(a + bi) = (a, b)$ is a well-defined group isomorphism. On the other hand, $\mathbb{C}$ and $\mathbb{R} \oplus \mathbb{R}$ are not isomorphic as rings: the former being an integral domain (in fact a field) but not the latter: $(1, 0) \cdot (0, 1) = (0, 0)$.

(b) $\mathbb{Q}[X]/(X^2 - X - 1)$ and $\mathbb{Q}[X]/(X^2 - 1)$ are isomorphic as $\mathbb{Q}$-vector spaces (of rank 2): a $\mathbb{Q}$-vector space isomorphism is given by mapping: $1 + (X^2 - X - 1) \mapsto 1 + (X^2 - 1)$ and $X + (X^2 - X - 1) \mapsto X + (X^2 - 1)$. Then, one extends it by linearity. However they are not isomorphic as rings since the former is a field (in fact isomorphic to the field $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} | a, b \in \mathbb{Q}\}$) as $X^2 - X - 1$ is an irreducible polynomial in $\mathbb{Q}[X]$ (one may apply the modular irreducibility test with $p = 2$), whereas the latter is not even an integral domain as $X \pm 1 + (X^2 - 1)$ are zero-divisors in the ring.