Johns Hopkins University, Department of Mathematics
110.402 Abstract Algebra - Spring 2014
Midterm (makeup) Exam

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 of Gaussian integers $R = \mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$, $\quad (i := \sqrt{-1} \in \mathbb{C})$.

   a) Give an explicit description of the set $H := R/(2)$ of classes of elements of R mod. (2) $((2) \subset R)$, in terms of polynomials in one variable of a precise type. Also, determine the cardinality of the set H.

   b) Is H a commutative ring with unit? Explain your answer.

   c) Is H an integral domain? Explain your answer.

   d) Is H a field? Explain your answer.

NOTE: No partial credit will be assigned to answers reporting only yes or no.

Solution: a) The ring R is isomorphic to the factor ring $\mathbb{Z}[X]/(X^2 + 1)$ (X = indeterminate): an isomorphism is provided by applying the First Isomorphism Theorem to the (surjective) homomorphism of rings $\varphi : \mathbb{Z}[X] \to \mathbb{Z}[i]$, $\varphi(1) = 1$, $\varphi(X) = i$, $\mathrm{Ker}(\varphi) = (X^2 + 1)$. By applying the Third Isomorphism Theorem we obtain

$$H = R/(2) \simeq \mathbb{Z}[X]/(2, X^2 + 1) \simeq (\mathbb{Z}/2\mathbb{Z})[X]/(X^2 + 1) = \mathbb{Z}_2[X]/((X + 1)^2).$$

Thus H consists of the classes of linear polynomials in X with coefficients in the field $\mathbb{Z}_2$, hence $|H| = 4 = \mathrm{Nr}(2)$, where $\mathrm{Nr} : \mathbb{Z}[i] \to \mathbb{Z}$ is the norm map.

b) H is a commutative ring with unit since H is the quotient ring of R = commutative ring with unit.

c) Note that H is a factor ring obtained factoring $\mathbb{Z}_2[X]$ with the principal ideal generated by the reducible polynomial $X^2 + 1 = (X + 1)^2$ (in $\mathbb{Z}_2[X]$). In particular $X + 1 \in H$ is a zero divisor, thus H is not an integral domain.

d) Since H is not an integral domain, it cannot be a field.

2. [30 points] Consider the ring $\mathbb{Q}(\sqrt{17}) := \{a + b\sqrt{17} | a, b \in \mathbb{Q}\}$.

a) Is $\mathbb{Q}(\sqrt{17})$ a field? Explain your answer.

b) Determine a proper ideal $I \subset \mathbb{Q}[X]$ ($X =$ variable) and an isomorphism of rings:

$$\mathbb{Q}[X]/I \xrightarrow[\sim]{\varphi} \mathbb{Q}(\sqrt{17}).$$

Explicitly define the isomorphism φ. Is I a prime ideal? Explain your answer.

c) Show that the ideal I as in b) is a principal ideal $I = (f(X))$, for some $f(X) \in \mathbb{Q}[X]$. Is $f(X) \in \mathbb{Z}[X]$ irreducible? Explain your answer.

NOTE: No partial credit will be assigned to answers reporting only yes or no.

Solution: a)+b)+c) $\mathbb{Q}(\sqrt{17})$ is a field: it is the field of fractions of the integral domain $\mathbb{Z}[\sqrt{17}]$. Alternatively, one can say that the ring homomorphism

$$\varphi : \mathbb{Q}[X] \to \mathbb{Q}(\sqrt{17}), \qquad \varphi(1) = 1,\ \varphi(X) = \sqrt{17}$$

is clearly surjective and by applying the First Isomorphism Theorem one deduces that $\mathbb{Q}[X]/(X^2+17) \simeq \mathbb{Q}(\sqrt{17})$. The polynomial $f(X) = X^2 + 17 \in \mathbb{Z}[X]$ is irreducible and Gauss' Lemma implies that the polynomial is also irreducible over $\mathbb{Q}$. Since $\mathbb{Q}[X]$ is a PID it follows that the ideal $I = (X^2 + 17)$ is prime and maximal in $\mathbb{Q}[X]$, hence $\mathbb{Q}(\sqrt{17})$ is a field.

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

Give a proof or disprove the following statement:

$$\mathbb{Z}[\sqrt{-3}] \quad \text{is an Euclidean domain}$$

NOTE: No partial credit will be assigned to answers reporting only yes or no.

Solution: In $\mathbb{Z}[\sqrt{-3}]$ the element 4 factors in two different ways as a product of irreducible elements: $4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{3})$. More precisely: $2 \in \mathbb{Z}[\sqrt{-3}]$ is an irreducible element since otherwise a proper factorization $2 = x \cdot y$, with $x, y \in \mathbb{Z}[\sqrt{-3}]$ would imply, by applying the norm map that $\mathrm{Nr}(2) = 4 = (a^2+3b^2)(a_1^2+3b_1^2)$, where $\mathrm{Nr}(x) = a^2+3b^2$ and $\mathrm{Nr}(y) = a_1^2+3b_1^2$. Then, one would get $a^2+3b^2 = 2 = a_1^2+3b_1^2$ which is impossible since $a, b, a_1, b_1 \in \mathbb{Z}$. Similarly one shows that $1 \pm \sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ are irreducible elements. Then, $\mathbb{Z}[\sqrt{-3}]$ is not UFD and hence it cannot be Euclidean.

4. [20 points] (**ANSWER THIS QUESTION 3.**)

(a) Which of the following $\mathbb{Z}$-modules is free?

$$(\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}, \qquad \mathbb{Q}/\mathbb{Z}.$$

(b) Consider $\mathbb{Q}$ as a $\mathbb{Z}$-module: are $\frac{2}{3}$ and $\frac{3}{2}$ linearly independent elements in $\mathbb{Q}$? Is $\mathbb{Q}$ a finitely generated $\mathbb{Z}$-module? Explain your answers.

NOTE: No partial credit will be assigned to answers reporting only yes or no.

Solution: a) $(\mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}$ is not free as it contains the torsion sub-$\mathbb{Z}$-module $\mathbb{Z}_2$. Also $\mathbb{Q}/\mathbb{Z} = \{q + \mathbb{Z} | q \in \mathbb{Q}\}$ is not free as every element in it has finite order.

b) $\frac{2}{3}$ and $\frac{3}{2}$ are not linearly independent elements in $\mathbb{Q}$ since $9\frac{2}{3} - 4\frac{3}{2} = 0$. $\mathbb{Q}$ is not finitely generated as abelian group, since if it were so it would necessarily be a cyclic group (since any two different rational numbers are always linearly dependent) and generated by some $q = \frac{r}{s}$, but then $\frac{1}{s+1}$ cannot be written as kq, for some $k \in \mathbb{Z}$.