THE JOHNS HOPKINS UNIVERSITY
Faculty of Arts and Sciences
FINAL EXAM - FALL SESSION 2006
110.401 - ADVANCED ALGEBRA I.

Examiner: Professor C. Consani
Duration: take home final.

No calculators allowed. Total Marks = 100

SOLUTIONS
1. [10 marks] Consider the ring of the Gaussian integers \( \mathbb{Z}[i] \) (\( i = \sqrt{-1} \)).

(a) Is \( 4 + i \) a prime element in \( \mathbb{Z}[i] \)?

(b) Compute the cardinality of \( \mathbb{Z}[i]/(4 + i) \). What group is it?

(c) Find the G.C.D.(1 + 3i, 5 + i).

**Sol.**

(a) \( N(4 + i) = 4^2 + 1^2 = 17 \) is a prime number in \( \mathbb{Z} \), and so \( 4 + i \) is an irreducible element of \( \mathbb{Z}[i] \). Moreover, \( \mathbb{Z}[i] \) is a Euclidean domain, and so every irreducible element is also a prime element. Therefore \( 4 + i \) is a prime element in \( \mathbb{Z}[i] \).

(b) The cardinality of \( R = \mathbb{Z}[i]/(4 + i) \) is precisely \( N(4 + i) = 17 \). Let \( I = (4 + X) \). By the third isomorphism theorem we have: \( \mathbb{Z}[X]/(X^2 + 1, 4 + X) \cong \mathbb{Z}[X]/I/(X^2 + 1, 4 + X)/I \cong \mathbb{Z}/17\mathbb{Z} \), where the last isomorphism is obtained by noticing that \( X^2 + 1 = -(4 + X)(4 - X) + 17 \) in \( \mathbb{Z}[X] \), so that \( X^2 + 1 = 17 \) in \( \mathbb{Z}[X]/I \). It follows that \( R \) is the cyclic group of order 17.

(c) We apply the division algorithm in \( \mathbb{Z}[i] \):

\[
\frac{5 + i}{1 + 3i} = \frac{4}{5} - \frac{7}{5}i
\]

and so we choose the approximate quotient \( 1 - i \), to get

\[
5 + i - (1 - i)(1 + 3i) = 1 - i
\]

Therefore

\[
5 + i = (1 - i)(1 + 3i) + 1 - i
\]

where \( N(1 - i) = 2 < N(1 + 3i) = 10 \). Now we repeat the process with \( 1 + 3i \) and \( 1 - i \):

\[
\frac{1 + 3i}{1 - i} = -1 + 2i
\]

and so

\[
1 + 3i = (-1 + 2i)(1 - i)
\]

and the division algorithm ends. The algorithm tells us that GCD(5+i, 1+3i) = 1−i.
2. [20 marks] Give a proof or disprove the following statement:

\( \mathbb{Z}[\sqrt{-3}] \) is an Euclidean domain.

**Sol.** \( \mathcal{O} = \mathbb{Z}[\frac{1 + \sqrt{-3}}{2}] \) is a Euclidean domain, but \( \mathbb{Z}[\sqrt{-3}] \) is a proper subring, so we may have some doubts that the division algorithm of \( \mathcal{O} \) when applied in \( \mathbb{Z}[\sqrt{-3}] \) holds within \( \mathbb{Z}[\sqrt{-3}] \). Similarly we may have some reasonable doubts that the unique factorization in \( \mathbb{Z}[\sqrt{-3}] \) holds, although \( \mathcal{O} \) is a UFD, and so we turn our attention to the possibility of finding an element of \( \mathbb{Z}[\sqrt{-3}] \) with non-unique factorization.

We search for possible candidates among elements of \( \mathbb{Z}[\sqrt{-3}] \) with small norm, the norm itself providing a means to discover possible factorizations. By trying out \( N(a + bi) = a^2 + 3b^2 \) for different small integer values of \( a \) and \( b \), we soon find that \( 4 = 1^2 + 3 \cdot 1^2 = 2^2 + 3 \cdot 0^2 \). So \( 4 = (1 + i\sqrt{3})(1 - i\sqrt{3}) = 2^2 \).

If \( \alpha \in \mathbb{Z}[\sqrt{-3}] \) is a unit, then there is a \( \beta \in \mathbb{Z}[\sqrt{-3}] \) such that \( \alpha \beta = 1 \), and so \( N(\alpha)N(\beta) = 1 \), which shows that \( N(\alpha) = 1 \). Conversely, if \( N(\alpha) = 1 \), since \( N(\alpha) = \alpha \bar{\alpha} \) we see that \( \alpha \) is a unit in \( \mathbb{Z}[\sqrt{-3}] \). Since the only integer solutions to \( a^2 + 3b^2 = 1 \) are \( a = \pm 1, b = 0 \), the units of \( \mathbb{Z}[\sqrt{-3}] \) are \( \pm 1 \). If \( 2 = \alpha \beta \) in \( \mathbb{Z}[\sqrt{-3}] \) then \( 4 = N(2) = N(\alpha)N(\beta) \). \( N(\alpha) = N(\beta) = 2 \) is impossible, since no element of \( \mathbb{Z}[\sqrt{-3}] \) has norm 2. So without loss we have \( N(\alpha) = 4 \), \( N(\beta) = 1 \) so \( \beta \) is a unit and hence 2 is irreducible in \( \mathbb{Z}[\sqrt{-3}] \). A similar argument shows that both \( 1 \pm i\sqrt{3} \) are irreducible since \( N(1 \pm i\sqrt{3}) = 4 \) also. Therefore 4 has two factorizations into irreducibles in \( \mathbb{Z}[\sqrt{-3}] \) which are clearly not associate, and thus \( \mathbb{Z}[\sqrt{-3}] \) is not a UFD, so also not a Euclidean domain.
3. [10 marks] Consider the domain \( R = \mathbb{Z}[\sqrt{3}] := \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\} \).

(a) Which among the following elements of \( R \) are invertible and why?

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

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

\[
(5 + 3\sqrt{3}) = (1 + \sqrt{3})
\]

Explain in details your answer.

(c) Is \((3 + \sqrt{3})\) a prime ideal of \( R \)? Explain in details.

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

**Sol.**

(a) We need only compute norms to see which elements in the list have norm ±1, where \( N(a + b\sqrt{3}) = a^2 - 3b^2 \). \( N(5 + 3\sqrt{3}) = -2, \) \( N(2 - \sqrt{3}) = 1, \) \( N(1 + \sqrt{3}) = -2, \) \( N(7 + 4\sqrt{3}) = 1 \). So the second and fourth elements in the list are units, the others are not.

(b) Yes, the equality holds since \( 5 + 3\sqrt{3} \) and \( 1 + \sqrt{3} \) are associates by part (a) of this exercise: \( 1 + \sqrt{3} = (2 - \sqrt{3})(5 + 3\sqrt{3}) \).

(c) No it is not a prime ideal. \( N(3 + \sqrt{3}) = 6 \). If \( \pi \) is a prime element in \( R \), then \( (\pi) \cap \mathbb{Z} \) is a prime ideal of \( \mathbb{Z} \), hence is \( p\mathbb{Z} \) for some prime \( p \in \mathbb{Z} \). Then \( p \in (\pi) \) shows that \( p = \pi \pi' \) in \( R \), and so \( p^2 = N(p) = N(\pi)N(\pi') \). Since \( \pi \) is not a unit in \( R \), \( N(\pi) \neq \pm 1 \), and it follows that \( p \mid N(\pi) \mid p^2 \) in integers. Since 6 is not a prime or the square of a prime (up to sign) in \( \mathbb{Z} \), \((3 + \sqrt{3})\) is not a prime ideal in \( R \).

(d) We consider the following ideal of \( \mathbb{Z}[X] \): \( \mathfrak{M} = (X + 1) + (X^2 - 3) = (X + 1, X^2 - 3) \). We have

\[
\frac{\mathbb{Z}[X]}{\mathfrak{M}} \cong \frac{\mathbb{Z}[X]}{(X+1)} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \cong \mathbb{F}_2
\]

by the third isomorphism theorem. Now \( \mathbb{Z}[X]/(X + 1) \cong \mathbb{Z} \) via the evaluation map \( X \mapsto -1 \), and under this isomorphism, the ideal \( \mathfrak{M}/(X + 1) \) corresponds to the ideal \( 2\mathbb{Z} \). Hence

\[
\frac{\mathbb{Z}[X]}{\mathfrak{M}/(X+1)} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \cong \mathbb{F}_2
\]

and therefore \( \mathfrak{M} \) is indeed a maximal ideal in \( \mathbb{Z}[X] \).

Why did we pick \( \mathfrak{M} \) as we did? Since \( \mathbb{Z}[X]/(X^2 - 3) \cong \mathbb{Z}[\sqrt{3}] \) via the evaluation map \( X \mapsto \sqrt{3} \), the fourth isomorphism theorem tells us that the ideals of \( \mathbb{Z}[X] \) containing \((X^2 - 3)\) are in one-to-one correspondence with the ideals of \( \mathbb{Z}[\sqrt{3}] \), and in particular that maximal ideals correspond to maximal ideals. The third isomorphism theorem tells us also that for any ideal \( I \) of \( \mathbb{Z}[X] \) containing \((X^2 - 3)\) we have

\[
\frac{\mathbb{Z}[X]}{I} \cong \frac{\mathbb{Z}[X]/(X^2 - 3)}{I/(X^2 - 3)} \cong \frac{\mathbb{Z}[\sqrt{3}]}{I}
\]

where \( \bar{I} \) is the ideal of \( \mathbb{Z}[\sqrt{3}] \) corresponding to \( I \) under the isomorphism induced by evaluation at \( \sqrt{3} \) described above. We don’t need to know whether \( \mathbb{Z}[\sqrt{3}] \) is a Euclidean domain, or a PID or even a UFD. But we do know by part (a) that \( 1 + \sqrt{3} \) is an irreducible factor of 2 in \( \mathbb{Z}[\sqrt{3}] \), and this makes it a good candidate, since a
first guess to form a maximal ideal of \( \mathbb{Z}[X] \) containing \((X^2 - 3)\) is simply to add in a prime element of \( \mathbb{Z} \), forming for example \((2, X^2 - 3)\). (Note however that this ideal is not maximal, and in fact is not even prime, in \( \mathbb{Z}[X] \). Arguments similar to the isomorphism arguments above show that \( \mathbb{Z}[X]/(2, X^2 - 3) \cong \mathbb{F}_2[X]/(X + 1)^2 \), or also similarly, that \( \mathbb{Z}[X]/(2, X^2 - 3) \cong \mathbb{F}_2[\sqrt{3}] \), which is not an integral domain since \( (1 + \sqrt{3})^2 = 4 + 2\sqrt{3} = 0 \mod 2 \).) Since 2 does not remain prime in \( \mathbb{Z}[\sqrt{3}] \) we instead choose a (hopefully) prime (but certainly irreducible) factor of 2 such as \( 1 + \sqrt{3} \), and consider the pre-image of the ideal \( (1 + \sqrt{3}) \) in \( \mathbb{Z}[X] \) under the evaluation map \( X \mapsto \sqrt{3} \), which is precisely \( \mathfrak{M} \). (\( \mathfrak{M} = (1 + \sqrt{3}) \) in the notation above.) That’s how we came upon our particular \( \mathfrak{M} \) as a candidate. (Note also that maximality of \( \mathfrak{M} \) shows that \( (1 + \sqrt{3}) \) is a maximal ideal of \( \mathbb{Z}[\sqrt{3}] \), and hence \( 1 + \sqrt{3} \) is a prime factor of 2.)

Given the discussion above, we could also try to choose an integer prime \( p \) which remains prime in \( \mathbb{Z}[\sqrt{3}] \). Say we have a prime \( p \in \mathbb{Z} \) which remains prime in \( \mathbb{Z}[\sqrt{3}] \). This occurs if and only if the reduction of \( X^2 - 3 \) modulo \( p \) is irreducible in \( \mathbb{F}_p[X] \). Let \( \mathfrak{M} = (p, X^2 - 3) \). Then

\[
\mathbb{Z}[X]/\mathfrak{M} \cong \frac{\mathbb{Z}[X]}{(p, X^2 - 3)} \cong \frac{\mathbb{F}_p[X]}{(X^2 - 3)}
\]

since the homomorphism “reduction of coefficients modulo \( p \)” which induces the isomorphism \( \mathbb{Z}[X]/p\mathbb{Z}[X] \cong (\mathbb{Z}/p\mathbb{Z})[X] \cong \mathbb{F}_p[X] \) takes \( \mathfrak{M} \) to the ideal \( (X^2 - 3) \) of \( \mathbb{F}_p[X] \), where the bar indicates reduction modulo \( p \). But since \( p \) remains prime in \( \mathbb{Z}[\sqrt{3}] \), \( X^2 - 3 \) is irreducible and hence prime in \( \mathbb{F}_p[X] \), so the ideal \( (X^2 - 3) \) is prime and hence maximal in the PID \( \mathbb{F}_p[X] \). Therefore \( \mathbb{Z}[X]/\mathfrak{M} \) is a field and \( \mathfrak{M} \) is a maximal ideal. To find a particular \( p \) in order to answer the question, we note that we have already seen that \( 2 \) does not remain irreducible in \( \mathbb{Z}[\sqrt{3}] \), and obviously \( 3 \) becomes reducible also. However the reduction of \( X^2 - 3 \mod 5 \) remains irreducible in \( \mathbb{F}_5[X] \) and so \( 5 \) is prime in \( \mathbb{Z}[\sqrt{3}] \). It follows that taking \( \mathfrak{M} = (5, X^2 - 3) \) would also work.
4. [5 marks] Do the equations

\[3X - 10Y = 2, \quad 2X + 6Y = 5\]

have solutions in \(\mathbb{Z}\)? If yes, determine for each equation a complete set of solutions.

**Sol.** \(2X + 6Y = 5\) certainly has no solutions in \(\mathbb{Z}\) since the left hand side of the equation is always even, the right hand side is odd. (A more formal way of saying this is that 5 is not a multiple of the GCD of 2 and 6, which is 2.)

Since the GCD of 3 and 10 is 1, by the division algorithm in \(\mathbb{Z}\) there exist integers \(A\) and \(B\) such that \(3A + 10B = 1\), and then certainly \(3(2A) + 10(2B) = 2\), so the first equation has solutions in \(\mathbb{Z}\). In particular one solution (found by observation) to \(3X - 10Y = 2\) is given by \(X_0 = 14, Y_0 = 4\). But then given this one particular solution we may find all solutions:

\[X = X_0 + m \frac{-10}{(3,10)} = 14 - 10m\]
\[Y = Y_0 - m \frac{3}{(3,10)} = 4 - 3m\]

for any \(m \in \mathbb{Z}\).
5. [10 marks] Consider the quotient ring $R = \mathbb{Z}[X]/(X^4 + 3X^3 + 1)$.

(a) Is $(\overline{2}) \subset R$ a maximal ideal of $R$? Why?

(b) Is $R$ a domain? Is $R$ a field? Explain.

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

**Sol.** (a) Yes it is a maximal ideal. Let $p(X) = X^4 + 3X^3 + 1$, $I = p(X)\mathbb{Z}[X] = (x^4 + 3x^3 + 1)$. We have $(2) = (2\mathbb{Z}[X] + I)/I$, and the third isomorphism theorem yields

$$\frac{\mathbb{Z}[X]}{I} \cong \frac{\mathbb{Z}[X]}{2\mathbb{Z}[X]+I} \cong \frac{\mathbb{Z}[X]}{2\mathbb{Z}[X]+I} \cong \frac{\mathbb{F}_2[X]}{(X^4 + X^3 + 1)}$$

where the last isomorphism is induced by reduction of coefficients modulo 2, which sends $p(X)$ to $q(X) = X^4 + X^3 + 1$. Now $q(X)$ has no roots in $\mathbb{F}_2$, so has no linear factors. Suppose $q(X) = (X^2 + aX + b)(X^2 + cX + d)$ factors into quadratics over $\mathbb{F}_2$, with $a, b, c, d \in \mathbb{F}_2$. Multiplying out, we find $q(X) = X^4 + (a+c)X^3 + (b+d+ac)X^2 + (bc + ad)X + bd$. Comparing coefficients we see $bd = 1 \Rightarrow b = d = 1$ and $a + c = 1 \Rightarrow a = 1, c = 0$, without loss of generality. But then $0 = bc + ad = 1$, a contradiction, and so $q(X)$ is irreducible over $\mathbb{F}_2$. Since $q(X)$ is irreducible, $\mathbb{F}_2[X]/(q(X))$ is a field, which proves that $(\overline{2})$ is a maximal ideal in $R$.

(b) $R$ is a domain but not a field. Since $q(X)$ is the reduction of $p(X)$ modulo 2 and $q(X)$ is irreducible in $\mathbb{F}_2[X]$, this proves that $p(X)$ is irreducible in $\mathbb{Z}[X]$. Since $\mathbb{Z}[X]$ is a UFD, $I$ is a prime ideal and so $R = \mathbb{Z}[X]/I$ is a domain. $(\overline{2})$ is a nonzero maximal ideal in $R$, hence $R$ cannot be a field. (The only ideals of a field are the zero ideal and the field itself.)

(c) Yes, $R$ has units besides $\pm 1$. For example,

$$(X^3 + 3X^2 + 1)(-X + I) = -X^4 - 3X^3 + I$$

$$= -X^4 - 3X^3 + p(X) + I = 1 + I$$

so $-X + I$ is a unit in $R$ which is not equal to $\pm 1 + I$, since $-X \pm 1 \notin I$. 
6. [15 marks] Let $H$ be a subgroup of a group $G$ and write

$$Cl(H) = \{g^{-1}Hg : g \in G\}$$

for the conjugacy class of $H$ in $G$. Show that

$$|Cl(H)| = |G : N_G(H)|$$

($N_G(H)$ = the normalizer of $H$ in $G$).

Assume that $G$ is a finite group and prove that $G$ cannot be the set-union of its conjugate subgroups ($\neq G$).

**Sol.** The group $G$ acts on the set of its subgroups by conjugation. The orbit of $H$ under this action is exactly $Cl(H)$. If $G$ is finite, we know that $|Orb(H)| = |G|/|Stab(H)|$. The stabilizer of $H$ is $N_G(H)$. Therefore, $|Cl(H)| = |G : N_G(H)|$. If $G$ is infinite, one can always argue that the map of sets

$$Cl(H) \rightarrow \{gN_G(H) | g \in G\}, \quad T = g_1Hg_1^{-1} \mapsto g_1N_G(G)$$

is (well defined) and bijective.

Now, consider $H < G$ (i.e. a proper subgroup of $G$). Call $|G : H| = h$ (note that $h > 1$). Because $H < N_G(H)$, it follows that $|G : N_G(H)| \leq h$. Therefore, $H$ has a most $h$ conjugate subgroups. All together they contain at most

$$(|H| - 1)h + 1 = |G| - (h - 1) < |G|$$

elements.
7. [10 marks] Show that a group $G$ cannot be described as a product of two conjugate subgroups different from $G$.

**Sol.** We prove the contrapositive. Suppose $G = HgHg^{-1}$ for some $H \leq G$ and $g \in G$. Since multiplication on the right by $g$ is a bijection of $G$ with itself, we have $G = Gg = HgHg^{-1}g = HgH$. Then we must have $1 = hgh'$ for some $h, h' \in H$, and so $g = h^{-1}h'^{-1} \in H$. Hence $gHg^{-1} = H$, and so $G = H^2 = H$. 
8. [20 marks] Show that if a group $G$ has two normal, proper, distinct subgroups $H$, $K$ of index $p > 1$, $p$ prime number, s.t. $H \cap K = \{1\}$, then:

$|G| = p^2$ and $G$ is not cyclic.

**Sol.** Let $H$ and $K$ be two distinct subgroups satisfying the hypothesis. Then neither subgroup can contain the other, since in that case the contained subgroup would then have index strictly greater than $p$. We have

$|G| = |G : \{1\}| = |G : H \cap K| < \infty$

since both indexes $|G : H|$ and $|G : K|$ are finite. Thus $G$ cannot be cyclic, since $|H| = |G|/|G : H| = |G|/|G : K| = |K|$, and cyclic groups have unique subgroups of any given (allowable) order.

Since $K$ is a normal subgroup of $G$, $HK = KH$ is a subgroup and $H < G = N_G(K)$, so we can apply the second isomorphism theorem to conclude that $H/(H \cap K) \cong HK/K$. Now $K \leq HK \leq G$, and since $K$ is normal in $G$, $HK/K \leq G/K$. Moreover, $|G/K| = p$ is prime, so either $HK/K = \{K\}$ (the trivial group in $G/K$) and hence $HK = K$, or $HK/K = G/K$ and hence $HK = G$ (by the fourth isomorphism theorem, if you like).

If $HK = K$ then we have $H \leq HK = K$, which we have already noted is not possible; hence $HK = G$. Since $H \cap K = \{1\}$ we find that $H$ is isomorphic to $G/K$, so $|H| = p$. But then $|G| = |G||H|/|H| = |G : H||H| = p^2$.

Note that without the assumption that $H$ and $K$ are distinct subgroups there is a counterexample to the question as literally stated: take $G = \mathbb{Z}/p\mathbb{Z}$ and $H = K = \{1\}$. Then $|G| = p$ and $G$ is cyclic.