George M. Bergman
3108 Etcheverry Hall

Fall 2001, Math 113, Sec. 3
Final Exam

12 Dec., 2001
12:30-3:30

1. (20 points, 4 points each.) Find the following.

(a) $(1,2,3,4)^{30}$ in S_5.

(b) The product $[a+bx][c+dx]$ in the field $\mathbf{Q}[x]/\langle x^2-x-1\rangle$, where $a, b, c, d \in \mathbf{Q}$. The answer should be given in the form $[p+qx]$ with $p, q \in \mathbf{Q}$.

(c) A nonzero polynomial over $\mathbf{Q}$ having $\sqrt[3]{1-\sqrt{3}}$ as a root.

(d) A splitting field of x^3-2 over $\mathbf{R}$.

(e) The characteristic of a field of 25 elements.

2. (20 points; 4 points each.) For each of the items listed below, either *give an example,* or give a brief reason why *no example exists.* (If you give an example, you do *not* have to prove that it has the property stated.)

(a) An abelian group which is not cyclic.

(b) A field which is not a ring.

(c) A ring which is not an integral domain.

(d) A Euclidean domain which is not a unique factorization domain.

(e) A unique factorization domain which is not a principal ideal domain.

3. Short proofs (30 points; 6 points each)

(a) Suppose G is a finite group acting on a set S, and x is an element of S. Recall that Gx denotes $\{gx \mid g \in G\}$, while G_x denotes $\{g \in G \mid gx = x\}$.

Prove using only the definition of action of G on S (which you are *not* asked to give) and facts about groups that $|Gx| = [G : G_x]$.

(b) Suppose R is a commutative ring with identity $1 \neq 0$ in which $\{0\}$ is a maximal ideal (i.e., a proper ideal which is not contained in any larger proper ideal). Show that R is a field. Do not assume any result about maximal ideals except the definition.

(c) Show that if a and b are nonzero elements of an integral domain R, and $aR = bR$, then a and b are associates (i.e., there exists a unit u such that $b = au$).

(d) Show that $x^2 - 7$ has no root in $\mathbf{Q}(\sqrt{3})$.

(In a similar situation, where the book said "the roots $\pm\sqrt{3}$ of the polynomial $x^2 - 3$ do not belong to $\mathbf{Q}(\sqrt{2})$ because they cannot be written in the form $a + b\sqrt{2}$", I pointed out that one needed a *proof* that $\pm\sqrt{3}$ could not be written in that form, and I showed you such a proof. The proof you give of the statement here can be the analog of my proof of the above fact, or a different proof if you have one.)

(e) Suppose R is a commutative ring with identity having characteristic $m > 0$ and S is a commutative ring with identity having characteristic $n > 0$. Show that the characteristic of the ring $R \oplus S$ is the least common multiple of m and n.

4. (30 points, 3 points each) Below, a theorem and a corollary are proved. After certain steps of the proof I have inserted parenthetical questions such as "(0 Why?)". Give your explanation at the bottom of the page after the boxed number corresponding to each question. Your reasons can be results proved in the text (you don't have to specify their statement-numbers!), observations about the given situation, or calculations. Do not worry about giving further reasons to support your reasons; one key fact or calculation is what is wanted in each case. Note also that if you can't justify some step, you may still assume it in justifying later steps.

Throughout this question, $\langle a+bi\rangle$ will denote the ideal generated by $a+bi$ in $\mathbf{Z}[i]$, while $\langle n\rangle$ will denote the ideal generated by n in $\mathbf{Z}$. Thus, $\mathbf{Z}/\langle n\rangle$ is the ring we have more often called $\mathbf{Z}_n$. When a symbol of the form $[x]$ is used, if it is referred to as a member of $\mathbf{Z}/\langle n\rangle$, it will denote the congruence class of an integer $x \in \mathbf{Z}$ by $\langle n\rangle$, while if it is referred to as a member of $\mathbf{Z}[i]/\langle a+bi\rangle$ it will denote the congruence class of an element $x \in \mathbf{Z}[i]$ by $\langle a+bi\rangle$.

Theorem. *If a and b are relatively prime integers, and $n = a^2+b^2$, then $\mathbf{Z}[i]/\langle a+bi\rangle \cong \mathbf{Z}/\langle n\rangle$, as rings.*

Proof. Let $\varphi\colon \mathbf{Z} \to \mathbf{Z}[i]/\langle a+bi\rangle$ be the homomorphism defined by $\varphi(k) = [k] \in \mathbf{Z}[i]/\langle a+bi\rangle$ for all $k \in \mathbf{Z}$. We shall show this homomorphism is surjective, and has kernel $\langle n\rangle$. These facts imply the desired conclusion, $\mathbf{Z}[i]/\langle a+bi\rangle \cong \mathbf{Z}/\langle n\rangle$. (1 Why?)

To prove surjectivity, first note that there exist integers x and y such that $ax+by = 1$. (2 Why?) Hence the product $(a+bi)(y+xi) = (ay-bx) + (ax+by)i$ equals $c + i$, where $c = ay - bx \in \mathbf{Z}$. Hence in $\mathbf{Z}[i]$ we have $i \equiv -c \pmod{\langle a+bi\rangle}$ (3 why?), hence in $\mathbf{Z}[i]/\langle a+bi\rangle$, $[i] = [-c]$. Hence any $[p+qi] \in \mathbf{Z}[i]/\langle a+bi\rangle$ can be written $[p]+[q][i] = [p]+[q][-c] = [p+q(-c)] = \varphi(p-qc) \in \varphi(\mathbf{Z})$. So φ is surjective.

Let us now determine $\ker(\varphi)$. We note that if $m \in \ker(\varphi)$, then m must be a multiple of $a+bi$ in $\mathbf{Z}[i]$ ([4] why?), that is, we can write

$$m = (a+bi)(u+vi) \tag{1}$$

where $u, v \in \mathbf{Z}$. Expanding the above equation and looking at its imaginary part, we get $0 = av+bu$, hence

$$av = -bu, \tag{2}$$

so that $a \mid bu$. This in turn implies $a \mid u$ ([5] why?). Writing $u = aw$ $(w \in \mathbf{Z})$, substituting into (2), and cancelling a, we get $v = -bw$. Substituting these formulas for u and v into (1) we get $m = (a+bi)(aw-bwi) = w(a+bi)(a-bi) = w(a^2+b^2) = wn \in \langle n \rangle$. This shows that $\ker(\varphi) \subseteq \langle n \rangle$. On the other hand, $n = (a+bi)(a-bi) \in \langle a+bi \rangle$, so $n \in \ker(\varphi)$. Hence $\langle n \rangle = \ker(\varphi)$ ([6] why?), completing the proof. □

Corollary. *For any integer $n > 1$, the following conditions are equivalent:*

(a) *The ring $\mathbf{Z}/\langle n \rangle$ contains a square root of $[-1]$.*

(b) *There exist relatively prime integers a and b such that $a^2+b^2 = n$.*

Proof. Assuming (a), let c be an integer such that $[c]^2 = [-1]$ in $\mathbf{Z}/\langle n \rangle$. Let us define $\varphi: \mathbf{Z}[i] \to \mathbf{Z}/\langle n \rangle$ by $\varphi(x+yi) = [x+yc]$. This clearly respects addition; a quick calculation using the equation $[c]^2 = [-1]$ shows that it also respects multiplication, i.e., that $\varphi((x+yi)(x'+y'i)) = \varphi(x+yi)\,\varphi(x'+y'i)$. ([7] Show this calculation.) Hence φ is a ring homomorphism. Hence $\ker(\varphi) = \langle a+bi \rangle$ for some $a, b \in \mathbf{Z}$ ([8] why?).

I claim that a and b are relatively prime. For if they had a nonunit common divisor d, then every element of $\langle a+bi \rangle$ would be a multiple of d, hence the real and imaginary parts of any such element (i.e., the coefficients of 1 and i) would be divisible by d in $\mathbf{Z}$. However $c - i \in \langle a+bi \rangle$ ([9] why?), and its imaginary part, -1, is not divisible by any nonunit.

Note also that φ is surjective (has all of $\mathbf{Z}/\langle n \rangle$ as its image) ([10] why?).

Now by the Fundamental Homomorphism Theorem for Rings, the image of φ is isomorphic to $\mathbf{Z}[i]/\ker(\varphi) = \mathbf{Z}[i]/\langle a+bi \rangle$, which by the preceding theorem is isomorphic to $\mathbf{Z}/\langle a^2+b^2 \rangle$. Hence $\mathbf{Z}/\langle n \rangle \cong \mathbf{Z}/\langle a^2+b^2 \rangle$. The first of these rings has n elements and the second has a^2+b^2 elements, so $n = a^2+b^2$, proving (b).

Conversely, assuming (b), the preceding theorem tells us that $\mathbf{Z}[i]/\langle a+bi \rangle \cong \mathbf{Z}/\langle n \rangle$. The former ring has a square root of -1 (that is, a square root of the negative of its multiplicative identity element), namely $[i]$, hence so must the latter, proving (a). □