Problem Set 11

Due Thursday, November 20

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly.* As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. Prove that a finite domain (i.e., an integral domain that is finite as a set) is a field.

Proof. Let R be a finite domain, and consider any nonzero element $x \in R$. Since R is finite, there are only finitely many elements of the form x^n with $n \geqslant 0$. In particular, there exist $n > m$ such that $x^n = x^m$. Thus by the cancellation rule, we have

$$x^m \cdot x^{n-m} = x^m \implies x^{n-m} = 1.$$

Note that $a = n - m > 0$ and $x^a = 1$. In particular, x is a unit, with inverse x^{a-1}. We conclude that R is a field. □

Problem 2. Define $N \colon \mathbb{C} \to \mathbb{R}$ to be the square of the complex norm; that is,

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2.$$

You can use without proof that N satisfies $N(\alpha\beta) = N(\alpha)N(\beta)$ for any $\alpha, \beta \in \mathbb{C}$.

a) Show that the only units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

Proof. First, note that given $a + bi \in \mathbb{Z}[i]$, we have

$$N(a + bi) = a^2 + b^2 \in \mathbb{Z},$$

and in fact $N(a + bi) \geqslant 0$. If $\alpha\beta = 1$, then $N(\alpha)N(\beta) = 1$ and hence the nonnegative integers $N(\alpha)$ and $N(\beta)$ must satisfy $N(\alpha) = N(\beta) = 1$. We conclude that $\alpha \in \{\pm 1, \pm i\}$.

On the other hand, -1 is its own inverse and $i(-i) = 1$, so ± 1 and $\pm i$ are all units. □

b) Prove that the only units of the ring $\mathbb{Z}[\sqrt{-5}]$ are ± 1.

Proof. Note that the norm of $\alpha = a + b\sqrt{-5}$ is $N(\alpha) = a^2 + 5b^2$. It α is a unit, then as in the previous proof its norm would have to be 1 and this can only occur if $a = \pm 1$ and $b = 0$. □

c) Are there units in $\mathbb{Z}[\sqrt{2}]$ other than ± 1?

Solution: Yes, for instance $3+2\sqrt{2}$ is a unit since $(3+2\sqrt{2})(3-2\sqrt{2}) = 9-4\cdot 2 = 1$. Note that the trick we used on the Gaussian integers and $\mathbb{Z}[\sqrt{-5}]$ does not apply here, as the norm of $\alpha = a+b\sqrt{2}$ is

$$N(\alpha) = (a+b\sqrt{2})^2 = a^2 + ab\sqrt{2} + 2b^2.$$

Problem 3. Let R be a ring and $R[X]$ be a polynomial ring over R. For a nonzero element

$$f(X) = r_0 + r_1 X + \cdots + r_n X^n \in R[X]$$

we define the degree of $f(X)$ to be $\max\{i \mid r_i \neq 0\}$, denoted $\deg(f(X))$. Show that if R has no zerodivisors, then $R[X]$ has no zerodivisors, and

$$\deg(f(X)g(X)) = \deg(f(X)) + \deg(g(X))$$

for all nonzero polynomials $f(X), g(X) \in R[X]$.

Proof. Write $f(X) = r_0 + r_1 X + \cdots + r_n X^n$ and $g(X) = s_0 + s_1 X + \cdots + s_m X^m$ with $r_n, s_m \neq 0$, so $n = \deg(f)$ and $m = \deg(g)$ Then the X^{n+m} coefficient of $f(X)g(X)$ is $r_n s_m \neq 0$, and for any $k > n+m$, the X^k coefficient of $f(X)g(X)$ is 0, so $\deg(f(X)g(X)) = n+m$. □

Problem 4. Let R be a ring.

a) Prove that an ideal I of R is proper if and only if I contains no units.

Proof. Let I be an ideal. If it contains no units, then it does not contain 1 and hence $I \neq R$. If I contains a unit u, then for all $r \in R$,

$$r = (ru^{-1})u \in I$$

and hence $I = R$. □

b) Assume R is commutative. Show that R is a field if and only if its only ideals are $\{0\}$ and R.

Proof. Suppose R is a field. Every nonzero ideal I contains a nonzero element u, but since R is a field the element u must be unit. By (1.1), $I = R$. Assume R has exactly two ideals, $\{0\}$ and R. If $0 \neq a \in R$, then the ideal $(a) = Ra$ is nonzero, and thus $(a) = R$. In particular, there is $u \in R$ such that

$$au = ua = 1.$$

Thus a is a unit, and therefore R is a field. □

c) Show that the only ideals of $R = \mathrm{Mat}_{2\times 2}(\mathbb{R})$ are $\{0\}$ and R, and yet R is not a division ring.

Proof. Let I be a nonzero ideal in R and suppose $A \in I$ is any nonzero matrix. By elementary linear algebra, we we may do row and column operations to get either

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \text{or} \qquad B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

Row and column operations amount to multiplying on the left or right by (invertible) matrices, so we can multiply A by other matrices on the left and/or right and obtain either I_2 or B. We conclude that $I_2 \in I$ or $B \in I$.

If $B \in I$, then we can apply a row operation and a column operation to B to obtain

$$C = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus $C \in I$. Therefore,

$$I_2 = B + C \in I.$$

Either way, we conclude that $I_2 \in I$, and thus $I = R$ by (1.1).

But R is not a division ring since it has many nonzero, nonunit elements; for example, B is nonzero but not invertible, since its determinant is zero and all invertible matrices have invertible determinant. □