Math 308
3-6-1994

Solutions to Problem Set 3.

[page 252]

5. Let F be a field and let a be a nonzero element of F.

a. If $af(x)$ is irreducible over F, prove that $f(x)$ is irreducible over F.

b. If $f(ax)$ is irreducible over F, prove that $f(x)$ is irreducible over F.

c. If $f(x+a)$ is irreducible over F, prove that $f(x)$ is irreducible over F.

For (a), suppose $f(x) = g(x)h(x)$. Then $af(x) = [ag(x)]h(x)$. Since $af(x)$ is irreducible, either $ag(x)$ or $h(x)$ is a unit. If $ag(x)$ is a unit, it's a nonzero constant, so the same is true of $g(x)$, and $g(x)$ is a unit. Therefore, either $g(x)$ or $h(x)$ is a unit, and $f(x)$ is irreducible.

For (b), suppose $f(x) = g(x)h(x)$. Then $f(ax) = g(ax)h(ax)$. Since $f(ax)$ is irreducible, either $g(ax)$ is a unit or $h(ax)$ is a unit. But $g(x)$ has the same degree as $g(ax)$ and $h(x)$ has the same degree as $h(ax)$, so either $g(x)$ is a unit or $h(x)$ is a unit. Therefore, $f(x)$ is irreducible.

For (c), suppose $f(x) = g(x)h(x)$. Then $f(x+a) = g(x+a)h(x+a)$. Since $f(x+a)$ is irreducible, either $g(x+a)$ is a unit or $h(x+a)$ is a unit. But $g(x)$ has the same degree as $g(x+a)$ and $h(x)$ has the same degree as $h(x+a)$, so either $g(x)$ is a unit or $h(x)$ is a unit. Therefore, $f(x)$ is irreducible. $\square$

---

6. Show that x^4+1 is irreducible over $\mathbb{Q}$ but reducible over $\mathbb{R}$.

$x^4+1 = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$, so x^4+1 is reducible over $\mathbb{R}$.
Let $x = y+1$. Then

$$x^4+1 = (y+1)^4+1 = y^4+4y^3+6y^2+4y+2.$$

$y^4+4y^3+6y^2+4y+2$ is irreducible over $\mathbb{Q}$ by Eisenstein using the prime 2. By Problem 5(c), x^4+1 is irreducible over $\mathbb{Q}$ as well. $\square$

---

7. Construct a field of order 25.

I will use the result of Problem 12. It suffices to find an irreducible polynomial of degree 2 over $\mathbb{Z}_5$. x^2+2 has no roots in $\mathbb{Z}_5$:

x	0	1	2	3	4
x^2+2	2	3	1	1	3

Hence, x^2+2 is irreducible over $\mathbb{Z}_5$, and $\mathbb{Z}_5[x]/\langle x^2+2\rangle$ is a field with 25 elements. $\square$

---

10. Determine which of the following polynomials below are irreducible over $\mathbb{Q}$.

a. $x^5+9x^4+12x^2+6$

b. x^4+x+1

c. x^4+3x^2+3

d. $x^5 + 5x^2 + 1$

e. $\dfrac{5}{2}x^5 + \dfrac{9}{2}x^4 + 15x^3 + \dfrac{3}{7}x^2 + 6x + \dfrac{3}{14}$

$x^5 + 9x^4 + 12x^2 + 6$ is irreducible by Eisenstein with the prime 3.

$x^4 + x + 1$ reduces to $x^4 + x + 1$ mod 2. $x^4 + x + 1$ has no roots in $\mathbb{Z}_2$, so it has no linear (or cubic) factors. Hence, if it factors it must do so as a product of two quadratics. The quadratics over $\mathbb{Z}_2$ are $x^2 + 1$, $x^2 + x$, and $x^2 + x + 1$. The first two have $x = 1$ as a root, so they can't be factors of $x^4 + x + 1$. Since

$$(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq x^4 + x + 1,$$

$x^4 + x + 1$ has no quadratic factors over $\mathbb{Z}_2$. Therefore, $x^4 + x + 1$ is irreducible over $\mathbb{Z}_2$. Since it has the same degree as the original polynomial, $x^4 + x + 1$ is irreducible over $\mathbb{Q}$.

$x^4 + 3x^2 + 3$ is irreducible by Eisenstein using the prime 3.

Seeting $x = y - 1$ yields

$$x^5 + 5x^2 + 1 = y^5 - 5y^4 + 10y^3 - 5y^2 - 5y + 5.$$

$y^5 - 5y^4 + 10y^3 - 5y^2 - 5y + 5$ is irreducible by Eisenstein using the prime 5. So $x^5 + 5x^2 + 1$ is irreducible by Problem 5(c).

$$14 \cdot \left(\frac{5}{2}x^5 + \frac{9}{2}x^4 + 15x^3 + \frac{3}{7}x^2 + 6x + \frac{3}{14}\right) = 35x^5 + 63x^4 + 210x^3 + 6x^2 + 84x + 3.$$

$35x^5 + 63x^4 + 210x^3 + 6x^2 + 84x + 3$is irreducible by Eisenstein using the prime 3. Hence, $\dfrac{5}{2}x^5 + \dfrac{9}{2}x^4 + 15x^3 + \dfrac{3}{7}x^2 + 6x + \dfrac{3}{14}$ is irreducible by Problem 5(b). $\square$

---

11. Show that $x^2 + x + 4$ is irreducible over $\mathbb{Z}_{11}$.

x	0	1	2	3	4	5	6	7	8	9	10
$x^2 + x + 4$	4	6	10	5	2	1	2	5	10	6	4

The quadratic has no roots in $\mathbb{Z}_{11}$, so it has no linear factors, so it's irreducible. $\square$

---

12. Suppose $f(x) \in \mathbb{Z}_p[x]$ and is irreducible over $\mathbb{Z}_p$. If $\deg f(x) = n$, prove that $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field with p^n elements.

Since f is irreducible, $\langle f(x)\rangle$ is maximal, and $\mathbb{Z}_p[x]/\langle f(x)\rangle$ is a field.

Let $g(x) \in \mathbb{Z}_p[x]$. By the Division Algorithm,

$$g(x) = f(x)q(x) + r(x), \qquad \deg r < \deg f = n.$$

Thus,

$$g(x) + \langle f(x)\rangle = f(x)q(x) + r(x) + \langle f(x)\rangle = r(x) + \langle f(x)\rangle.$$

Now $r(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$, so every element of $\mathbb{Z}_p[x]/\langle f(x)\rangle$ has the form

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle f(x)\rangle$$

for $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}_p$. Since there are p choices for each of the a's, this proves that $\mathbb{Z}_p[x]/\langle f(x)\rangle$ has *at most* p^n elements.

To show that there are *exactly* p^n elements, I must show that the representation above is unique. Suppose

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle f(x)\rangle = a_0' + a_1 x' + \cdots + a_{n-1}' x^{n-1} + \langle f(x)\rangle.$$

Then

$$(a_0 - a_0') + (a_1 - a_1')x + \cdots + (a_{n-1} - a_{n-1}')x^{n-1} \in \langle f(x)\rangle.$$

But f has degree n, so it can't divide the polynomial on the left (which has degree $n-1$) unless the polynomial on the left is 0. This implies that $a_i = a_i'$ for all i.

Hence, every element of $\mathbb{Z}_p[x]/\langle f(x)\rangle$ can be uniquely written in the form

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + \langle f(x)\rangle.$$

Therefore, $\mathbb{Z}_p[x]/\langle f(x)\rangle$ has p^n elements. $\square$

[page 270]

2. Show that the union of a chain $I_1 \subset I_2 \subset \cdots$ of ideals of a ring R is an ideal of R.

Let $I_1 \subset I_2 \subset \cdots$ be a chain of ideals and let $I = \bigcup_n I_n$. Since $0 \in I_1$, $0 \in I$ and I is nonempty. Let $x, y \in I$. If $x \in I_m$ and $y \in I_n$, then either $I_m \subset I_n$ or $I_n \subset I_m$. In the first case, $x, y \in I_n$ so $x - y \in I_n \subset I$. In the second case, $x, y \in I_m$ so $x - y \in I_m \subset I$. Thus, I is an additive subgroup.

I will take the problem to be talking about *left ideals*; the result is true for right ideals or two-sided ideals as well.

Let $x \in I$ and $r \in R$. If $x \in I_n$ then $rx \in I_n \subset I$. Therefore, I is an ideal. $\square$

---

3. Suppose a and b belong to an integral domain, $b \neq 0$, and a is not a unit. Show that $\langle ab\rangle$ is a proper subset of $\langle b\rangle$.

Anything divisible by ab is divisible by b, so $\langle ab\rangle \subset \langle b\rangle$. If $\langle ab\rangle = \langle b\rangle$, then $b \in \langle ab\rangle$, so $b = abc$ for some c. Since $b \neq 0$, I may cancel b's to obtain $1 = ac$. This means that a is a unit $\times$. Hence, $\langle ab\rangle$ is a proper subset of $\langle b\rangle$. $\square$

---

4. Let D be an integral domain. Define $a \sim b$ if a and b are associates. Show that this defines an equivalence relation on D.

$a = 1 \cdot a$, so $a \sim a$ for all a.

If $a \sim b$, then $a = ub$ for u a unit. Then $b = u^{-1}a$, so $b \sim a$.

If $a \sim b$ and $b \sim c$, then $a = ub$ and $b = vc$, where u and v are units. Then $a = uvc$, and $(uv)(v^{-1}u^{-1}) = 1$ shows that uv is a unit. Hence, $a \sim c$. Therefore, $\sim$ is an equivalence relation. $\square$

I'm going to need the following lemma.

Lemma. Let p be a positive integer.

(a) The map $N : \mathbb{Z}[\sqrt{-p}] \to \mathbb{Z}$ defined by $N(a + b\sqrt{-p}) = a^2 + pb^2$ satisfies $N(xy) = N(x)N(y)$.

(b) The map $N : \mathbb{Z}[\sqrt{p}] \to \mathbb{Z}$ defined by $N(a + b\sqrt{-p}) = a^2 - pb^2$ satisfies $N(xy) = N(x)N(y)$.

Proof. For part (a):

$$(a+b\sqrt{-p})(c+d\sqrt{-p}) = (ac-pbd)+\sqrt{-p}(ad+bc),$$

$$N\left[(a+b\sqrt{-p})(c+d\sqrt{-p})\right] = (ac-pbd)^2+p(ad+bc)^2 = a^2c^2-2pabcd+p^2b^2d^2+pa^2d^2+2pabcd+pb^2c^2 =$$

$$a^2(c^2+pd^2)+pb^2(c^2+pd^2) = (a^2+pb^2)(c^2+pd^2) = N(a+b\sqrt{-p})N(c+d\sqrt{-p}).$$

For part (b):

$$(a+b\sqrt{p})(c+d\sqrt{p}) = (ac+pbd)+\sqrt{p}(ad+bc),$$

$$N\left[(a+b\sqrt{p})(c+d\sqrt{p})\right] = (ac+pbd)^2-p(ad+bc)^2 = a^2c^2+2pabcd+p^2b^2d^2-pa^2d^2-2pabcd-pb^2c^2 =$$

$$a^2(c^2-pd^2)-pb^2(c^2-pd^2) = (a^2-pb^2)(c^2-pd^2) = N(a+b\sqrt{p})N(c+d\sqrt{p}).\ \square$$

---

11. Show that $\mathbb{Z}[\sqrt{-6}]$ is not a unique factorization domain. (Hint: Factor 10 in two ways.) Why does this show that $\mathbb{Z}[\sqrt{-6}]$ is not a principal ideal domain?

$10 = 2\cdot 5 = (2+\sqrt{-6})(2-\sqrt{-6})$. If I can show 2, 5, $2+\sqrt{-6}$, and $2-\sqrt{-6}$ are irreducible, I will have factored a number into irreducibles in two different ways, proving that $\mathbb{Z}[\sqrt{-6}]$ is not a unique factorization domain.

Define $N(a+b\sqrt{-6}) = a^2+6b^2$. The preceding lemma shows that $N(xy) = N(x)N(y)$.

Note that $N(a+b\sqrt{-6}) = 1$ implies that $a = \pm 1$ and $b = 0$. Thus, $a+b\sqrt{-6} = \pm 1$ is a unit.

Note also that $N(a+b\sqrt{-6}) = a^2+6b^2 = 2$ is impossible. For if $b \ne 0$, then $a^2+6b^2 \ge 6$. Hence, $b = 0$, but then $a^2 = 2$, which has no solutions in $\mathbb{Z}$.

By similar reasoning, $N(a+b\sqrt{-6}) = a^2+6b^2 = 5$ is impossible.

To show 2 is irreducible, suppose $2 = xy$, so $4 = N(2) = N(x)N(y)$. Since these are all integers, either $N(x) = N(y) = 2$ (impossible) or one of $N(x)$, $N(y)$ is 1 and the other is 4. But $N(x) = 1$ implies x is a unit and $N(y) = 1$ implies y is a unit. Hence, 2 is irreducible.

To show that 5 is irreducible, suppose $5 = xy$, so $25 = N(2) = N(x)N(y)$. Since these are all integers, either $N(x) = N(y) = 5$ (impossible) or one of $N(x)$, $N(y)$ is 1 and the other is 25. But $N(x) = 1$ implies x is a unit and $N(y) = 1$ implies y is a unit. Hence, 5 is irreducible.

To show that $2+\sqrt{-6}$ is irreducible, suppose $2+\sqrt{-6} = xy$, so $10 = N(2) = N(x)N(y)$. Since these are all integers, either one of $N(x)$, $N(y)$ is 2 and the other 5 (impossible) or one of $N(x)$, $N(y)$ is 1 and the other is 10. But $N(x) = 1$ implies x is a unit and $N(y) = 1$ implies y is a unit. Hence, $2+\sqrt{-6}$ is irreducible. The same argument shows that $2-\sqrt{-6}$ is irreducible.

By my initial remarks, this proves that $\mathbb{Z}[\sqrt{-6}]$ is not a unique factorization domain.

Since PIDs and UFDs, it follows that $\mathbb{Z}[\sqrt{-6}]$ is not a PID, either. $\square$

---

20. In $\mathbb{Z}[\sqrt{5}]$, prove that both 2 and $1+\sqrt{5}$ are irreducible but not prime.

Define $N(a+b\sqrt{5}) = a^2-5b^2$. The lemma above shows that $N(xy) = N(x)N(y)$.

Observe that if $N(a+b\sqrt{5}) = \pm 1$, then $a+b\sqrt{5}$ is a unit. For $a^2-5b^2 = \pm 1$ implies $(a+b\sqrt{5})(a-b\sqrt{5}) = \pm 1$.

To show that 2 is irreducible, suppose $2 = xy$, so $4 = N(2) = N(x)N(y)$. If one of $N(x)$, $N(y)$ is ± 1 and the other is ± 4 then one of x, y is a unit.

Otherwise, $N(x) = N(y) = 2$ or $N(x) = N(y) = -2$. Write $x = a+b\sqrt{5}$.

If $a^2-5b^2 = 2$, reduce mod 5 to get $a^2 = 2 \bmod 5$. Squaring 0, 1, 2, 3, 4 mod 5 proves $a^2 = 2 \bmod 5$ has no solutions.

If $a^2-5b^2 = -2$, reduce mod 5 to get $a^2 = 3 \bmod 5$. Squaring 0, 1, 2, 3, 4 mod 5 proves $a^2 = 3 \bmod 5$ has no solutions.

This proves that 2 is irreducible. Now $N(1+\sqrt{5}) = -4$, so essentially the same argument shows that $1+\sqrt{5}$ is irreducible.

Next, I'll show 2 and $1+\sqrt{5}$ are not prime.

Note that $2 \mid (-4) = (1+\sqrt{5})(1-\sqrt{5})$. But for no $a + b\sqrt{5}$ do I have $2 \cdot (a + b\sqrt{5}) = 1 + \sqrt{5}$ or $2 \cdot (a + b\sqrt{5}) = 1 - \sqrt{5}$. Hence, 2 divides a product without dividing either factor, so 2 is not prime.

Likewise, $1+\sqrt{5} \mid (1+\sqrt{5})(1-\sqrt{5}) = (-4) = (2)(-2)$. I'll show that $1+\sqrt{5}$ does not divide 2 or -2.

$(a+b\sqrt{5})(1+\sqrt{5}) = 2$ implies $a + 5b = 2$ and $a + b = 0$. Subtracting the second equation from the first yields $4b = 2$, which has no solutions in $\mathbb{Z}$. So $1+\sqrt{5}$ does not divide 2.

$(a+b\sqrt{5})(1+\sqrt{5}) = -2$ implies $a + 5b = -2$ and $a + b = 0$. Subtracting the second equation from the first yields $4b = -2$, which has no solutions in $\mathbb{Z}$. So $1+\sqrt{5}$ does not divide -2.

Thus, $1+\sqrt{5}$ divides a product without dividing either factor, so $1+\sqrt{5}$ is not prime. $\square$

---

30. Show that an integral domain with the property that every strictly decreasing chain of ideals $I_1 \supset I_2 \supset \cdots$ must be finite in length is a field.

Let $a \neq 0$. I will show that a is invertible. Consider the sequence of ideals

$$\langle a \rangle \supset \langle a^2 \rangle \supset \cdots.$$

By assumption, this chain is finite, so $\langle a^n \rangle = \langle a^{n+1} \rangle$ for some $n \geq 1$. Then $a^n \in \langle a^{n+1} \rangle$, so $a^n = ra^{n+1}$ for some r. $a \neq 0$, so I may cancel a^n's from both sides, leaving $1 = ar$. Therefore, r is the inverse of a. $\square$

"Experience teaches only the teachable." - Aldous Huxley