

**MATH 632 Homework List 4** 27 March 2000

Sections 4, 5, & 6: Factorization

The following problems give you practice with the material. I will ask you to hand in *some* of them for a grade later. I may also assign additional problems.

We will not go through Chapter 11 in order (and we will not do all of it). We may even do parts of sections at different times. Thus the listing of the homework problems below may not match the order in which you can do them or in which they will be collected: this may even be true of problems in a single section.

*Problems* from Chapter 11 of Artin, pp. 440–448

- §1 #1,3,4a,5(at least a),6,7,8,9a,10,15
- §2 #1,2,3,4,7,8,9,11a,12,13(trivial),19
- §3 #1,2,5,6,8,9
- §4 #1,2,3,4,6,7,8,9ace,12,13,16
- §5 #1,2,3,6
- §6 #1,3
- §7 #2,9
- §11 #1(definition should be  $\sigma(a + b\delta) = |a^2 - 2b^2|$ ),4
- §12 #4,5,9

*Problems* from the class notes (Sections 5, 6, and 7 on the web page)

**Problem 5.A.** Let  $R$  be a commutative ring with  $0 \neq 1$  and suppose there is a size function  $\sigma$  on  $R$ . Prove that  $R$  is an integral domain.

**Problem 5.B.** It is possible to weaken the assumptions defining a Euclidean ring and still prove the unique factorization theorem.

Here is a an extended problem. Define a *generalized size function* to be a map  $\sigma : R \rightarrow X$  for some *well-ordered set*  $X$ , satisfying  $\sigma(0) < \sigma(a)$  for all  $a \in R, a \neq 0$ , and define a *generalized Euclidean domain* to be an integral domain with a generalized size function satisfying the Division Algorithm. Show that (almost?) all of the results of this section hold for generalized Euclidean domains.

This would be straightforward, except that we would like to know  $\sigma(ab) > \sigma(a)$  whenever  $a, b$  are not zero or units. You may need to assume this holds. Ultimately this can be proved, but the size function  $\sigma$  may have to be modified.

**Problem 5.C.** Let  $R$  be a Euclidean domain with size function  $\sigma$ . Prove that if  $a \in R$ , then  $\sigma(a) = \sigma(1)$  iff  $a$  is a unit. Prove that if  $b \in R$  is nonzero and not a unit, then  $\sigma(b) > \sigma(1)$ .

**Problem 5.D.** Let  $R$  be an integral domain. Prove that  $a, b \in R$  are associates iff  $a = bu$  for some unit  $u \in R$ . Of course, we also have  $b = au^{-1}$  when this is the case.

**Problem 5.E.** A *principal ideal domain*, abbreviated PID, is an integral domain  $R$  in which every ideal is of the form  $aR$  for some  $a \in R$ .

- (1) Prove that every Euclidean domain is a PID. (Hint: If  $I \triangleleft R$ , pick the nonzero element  $a \in I$  with  $\sigma(a)$  as small as possible.)
- (2) Prove that the gcd exists and can be expressed as a linear combination — just as in a Euclidean domain — in a PID. (Hint: the gcd of  $a_1, \dots, a_n$  can be obtained from the ideal  $a_1R + \dots + a_nR$  generated by  $a_1, \dots, a_n$ .)

**Problem 5.F.** Let  $R$  be an integral domain. If  $p \in R$  is nonzero and not a unit, and  $p$  has the property that  $p | ab$  implies  $p | a$  or  $p | b$ , it is common to call  $p$  *prime*. We have just shown that every irreducible element in a Euclidean domain is prime. This result fails in arbitrary integral domains. However, its converse is always valid.

Prove that if  $R$  is an integral domain and  $p \in R$  is prime in the above sense ( $p$  is nonzero and not a unit, and  $p | ab$  implies  $p | a$  or  $p | b$ ), then  $p$  is irreducible.

**Problem 5.G.** Let  $R$  be a Euclidean domain, let  $a, b, c \in R$ , and suppose  $a, b$  are relatively prime. If  $a \mid c$  and  $b \mid c$ , prove that  $ab \mid c$ .

**Problem 5.H.** Show that  $\mathbb{Z}[\sqrt{-2}]$  and  $\mathbb{Z}[\sqrt{2}]$  are Euclidean domains.

Hint: the natural size function to try for  $\mathbb{Z}[\sqrt{n}]$  is  $\sigma(a + b\sqrt{n}) = |(a + b\sqrt{n})(a - b\sqrt{n})|$ .

**Problem 5.I.** Let  $R$  be a Euclidean domain with size function  $\sigma$  and let  $a_1, \dots, a_n \in R$ , not all of them 0. Prove that a common divisor  $d$  of  $a_1, \dots, a_n$  is a gcd of  $a_1, \dots, a_n$  iff  $\sigma(d)$  is as large as possible for common divisors.

**Problem 5.J.** Let  $n \in \mathbb{Z}, n < -2$  and set  $R = \mathbb{Z}[\sqrt{n}]$ . Prove that 2 is an irreducible element in  $R$ , but that it does not have the property that  $2 \mid ab$  implies  $2 \mid a$  or  $2 \mid b$ . Conclude from this that  $R$  is not a Euclidean domain.

Hint: you may want to use the norm  $N(a + b\sqrt{n}) = a^2 + |n|b^2$  in your proof.

**Problem 6.A.** Show that the following is a complete list of irreducible elements in  $\mathbb{Z}[i]$ , up to associates. (Each element on the list has 3 other associates.)

- (1)  $1 + i$ ;
- (2) Prime integers  $p$  with  $p \equiv 3 \pmod{4}$ ;
- (3) The numbers  $a + bi$  and  $a - bi$ , where  $a, b$  are positive integers such that  $a^2 + b^2$  is prime and  $a \geq b$ . There is a unique pair  $(a, b)$  with these properties and with  $a^2 + b^2 = p$  for every prime integer  $p$  with  $p \equiv 1 \pmod{4}$ .

For example, the irreducibles in  $\mathbb{Z}[i]$  of absolute value at most 7 (norm less than 50) are — up to associates —  $1 + i, 2 \pm i, 3, 3 \pm 2i, 4 \pm i, 5 \pm 2i, 6 \pm i, 5 \pm 4i, 7$ .

Another way to state the result is: every prime integer  $p \equiv 3 \pmod{4}$  remains irreducible in  $\mathbb{Z}[i]$ , while every other prime integer  $p$  factors as  $p = q\bar{q}$ , where  $q, \bar{q}$  are non-real irreducible elements of  $\mathbb{Z}[i]$ . The elements  $q, \bar{q}$  are associates only if  $p = 2$ . This is a complete list of the irreducible elements of  $\mathbb{Z}[i]$  (up to association). We sometimes state (part of) this conclusion as: primes congruent to 3 mod 4 remain prime in  $\mathbb{Z}[i]$ , while other primes split. The prime 2 is special, since it can be factored as  $-i(1 + i)^2$ : we say 2 *ramifies* in this extension of  $\mathbb{Z}$ .

**Problem 6.B.** Let  $n$  be a nonzero integer.

- (1) Prove that there are unique integers  $k, m$  with  $k > 0$ ,  $m$  squarefree, and  $n = k^2m$ .
- (2) Prove that the fraction field of  $\mathbb{Z}[\sqrt{n}]$  is (isomorphic to)  $\mathbb{Q}[\sqrt{n}] = \mathbb{Q}[\sqrt{m}]$ .
- (3) It is a fact that the integral closure of  $\mathbb{Z}[\sqrt{n}]$  is  $\mathbb{Z}[\sqrt{m}]$  if  $m \equiv 2, 3 \pmod{4}$  and is  $\{a + b\sqrt{m} \mid a, b \in \mathbb{Z} \text{ or } a = A/2, b = B/2 \text{ for odd } A, B \in \mathbb{Z}\}$  if  $m \equiv 1 \pmod{4}$ . You can assume this or prove it if you're ambitious.
- (4) Prove that the integral closure of  $\mathbb{Z}[\sqrt{n}]$  is  $\mathbb{Z}[\delta]$ , where  $\delta = \sqrt{m}$  if  $m \equiv 2, 3 \pmod{4}$  and  $\delta = (-1 + \sqrt{m})/2$  if  $m \equiv 1 \pmod{4}$ .

**Problem 6.C.** Let  $a, b, c, n$  be positive integers with  $c^n = ab$ . If  $\gcd(a, b) = 1$ , prove that there are relatively prime positive integers  $r, s$  with  $a = r^n, b = s^n$ .

**Problem 6.D.** Let  $R$  be a UFD, let  $a, b, c \in R$ , let  $n$  be a positive integer, and suppose  $a, b$  are relatively prime. If  $c^n = ab$ , prove that there are relatively prime  $r, s \in R$  and a unit  $u \in R$  with  $a = ur^n, b = u^{-1}s^n$ .

**Problem 7.A.** Let  $f = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$  with  $a_n \neq 0$ . Prove that the only integers that can be roots of  $f$  are the integers that divide  $a_0$ . Prove that the only rational numbers that can be roots of  $f$  are rational numbers  $b/c$  where  $b \mid a_0, c \mid a_n$ .

**Problem 7.B.** Let  $f \in \mathbb{Z}[x]$  and let  $p$  be a prime integer such that  $p$  does not divide the leading coefficient of  $f$ . Prove that if the reduction  $\pi_p(f)$  is irreducible in  $\mathbb{Z}_p[x]$ , then there is no factorization  $f = gh$  in  $\mathbb{Z}[x]$  with  $g, h$  non-constant.

This does not quite say that  $f$  is irreducible, since we could have a silly factorization like  $2x = 2 \cdot x$ , which is not a trivial factorization in  $\mathbb{Z}[x]$ , since neither of  $2, x$  is a unit. In particular,  $2x$  is irreducible in  $\mathbb{Q}[x]$  but is not irreducible in  $\mathbb{Z}[x]$ .

**Problem 7.C.** Let  $F$  be a field with the property that neither of the equations  $t^2 = -1$  or  $t^2 + t - 1 = 0$  has a solution in  $F$ . Show that  $x^4 - x^2 - 1$  is irreducible in  $F[x]$ . Show that this applies in  $\mathbb{Z}_3[x]$ .

If you know some number theory, you might be able to prove this applies in  $\mathbb{Z}_p[x]$  whenever  $p$  is a prime with  $p \equiv 3, 7 \pmod{20}$ .

**Problem 7.D.** Show that  $x^4 - x - 4$  is irreducible in  $\mathbb{Z}[x]$ .

**Problem 7.E.** Let  $F$  be a field and let  $f = x^4 + 1 \in F[x]$ .

- (1) Prove that  $f$  is irreducible in  $F[x]$  iff  $F$  does not contain a square root of any of  $-2, -1, 2$ .
- (2) Conclude that if  $F$  is any finite field,  $f$  is not irreducible in  $F[x]$ . This may require the following fact, which you can prove. If  $F$  is a finite field whose characteristic is not 2, the set of nonzero squares in  $F$  forms a subgroup of  $F \setminus \{0\}$  of index 2.

**Problem 7.F.** Let  $f = x^4 + 1$ .

- (1) Prove that  $f$  is reducible in  $\mathbb{Z}_p[x]$  for all primes  $p$ .
- (2) Prove that  $f$  is irreducible in  $\mathbb{Z}[x]$ .

**Problem 7.G.** Let  $R$  be an integral domain and suppose  $g, h \in R[x]$  satisfy  $gh = ax^n$  for some nonzero  $a \in R$ . Prove that  $g = bx^k, h = cx^\ell$  for some  $k, \ell$  and some nonzero  $b, c \in R$ .

**Problem 7.H.** Let  $F$  be a field and let  $f \in F[x]$ . Prove the following statements.

- (1) If  $\deg f = 0$ , then  $f = 0$  or  $f$  is a unit.
- (2) If  $\deg f = 1$ , then  $f$  is irreducible in  $F[x]$ .
- (3) If  $\deg f = 2$  or  $\deg f = 3$ , then  $f$  is irreducible in  $F[x]$  if and only if  $f$  has no roots in  $F$ .

**Problem 7.I.** Let  $R$  be a UFD, and let  $a_1, \dots, a_n, a, b, c \in R$ . Prove the following statements.

- (1) If  $a, b$  are relatively prime and  $a \mid bc$ , then  $a \mid c$ .
- (2) If  $a$  is irreducible and  $a \mid bc$ , then  $a \mid b$  or  $a \mid c$ .
- (3) If  $a, b$  are relatively prime and  $a \mid c, b \mid c$ , then  $a \mid bc$ .

**Problem 7.J.** Let  $R$  be a UFD with fraction field  $F$ . If  $f, g \in F[x]$ , prove that  $c(fg) = c(f)c(g)$ .

You may use the version of Gauss's Lemma that says a product of primitive polynomials is primitive.

**Problem 7.K.** Let  $R$  be a UFD with fraction field  $F$ . Prove that following statements.

You may use the version of Gauss's Lemma that says that if  $f, g \in F[x]$  and  $f = c(f)f_0, g = c(g)g_0$  where  $f_0, g_0$  are primitive, then  $f \mid g$  in  $F[x]$  if and only if  $f_0 \mid g_0$  in  $R[x]$ .

- (1) Let  $f, g \in R[x]$  and suppose  $f$  is primitive. Then  $f \mid g$  in  $R[x]$  if and only if  $f \mid g$  in  $F[x]$ .
- (2) Let  $f, g \in R[x]$ . Then  $f, g$  are relatively prime in  $F[x]$  if and only if the only common factors of  $f, g$  in  $R[x]$  are constants.
- (3) Let  $f, g \in R[x]$  and suppose one of them is primitive. Then  $f, g$  are relatively prime in  $F[x]$  if and only if the only they are relatively prime in  $R[x]$ .

**Problem 7.L.** Let  $R$  be a UFD with field of fractions  $F$  and let  $f \in R[x]$ . Prove that  $f$  is irreducible in  $R[x]$  if and only if either (a)  $f$  is a constant that is irreducible in  $R$  or (b)  $f$  is primitive and  $f$  is irreducible in  $F[x]$ .

You may use the version of Gauss's Lemma that says that when  $f$  is primitive, then  $f$  is irreducible in  $F[x]$  if and only if  $f$  is irreducible in  $R[x]$ .

**Problem 7.M.** Let  $R$  be an integral domain such that  $R[x]$  is a UFD. Prove that  $R$  is a UFD.