

Math 123: Abstract Algebra II

Solution Set # 1

Gregg Musiker

February 11, 2002

1 Chapter 11, Section 1

1.1 Problem 1

$a + b = p$ where p is prime, $a, b, p > 0$. Assume $d|a$ and $d|b$. Then $d|a + b$ so $d|p$. Since p is prime $d = 1$ or p . but $p|a$ and $p|b$ implies $a, b \geq p$. But then $a + b > p$. $\Rightarrow \Leftarrow$

1.2 Problem 8

a) In $F_2[X]$, if $x = 0$ or $x = 1$, $x^3 + x + 1 = 1$ thus $x^3 + x + 1 = 1$ has no linear factors. A reducible cubic must factor into three linear irreducibles or a quadratic and linear irreducible. Since it has no linear factors, $x^3 + x + 1 = 1$ is irreducible.

b) By the quadratic formula, $x^2 - 3x - 3$ has the roots $x = \frac{3 \pm \sqrt{21}}{2}$ so in $F_5[X]$, it has the roots $x = \frac{3 \pm \sqrt{1}}{2} = 1$ or 2 thus $x^2 - 3x - 3 = (x - 1)(x - 2)$.

c) By the quadratic formula, $x^2 + 1$ has the roots $x = \pm\sqrt{-1}$ since F_7 does not contain $\pm\sqrt{-1}$, (Try squaring $0, \dots, 6$ modulo 7 or apply quadratic reciprocity, etc.) $x^2 + 1$ is irreducible in $F_7[x]$.

1.3 Problem 9

a) Suppose f_1, f_2, \dots, f_n are all of the monic irreducible polynomials of $F[x]$. Let $g = f_1 f_2 \cdots f_n + 1$. $f_i \nmid g \forall i$. Since $F[x]$ is a U.F.D. (in fact it is a Euclidean domain by Proposition 2.18, which implies it is a P.I.D. and thus a U.F.D.), one can factor g into irreducibles, hence $\exists f_a$ s.t. f_a is irreducible and $f_a|g$. f_a must be different than any of the initial f_i since f_i cannot divide both $N = f_1 f_2 \cdots f_n$ and $N + 1$. Also, $N + 1$ is not a unit because $\deg(f_i) \geq 1$ so $\deg(N + 1) \geq 1$ but units in $F[x]$ have degree zero. In fact x is the only prime in $F[[x]]$ up to associates.

b) This fails for $F[[x]]$ because the last line fails (i.e. there exist irreducibles f_i that DO divide both $N = f_1 f_2 \cdots f_n$ and $N + 1$) This works because x is

irreducible and $x + 1$ is a unit in $F[[x]]$ thus $N = x$ implies $N + 1 = x + 1$ but $x + 1$ is a unit and thus there are no extraneous irreducibles dividing it.

1.4 Problem 14

Let $f(x) \in F[x]$ have a multiple root ($f(x) = (x - \alpha)^2 g(x)$). Then the derivative of f ,

$$f' = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x).$$

Assuming f is irreducible in $F[x]$, $\gcd(f, f') = 1$ or f . (F is a field thus $F[x]$ is a Euclidean domain, and thus \gcd is well-defined.)

$f \nmid f'$ because $\deg(f) \geq \deg(f')$. Thus $\gcd(f, f') = 1$ hence $\exists h_1, h_2$ s.t. $fh_1 + f'h_2 = 1$ for all x (*).

But since F is a subfield of the complex numbers, it is valid to let $x = \alpha \in C$ but $f(\alpha) = f'(\alpha) = 0$ and thus (*) cannot hold. Thus f must be reducible if it has a multiple root and if f is irreducible, it cannot have a multiple root.

2 Chapter 11, Section 2

2.1 Problem 2

a) Prove that $R = Z[\zeta], \zeta = e^{\frac{2\pi i}{3}}$ is a Euclidean domain

Picturing R as a lattice (as Artin does for $Z[i]$) in the complex plane where formed by additions of the vectors $(1,0)$ and $(-\sqrt{3}/2, 1/2)$. Thus the grid will be composed of rhombuses of base length 1, and perpendicular height $1/2$. The *distance*² from the center (worst case) of a rhombus to any of the corners is $1 - \frac{\sqrt{3}}{4} < 1$. Thus if one looks at the multiples of $x \in R$ one looks at a sublattice and find that the remainder will have norm less than the norm of x .

b) Prove that $R = Z[\sqrt{-2}]$ is a Euclidean domain

Again, this can be proved algebraically or geometrically. Proceeding geometrically, one find the grid made up of rectangles of length 1 and width $\sqrt{2}$. Since the center is a distance of $\sqrt{3}/2$ from any of the corners, by logic similar to example (a), $N(r) \leq 3/4N(x)$.

2.2 Problem 4

if $d = \gcd(a, b) \in R$ (R is a PID), then $\exists c_1, c_2 \in R$ s.t. $d = ac_1 + bc_2$. Assume $a, b \in Z$, and d is the \gcd in Z , d' is the \gcd in $Z[i]$. $d'|a, d'|b \Rightarrow d'|d$ in Z . In $Z[i]$, there also exist $c_3, c_4 \in Z[i]$ s.t. $ac_3 + bc_4 = d'$. $d|a, d|b \Rightarrow d|d'$ in $Z[i]$. Thus d and d' are associates in $Z[i]$ (Note: \gcd is only defined up to associate).

2.3 Problem 5

Assume R is an integral domain. thus if $xy = 0$, $x = 0$ or $y = 0$. Let p be a prime in R . $p|ab$ implies $p|a$ or $p|b$. assuming p is reducible, $p = vw$ where v, w

are not units in R .

$p|vw$ so $p|v$ or $p|w$. W.L.O.G. assume $p|v$. Then there exists a non-unit x s.t. $px = v$. Thus $p = vw = pxw$ and $p(1 - xw) = 0$.

Since $p \neq 0$, and R is an integral domain, $1 - xw = 0$. thus $1 = xw$ which means w is a unit, thus contradicting our assumptions. Thus all primes in an integral domain are irreducible.

(NOTE: important to show that R must be an integral domain for primes to be irreducibles.) The cancellation law is equivalent to the statement $p = pxw \Rightarrow 1 = xw$ and only holds in an integral domain. Also, the Artin defines irreducible and associate only in an integral domain. To see what goes wrong outside an integral domain, consider $3, 9 \in Z/(12)$. $3 * 9 = 3$ thus $3|9$ and $9|3$ but 3 and 9 do not differ by a unit. Also 3 is clearly not irreducible nor even reducible into finitely many irreducibles.

2.4 Problem 8

Find the gcd of $(11 + 7i, 18 - i)$ in $Z[i]$.

$N(11 + 7i) = 160$, and $N(18 - i) = 325$. So dividing $11 + 7i$ into $18 - i$, we get $(1 - i)$ with a remainder of $3i$.

Since $N(3i) = 9 \leq 1/2N(11 + 7i)$, we have found a valid version of $b = aq + r$. Dividing $3i$ into $(11 + 7i)$ (since $\gcd(a,b) = \gcd(a,r)$ if $N(b) > N(a)$) we get $(-4i + 2)$ with a remainder of $(-1 + i)$.

$N(-1 + i) = 4 \leq 1/2N(9i)$. Dividing $(-1 + i)$ into $(3i)$, I get $(-i + 1)$ with a remainder of i . Since $N(i) = 1 \leq 1/2N(-1 + i)$, this is a valid remainder.

In fact, $N(i) = 1$, means that i is a unit and thus gcd of $(11 + 7i, 18 - i)$ is 1 up to a unit.

3 Chapter 11, Section 3

3.1 Problem 3

• **Proof 1.** Let $f, g \in C[x, y]$ s.t. f is irreducible and suppose $V(f) \subset V(g)$.

By the classical Nullstellensatz (Artin Thm 10.8.7) since g is identically zero on the set $V(f)$, $g^n \in (f)$ for some positive integer n . Thus $f|g^n$. Since f is irreducible, $f|g$.

(NOTE: $f|ab \Rightarrow f|a$ or $f|b$ requires f to be prime, and irreducible only implies prime in a PID which $C[x, y]$ is not. However, in the special case of $f|g \cdots g$, irreducibility is enough:

Assume not, that there exists positive integer j s.t. $f|g^{j+1}$ but $f \nmid g^j$. Then writing out the RHS as irreducibles, $g \cdot g^j = fh_1 \cdots h_n$. Since $C[x, y]$ is a UFD, g must factor into associates of a subset of f, h_1, \dots, h_n . Cancelling those from both sides, $g^j = h_{i_1} \cdots h_{i_m}$ where f does not equal any h_{i_j} otherwise $f|g^j$. However, this implies $f|g$.)

• **Proof 2.** If f is a constant, $f|g$ trivially. Any non-constant bivariate complex polynomial has infinitely many zeros. To see this, imagine letting $f_\alpha(x) = f(x, \alpha)$ and vary α to get an infinite number of zeros. Thus g has infinitely many zeros, hence f and g share an infinite number of zeros. By (Artin Prop. 10.8.8), f and g have a nonconstant polynomial factor in common. Since f is irreducible, $f|g$.

• **Proof 3 (Thanks to Ed Dean).** Let $g(x, y) = p_1(x, y) \cdots p_k(x, y)$ be a factorization of g into irreducibles. Then $V(g) \subset \cup_{i=1}^k V(p_k)$. Let $I(V(f))$ and $I(V(g))$ be the ideal of these varieties. $I(V(g)) = (\prod_{i=1}^k p_k) \subset I(V(f))$. Since f is irreducible, $I(V(f)) = (f)$. Hence f is an associate of p_k thus $f|g$.

3.2 Problem 4

Let $f(x), g(x) \in Z[x] \subset Q[x]$.

• Assume $(f(x), g(x))$ contains an integer $c \in Z$. Then $\exists p(x), q(x) \in Z[x]$ s.t.

$$f(x)p(x) + g(x)q(x) = c.$$

Thus $\exists p_o(x), q_o(x) \in Q[x]$ s.t.

$$f(x)p_o(x) + g(x)q_o(x) = 1$$

and thus the gcd of $f(x)$ and $g(x)$ is 1.

• Assume $f(x)$ and $g(x)$ are relatively prime in $Q[x]$. Thus

$$f(x)p_o(x) + g(x)q_o(x) = 1$$

and clearing the denominators of $p_o(x)$ and $q_o(x)$, $f(x)p(x) + g(x)q(x) = c$, and $(f(x), g(x))$ contains an integer c .