

MODEL ANSWERS TO THE SIXTH HOMEWORK

10. We will repeatedly use the fact that if a polynomial of degree at most three is not irreducible, it must in fact have a root, as it must have a linear factor.

(a) $x^2 + 7$ cannot have a root over \mathbb{R} as $a^2 + 7 \geq 7$, for all $a \in \mathbb{R}$.

(b) This is slightly tricky. Probably the best way to proceed is as follows. Suppose that $a/b \in \mathbb{Q}$ is a root, where a and b are coprime integers. We have

$$(a/b)^3 - 3(a/b) + 3 = 0.$$

Multiplying through by b^3 gives,

$$a^3 - 3ab^2 + 3b^3 = 0.$$

Reducing modulo three, it follows that a is divisible by 3. Thus $a = 3c$, some c . Substituting, we have

$$(3c)^3 - 3^2cb^2 + 3b^3 = 0.$$

Cancelling one power of 3, we have

$$b^3 - 3b^2c + 9c = 0.$$

Reducing modulo three again, we have that b is divisible by three. But this contradicts the fact that a and b are chosen to be coprime.

(c) It suffices to observe that $0 + 0 + 1 = 1 + 1 + 1 = 1 \neq 0$.

(d) Note that we are asking if -1 is a square or not, in \mathbb{Z}_{19} . As $(-a)^2 = a^2$, it suffices to consider $0 \leq a \leq 9$.

$$\begin{array}{cccccc} 0^2 = 0 & 1^2 = 1 & 2^2 = 4 & 3^2 = 9 & 4^2 = 16 & \\ 5^2 = 25 = 6 & 6^2 = 36 = -2 & 7^2 = 49 = 11 & 8^2 = 64 = 7 & 9^2 = 81 = 5 & \end{array}$$

Thus $x^2 + 1$ does not have a root and so it must be irreducible.

(e) Again it suffices to check that 9 is not a cube root in \mathbb{Z}_{13} . As $(-a)^3 = -a^3$, it suffices to check that for $0 \leq a \leq 4$, $a^3 \neq \pm 9 = 9, 4$.

We compute

$$0^3 = 0, \quad 1^3 1^3 = 1, \quad 2^3 = 8, \quad 3^3 = 27 = 1 \quad 4^3 = 64 = 12.$$

(f) We first check that $x^4 + 2x^2 + 2$ does not have any linear factors. This is equivalent to checking that it does not have any roots, which is clear as

$$a^4 + 2a^2 + 2 \geq 2$$

for any real number a .

The only other possibility to eliminate is that it is a product of quadratic factors. Suppose that

$$x^4 + 2x^2 + 2 = f(x)g(x),$$

where both f and g are quadratic. Moving the coefficient of x^2 in f from f to g , we might as well assume that f is monic, that is, its top coefficient is 1. In this case g is monic as well. Thus

$$x^4 + 2x^2 + 2 = (x^2 + ax + b)(x^2 + cx + d),$$

where a, b, c and d are rational numbers. Comparing coefficients of x^3 , we get

$$a + c = 0.$$

Renaming, we get

$$x^4 + 2x^2 + 2 = (x^2 + ax + b)(x^2 - ax + c).$$

Looking at the coefficient of x , we get

$$ac - ab = 0.$$

Thus either $a = 0$ or $b = c$. Suppose $a = 0$. Replacing x^2 by y , we get

$$y^2 + 2y + 2 = (y + a)(y + b),$$

some a and b . In this case the polynomial $y^2 + 2y + 2$ would have a real root. But

$$y^2 + 2y + 2 = (y + 1)^2 + 1$$

so that if $a \in \mathbb{R}$, we have

$$a^2 + 2a + 2 = (a + 1)^2 + 1 \geq 1 > 0.$$

The only remaining possibility is that $b = c$. In this case $b^2 = 2$, which is impossible, as b is a rational number.

13. Let

$$\phi: \mathbb{R} \longrightarrow \mathbb{C}$$

be the obvious inclusion. Applying the universal property of a polynomial ring, define a ring homomorphism

$$\phi: \mathbb{R}[x] \longrightarrow \mathbb{C}$$

by sending x to i . ϕ is obviously surjective as $\mathbb{R} \cup \{i\}$ generates \mathbb{C} . Let I be the kernel. This is an ideal in $\mathbb{R}[x]$. Therefore it must be principal. On the other hand $x^2 + 1$ is clearly in the kernel and $x^2 + 1$ is irreducible over \mathbb{R} , whence prime. It follows that $I = \langle x^2 + 1 \rangle$, and that I is a prime ideal. By the Isomorphism Theorem, the result follows.

14. (a) To show that $x^2 + 1$ is irreducible, it suffices to check that -1 is not a square in F . We compute a^2 , $0 \leq a \leq 5$. We have

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 16 = 5, \quad 5^2 = 25 = 3.$$

Thus $x^2 + 1$ is irreducible. As F is a field, $F[x]$ is a UFD. Thus $x^2 + 1$ is prime. Thus $I = \langle x^2 + 1 \rangle$ is a prime ideal and so

$$L = F[x]/I,$$

is an integral domain.

I claim that every element of L is represented uniquely by a polynomial of the form $ax + b$, where a and b are in F .

First suppose that we have a coset $g + I$. By the division algorithm, we may write

$$g = qf + r,$$

where the degree of r is at most one and $f = p$. Thus $r = ax + b$, for some a and b and moreover $g + I = r + I$.

On the other hand if $ax + b + I = cx + d + I$, then $(a - c)x + (b - d) \in I$. As I is generated by a polynomial of degree two, the only non-zero elements of I have degree at least two. Thus $(a - c)x + b - d = 0$, so that $a = c$ and $b = d$. The claim follows.

In this case L has $121 = 11^2$ elements. As L is finite, it is in fact a field and we are done.

(b) It suffices, repeating the argument above, to show that $x^3 + x + 4$ is irreducible. To prove this we show it does not have any roots. We compute

$$\begin{array}{ll} 0^3 + 0 + 4 = 4 & 1^3 + 1 + 4 = 6 \\ 2^3 + 2 + 4 = 3 & 3^3 + 3 + 4 = 1 \\ 4^3 + 4 + 4 = 5 & 5^3 + 5 + 4 = 4 \\ 6^3 + 6 + 4 = -5^3 - 5 + 4 = 6 & 7^3 + 7 + 4 = -4^3 - 4 + 4 = 2 \\ 8^3 + 8 + 4 = -3^3 - 3 + 4 = 4 & 9^3 + 9 + 4 = -2^3 - 2 + 4 = 3 \\ 10^3 + 10 + 4 = -1^3 - 1 + 4 = 2. \end{array}$$

2. Chapter 4, §6. 1. The map $\phi: \mathbb{Q}[x] \rightarrow \mathbb{Q}[x]$, defined by

$$f(x) \rightarrow f(x + 1)$$

is an automorphism of $\mathbb{Q}[x]$. On the other hand, any isomorphism $R \rightarrow S$ clearly induces a correspondence between the irreducible elements of R and of S .

2. By Gauss' Lemma, it suffices to prove that $x^3 - 3x + 2$ is irreducible over \mathbb{Z} . Suppose not. Then it must factor as

$$x^3 + 3x - 2 = (x + a)(x^2 + bx + c),$$

where a , b and c are all integers. It follows that $ac = 2$, so that a divides 2. In this case, either ± 1 or ± 2 would be a root of $x^3 - 3x + 2$. We compute

$$1^3 + 3 - 2 = 2 \quad (-1)^3 - 3 - 2 = -6, \quad 2^3 + 6 - 2 = 12 \quad (-2)^3 - 6 - 2 = -16.$$

3. By Gauss' Lemma it suffices to prove that $f(x)$ is irreducible over the integers. Let a be any integer which is divisible either by 3 and not by 9, or divisible by 5 and not divisible by 25. By Eisenstein's criterion, applied to $f(x)$ with $p = 3$ or $p = 5$ as appropriate, it follows that $f(x)$ is irreducible. On the other hand there are clearly infinitely many such choices of a .

4. and 5. are proved in the Lecture notes.

6. Let $\phi: R \rightarrow S$ be any ring isomorphism. It is clear that $r \in R$ is irreducible if and only if $\phi(r)$ is irreducible.

7 and 8. follow from 9.

9. By the universal property of a polynomial ring, there is a unique ring homomorphism

$$\phi: F[x] \rightarrow F[x]$$

which sends x to $bx + c$. Thus it suffices to find the inverse map. Let

$$\psi: F[x] \rightarrow F[x]$$

by the unique ring homomorphism which sends x to $(x - c)/b$. The composition sends x to x and by uniqueness the composition is therefore the identity. Thus ϕ is an automorphism.

10. By the uniqueness part of the universal property, it suffices to prove that the image of x has degree one, since if x is sent to $g(x)$, then $f(x)$ is sent to $f(g(x))$, which has degree the product of the degrees of f and g .

Suppose that ϕ is an automorphism of $F[x]$. Note that $F \cup \{x\}$ generates $F[x]$ as a ring. Thus $\phi(x)$ must have the same property. But if $g(x)$ is any element of $F[x]$ the ring generated by $g(x)$ and F is equal to the set of all polynomials of the form $f(g(x))$. Any such polynomial has degree the product of the degrees. Thus to get degree one polynomials, the degree of $g(x)$ must be one. Thus $\phi(x)$ must have degree one.

11. By 10, $\phi(x)$ has degree one. Thus $\phi(x) = bx + c$, where $b \neq 0$. It follows, by the universal property of a polynomial ring, that there is a unique ring homomorphism such that $\phi(f(x)) = f(bx + c)$. We have already seen that any such ϕ is a ring automorphism.

12. Let $b = -1$ and $c = 0$. Then $\phi(x) = -x$ is an automorphism of order two.

13. This has almost nothing to do with polynomials. Let R be any ring which contains a copy of the rationals $F_0 \simeq \mathbb{Q}$. Note that F_0 is generated by 1 as a field. Indeed since F_0 contains a copy of the integers, R_0 , it follows that R has characteristic zero. Let $\phi: R \rightarrow R$ be any automorphism of R . Then $\phi(1) = 1$, by definition. Since R_0 is generated by 1, ϕ acts as the identity on R_0 . Since F_0 is the field of

fractions of R_0 , it follows that ϕ acts on F_0 as the identity (formally, by the universal property of the field of fractions).

14. Let ζ be a primitive n th root of unity. That is, pick $\zeta \in \mathbb{C}$ such that

$$\zeta^n = 1,$$

whilst no smaller power is equal to one. For example

$$\zeta = e^{\frac{2\pi i}{n}}$$

will do. Let $\phi(x) = \zeta x$. Then $\phi(x)$ is an automorphism by 9. Clearly ϕ^n is the identity, but if $m < n$, then ϕ^m is not, as $\phi^m(1) = \zeta^m \neq 1$. Thus ϕ is an automorphism of order n .

3. Chapter 5, §1. 3. (a) Let $f(y) \in T$. Then we may write

$$f(y) = \sum_k b_k y^k$$

where $b_k \in R[x]$. For each k we may write

$$b_k = b_k(x) = \sum_l c_l x^l,$$

where $c_l \in R$.

Applying the distributive law, collecting together like terms and rearranging, it is clear we may expand f in the given form.

(b) Two elements of T are equal if and only if the coefficients of $x^i y^j$ are equal for all i and j .

(c) Add corresponding coefficients.

(d) Suppose that

$$f(x, y) = \sum a_{ij} x^i y^j \quad \text{and} \quad g(x, y) = \sum b_{ij} x^i y^j.$$

Then

$$f(x, y)g(x, y) = \sum c_{ij} x^i y^j,$$

where

$$c_{ij} = \sum_{k,l} a_{kl} b_{i-k, j-l}.$$

4. $D[x, y]$ is naturally isomorphic to $D[x][y]$. As D is an integral domain, it follows that $D[x]$ is an integral domain. But then $D[x][y]$ is also an integral domain.

Bonus Problems 3. Chapter 4 §5 23. To show that $x^3 \pm 2$ is irreducible, it suffices to check that ± 2 is not a cube. It is enough to compute a^3 , for $0 \leq a \leq 3$.

$$0^3 = 0 \quad 1^3 = 1 \quad 2^3 = 8.$$

Thus both of $x^3 \pm 2$ are irreducible. Define a map

$$\phi: R[x] \longrightarrow R[x]$$

by acting as the identity on R and sending x to $-x$. By the universal property of a polynomial ring ϕ is in fact a ring homomorphism. Moreover ϕ is a bijection. Indeed it is own inverse. Thus ϕ is an automorphism.

It is clear that if ϕ is an automorphism of any ring, and I is an ideal of R and $J = \phi(I)$, then

$$R/I \simeq R/J.$$

Set $I = \langle x^3 - 2 \rangle$. Then $J = \langle x^3 + 2 \rangle$ and the result follows.

24. Let

$$\phi: \mathbb{Q}[x] \longrightarrow \mathbb{C}$$

be the ring homomorphism, obtained from the universal property of a polynomial ring, where we send x to α and include \mathbb{Q} into \mathbb{C} . In this case, the image of ϕ is the set

$$\{ a + b\alpha \mid a, b \in \mathbb{Q} \}.$$

Note that $\alpha^2 = -\alpha - 1$, so that this set is indeed closed under multiplication. Now the polynomial $x^2 + x + 1$ has no roots over \mathbb{Q} . Thus it is irreducible. It follows that the ideal $\langle x^2 + x + 1 \rangle$ is prime and that it is the kernel of ϕ . As we are in a PID it is therefore maximal. Thus the quotient is a field and we are done by the Isomorphism Theorem. We write down the inverse of $a + b\alpha$ by hand. In the end, probably the easiest thing is to use the trick of changing variables. Consider the polynomial

$$x^2 + x + 1.$$

If we complete the square, we get

$$(x + 1/2)^2 + 3/4.$$

Changing variable, we set $y = x + 1/2$. Consider the polynomial

$$y^2 + 3/4 = 0.$$

Let β be a root of this polynomial. Possibly switching signs, we have $\alpha = \beta + 1/2$. Thus anything of the form $a + b\alpha$ is also of the form $a + b\beta$ (different a and b of course). The inverse of $a + b\beta$ is easy to compute. Replace this by its conjugate

$$a - b\beta.$$

Then

$$(a - b\beta)(a + b\beta) = a^2 + b^2(3/4) = n$$

So the inverse of

$$a + b\beta$$

is

$$\frac{1}{n}(a - b\beta).$$

25. I don't see how to do this without using some of the results from the next section.