MATH 6302 - Modern Algebra
Homework 9

Joel Sleeba

December 2, 2024

1. **Solution:** Let $\mathbb{F}$ be a field of characteristic 0 and $\mathbf{1}$ be its identity. Then the map

$$\mathbb{Z} \to \mathbb{F} : n \to n\mathbf{1}$$

is an injective ring homomorphism. Hence we see that $\mathbb{F}$ contains an isomorphic copy of $\mathbb{Z}$. Thus it must contain an isomorphic copy of its field of fractions, $\mathbb{Q}$.

If instead $\mathbb{F}$ has characteristic p, then $\mathbb{F} \cong \mathbb{F}_{p^n}$ for some n, then again we see that the subset $\{0, 1, 2, \dots p-1\}$ (where r means $r\mathbf{1}$) is a subfield isomorphic to $\mathbb{F}_p$.

Uniqueness in both of these cases follow from the fact that both the above subfields are generated by the identity element of the field, which is unique.

2. **Solution:** Let $T \subset R \times S$ be an ideal. We'll show that $I = \{r \in R : (r, \cdot) \in T\}$ and $J = \{s \in S : (\cdot, s) \in T\}$ are ideals in R, S and $T = I \times J$.

That $I \times J \subset T$ follows directly from the definition of the product of rings. Conversely if $(r, s) \in T$, then $r \in I, s \in J$ and thus $(r, s) \in I \times J$. Thus $T = I \times J$.

Now we'll show that I is an ideal of R. Let $r \in R$ and $i \in I$. Then there exists $j \in J$ such that $(i, j) \in I \times J$. Since $I \times J$ is an ideal of $R \times S$,

$$(r, 1)(i, j) = (ri, j) \in I \times J$$

Thus we see that $ri \in I$. By a symmetric argument, we'll get that $ir \in I$. Thus I is an ideal of R. The fact that J is an ideal of S follows from a similar argument.

3. **Solution:** Let $A_i = (n_i)$, where $1 \leq i \leq k$, be the ideal generated by the constant polynomials n_i in $R = \mathbb{Z}_d[x]$, the ring of polynomials with degree less than or equal to d. Since $(n_i, n_j) = 1$ for all $i \neq j$, by Bezout's lemma the ideals A_i and A_j are co-maximal whenever $i \neq j$. Then Chineese remainder theorem shows that the canonical map

$$\phi : R/A \to R/A_1 \times R/A_2 \times \ldots \times R/A_k$$

is a ring isomorphism where $A = A_1 \cap A_2 \cap \ldots \cap A_k$. Thus $(f_1 + A_1, f_2 + A_2, \ldots f_k + A_k) \in R/A_1 \times R/A_2 \times \ldots \times R/A_k$ has a pre-image $f + A \in R/A$. Notice that $A_1 \cap A_2 \cap \ldots \cap A_k = (n_1 n_2 \ldots n_k)$. Let $f \in R$ be a representative from $f + A$. We claim that f can be chosen such that the degree of f is d. In case the degree of f is not d, take $g = n_1 n_2 \ldots n_k x^d + f$, where r is the degree of f. Clearly $g \in f + A$, since $n_1 n_2 \ldots n_k x^d \in A$. Thus g is the function which satisfy the requirements of the question.

We'll slightly abuse the definition of A_i and A by viewing it as ideals of either $\mathbb{Z}_d[x]$ or $\mathbb{Z}_{d-1}[x]$ as we need.

Now if f_is are monic polynomials of degree d, consider the polynomials $\tilde{f}_i \in \mathbb{Z}_{d-1}[x]$, where $\tilde{f}_i$ is polynomial removing the x^d term from f. Let $\tilde{f} + A$ be the pre-image of $(\tilde{f}_1 + A_1, \tilde{f}_2 + A_2, \ldots, \tilde{f}_k + A_k)$ under ϕ. Like we did before, we can choose a representative $\tilde{f}$ for $\tilde{f} + A$ with degree $d - 1$. Let $f = x^d + \tilde{f}$. Since f, f_i are monic polynomials, we get that

$$f - f_i = \tilde{f} - \tilde{f}_i \in (n_i) = A_i$$

Thus we see that $f = f_i \mod n_i$ for each $1 \leq i \leq k$. Hence we are done.

4. **Solution:** Division algorithm in polynomial rings shows that for any polynomials $a, b \in \mathbb{F}[x]$, there exist unique polynomials $q, r \in \mathbb{F}[x]$ such that

$$a(x) = q(x)b(x) + r(x)$$

where the $\deg(r) < \deg(b)$. Here $b = f$ and therefore every $g \in \mathbb{F}[x]$ can be written as $g(x) = q(x)f(x) + r(x)$ where $\deg(r) < n = \deg(f)$. Thus we see that $a + (f) = r + (f)$. Hence the number of elements of $\mathbb{F}[x]/(f)$ is the number of all distinct polynomials of degree less than n in $\mathbb{F}[x]$, which is q^n, since $\mathbb{F}$ is a field of order q.

5. **Solution:** We know that for any ring R and an ideal I of R, R/I is a field if and only if I is a maximal ideal. Hence the problem reduces to proving $f \in \mathbb{F}[x]$ is irreducible if and only if (f) is a maximal ideal. One way is easy, if f is

reducible as $f(x) = p(x)q(x)$, where p, q are not units, then $(f) \subsetneq (p) \neq \mathbb{F}[x]$. Thus (f) cannot be a maximal ideal.

To show the converse, note that the existence of the division algorithm for $\mathbb{F}[x]$ makes it a Euclidean domain and hence a PID. Hence irreduciblity and primality coincides in $\mathbb{F}[x]$. Therefore if f is irreducible, then f is prime and (f) is a prime ideal, which again is a maximal ideal.

6. **Solution:** Since $\mathbb{F}[x]$ is a Euclidean domain for every field $\mathbb{F}$, we see that $p \in \mathbb{F}[x]$ is a prime if and only if it is irreducible. Hence the problem reduces to finding infinitely many irreducible elements in $\mathbb{F}[x]$.

   For the sake of contradiction, assume that $\mathbb{F}[x]$ has only finitely many irreducible polynomials. Let $p_1, p_2, \ldots, p_n$ be the exhaustive list of (non-constant) irreducible polynomials.

   $$q(x) = 1 + \prod_{i=1}^{n} p_i(x)$$

   Clearly the degree of $q(x)$ is greater than the degree of all p_i. Hence $q(x) \notin p_i(x)$. We claim that $q(x)$ is irreducible contradicting our assumption. If not, since $\mathbb{F}[x]$ is a UFD, we'll have

   $$q(x) = 1 + \prod_{i=1}^{n} p_i(x) = \alpha \prod_{k} p_{i_k}$$

   where $p_{i_k} \in \{p_1, p_2, \ldots, p_n\}$ and $\alpha \in \mathbb{F}$. This will make each p_{i_k} constant polynomials since

   $$1 = p_{i_k}\Big(\prod_{i=1, i \neq i_k}^{n} p_i - \prod_{k' \neq k} p_{i_{k'}} \Big)$$

   and we know that the only invertible polynomials in $\mathbb{F}[x]$ are the non-zero constant polynomials. This would contradict our assumptions on p_i. Hence we get that $\mathbb{F}[x]$ has infinitely many primes.

7. **Solution:** Since $\mathbb{F}[x]$ is an ED, and hence a UFD, let $p(x) = p_1(x)p_2(x)\ldots p_n(x)$ be a factorization of p into irreducible factors unique upto units. We claim that all the ideals of $\mathbb{F}[x]/(p)$ are those generated by p_i, like $(p_i, p_j, \ldots p_k)/(p)$

From the 4th isomorphism theorem for the rings we know that if I is an ideal of R, $I \subset A \subset R$ is an ideal iff A/I is an ideal of R/I. Here, $R = \mathbb{F}[x]$, $I = (p)$. Hence $A/(p)$ is an ideal of $\mathbb{F}[x]/(p)$ if and only if A is an ideal of $\mathbb{F}[x]$ containing (p). If p has a factorization as above we clearly see that $(p) \subset (p_i, p_j, \ldots p_k)$.

Conversely, if I is any ideal containing p, then I must be contained in a maximal ideal say (q), where q is an irreducible polynomial in $\mathbb{F}[x]$. If $q \notin \{p_1, p_2, \ldots, p_n\}$ then q would be an irreducible factor of p contradicting our assumption. Thus we see that I must be an ideal generated by $p_i, p_j, \ldots p_k$. Thus fourth isomorphism theorem proves our assertion.

8. **Solution:**

   (a) We'll use Eisenstein criterion for $p = 2$. Since $2|a_i$ for all $i = 3, 2, 1, 0$ and $2^2 = 4 \not| 6 = a_0$ satisfies the Eisenstein criterion. Hence it is irreducible.

   (b) Again using Eisenstein criterion with $p = 3$, we see that the polynomial is irreducible.

   (c) Let $x^4 + 4x^3 + 6x^2 + 2x + 1 = (x + 1)^4 - 2x$. Now put $y = x + 1$ to transform the polynomial to $y^4 - 2y + 2$ which is clearly irreducible using Eisenstein criterion with $p = 2$.

   If it was possible to factor $(x + 1)^4 - 2x$ as $(x + 1)^4 - 2x = p(x)q(x)$, then $y^4 - 2y + 2 = p(y - 1)q(y - 1)$, would be reducible. Hence we see that the original polynomial is irreducible.

   (d)

$$(x + 2)^p - 2^p = \sum_{k=1}^{p} \frac{p!}{k!(p - k)!} x^k 2^{p-k}$$

   By Eisenstein criterion for p we get that the polynomial is irreducible, since p divides each $\frac{p!}{k!(p-k)!}$ but $p^2 \not| p$.

9. **Solution:** Since $x^2 + 1$ has no real roots, it is irreducible in $\mathbb{R}[x]$. Hence $(x^2 + 1)$ is a maximal ideal since $\mathbb{R}[x]$ is a PID. Thus $\mathbb{R}[x]/(x^2 + 1)$ is a field. Moreover

$$(ax + b)(cx + d) = acx^2 + (bc + ad)x + bd = (bc + ad)x + (bd - ac) \mod (x^2 + 1)$$

shows that

$$\phi : \mathbb{C} \to \mathbb{R}[x]/(x^2+1) := (a+ib) \to a + xb + (x^2+1)$$

is a ring homomorphism. Surjectivity of ϕ follows from the division algorithm on $\mathbb{R}[x]$. Also if $\phi(a+ib) = \phi(c+id)$, then $a-c+x(b-d) \in (x^2+1)$ which forces $a-c+x(b-d) = 0$ and hence $a+ib = c+id$. Hence we see that ϕ is a ring isomorphism.

10. **Solution:** Since $\mathbb{F}_{11}[x]$ is a Euclidean domain, by the division algorithm, every element of $\mathbb{F}_{11}[x]/(x^2+1)$ has a representative of the form $ax+b \in \mathbb{F}_{11}[x]$. Moreover $ax+b \in cx+b+(x^2+1)$ if and only if $(a-c)x+(b-d) \in (x^2+1)$ if and only if $(a-c)x+(b-d) = 0$. Thus we see that distinct polynomials $ax+b$ are in distinct classes of $\mathbb{F}_{11}[x]/(x^2+1)$. Since there are $11 \times 11 = 121$ polynomials of the form $ax+b$ in $\mathbb{F}_{11}[x]$, we see that there are 121 elements in $\mathbb{F}_{11}[x]/(x^2+1)$. That $\mathbb{F}_{11}[x]/(x^2+2x+2)$ also have 121 elements follow from the same reasoning.

    To show that the above rings are fields, it is enough to show that the polynomials x^2+1 and x^2+2x+2 are irreducible in $\mathbb{F}_{11}[x]$. This is because maximality and primality of ideals, and irreducibility and primality of elements agree on PIDs.

    To show that x^2+1 is irreducible it is enough to show it has no roots on $\mathbb{F}_11$. For the sake of contradiction, assume that $a^2+1 = 0 \mod 11$. Then $a^2 = 10$ mod 11 forces $a^2 = 11n+10$ forces a to be odd. We can verify that a cannot be either $1, 3, 5, 7, 9, 11$, exhausting every "odd" numbers in $\mathbb{F}_{11}$. Thus we see that x^2+1 does not have any root in $\mathbb{F}_{11}$. Hence x^2+1 is irreducible in $\mathbb{F}_{11}$.

    Since $x^2+2x+2 = (x+1)^2+1$, by the above reasoning, we see that x^2+2x+2 is also irreducible in $\mathbb{F}_{11}$. Hence the above quotient rings are indeed fields.

    Consider the map

    $$\phi : \mathbb{F}_{11}[x] \to \mathbb{F}_{11}[x] := p(x) \to p(x+1)$$

    We claim that the corresponding natural map

    $$\tilde{\phi} : \mathbb{F}_{11}[x]/(x^2+1) \to \mathbb{F}_{11}[x]/(x^2+2x+1) := [p(x)] \to [p(x+1)]$$

    is a well defined ring homomorphism.

    To prove the well definess of the map let $p(x) = ax+b+(x^2+1)q(x)$ for some $q(x) \in \mathbb{F}_{11}[x]$ such that $p(x) \in [ax+b]$. Then

    $$\phi(p(x)) = p(x+1) = ax+a+b+(x^2+2x+2)q(x+1)$$

shows that $\phi(p(x)) \in [\phi(ax+b)] = [ax+a+b]$. Thus we see that $\tilde{\phi}$ is a well defined map.

To show that $\tilde{\phi}$ is a ring homomorphism, consider $[ax+b], [cx+d] \in \mathbb{F}_{11}[x]/(x^2+1)$. Then

$$\begin{aligned}
\tilde{\phi}([ax+b]+[cx+d]) &= \tilde{\phi}([(a+c)x+(b+d)]) \\
&= [(a+c)x+(a+c)+(b+d)] \\
&= [ax+a+b]+[cx+c+d] \\
&= \tilde{\phi}([ax+b])+\tilde{\phi}([cx+d])
\end{aligned}$$

and

$$\begin{aligned}
\tilde{\phi}([ax+b][cx+d]) &= \tilde{\phi}([acx^2+(ad+bc)x+bd]) \\
&= \tilde{\phi}([(ad+bc)x+(bd-ac)]) \\
&= [(ad+bc)x+(ad+bc)+(bd-ac)] \\
&= [ac(x^2+2x+2)+(ad+bc)x+(ad+bc)+(bd-ac)] \\
&= [acx^2+(2ac+ad+bc)x+(ad+bc+bd+ac)] \\
&= [ax+a+b][cx+c+d] \\
&= \tilde{\phi}([ax+b])\tilde{\phi}([cx+d])
\end{aligned}$$

show that $\tilde{\phi}$ is a ring homomorphism and therefore a Field isomorphism.

11. **Solution:**

(a) We know that

$$\begin{aligned}
x^8-1 &= (x^4+1)(x^4-1) \\
&= (x^4+1)(x^2+1)(x^2-1) \\
&= (x^4+1)(x^2+1)(x+1)(x-1)
\end{aligned}$$

and

$$\begin{aligned}
x^6-1 &= (x^3+1)(x^3-1) \\
&= (x+1)(x^2-x+1)(x^2+x+1)(x-1)
\end{aligned}$$

Since x^2+1, x^2-x+1, and x^2+x+1 are irreducible in $\mathbb{Q}[x]$ having no roots, they are irreducible in $\mathbb{Z}[x]$. Moreover x^4+1 does not have any rational roots, so if it decomposes into factors, it must decompose as a product of two degree two polynomials in $\mathbb{Q}[x]$. Also we can verify that x^4+1 factors into

$$x^4 + 1 = (x^2 + 1 - 2\sqrt{x})(x^2 + 1 + 2\sqrt{x})$$

in $\mathbb{Q}[x]$. Since $\mathbb{Q}[x]$ is a UFD, this factorization is unique upto multiplication by units. Hence we see that x^4+1 is irreducible in $\mathbb{Z}[x]$. Thus the above is the decomposition of the above polynomials into irreducible factors in $\mathbb{Z}[x]$.

(b) In $\mathbb{Z}/2\mathbb{Z}[x]$, we have $x^2+1 = x^2+2x+1 = (x+1)^2$, and $x-1 = x+1$. Also $x^4+1 = (x^2+1)^2 - 2x^2 = (x^2+1)^2 = (x^2+2x+1)^2 = (x+1)^4$. Combining all of this together, we get

$$x^8 - 1 = (x+1)^8$$

Similarly, $x^2-x+1 = x^2+x+1$. Since $\mathbb{Z}/2\mathbb{Z}$ is a field and x^2+x+1 has no roots in it, we see that x^2+x+1 is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$. Thus

$$x^6 - 1 = (x^2+x+1)^2(x+1)^2$$

(c) In $\mathbb{Z}/3\mathbb{Z}[x]$, x^2+1 is irreducible since it has no roots. Moreover x^4+1 is irreducible for the same reasons why it is irreducible in $\mathbb{Z}[x]$. Thus we get

$$x^8 - 1 = (x^4+1)(x^2+1)(x+2)(x+1)$$

Similarly, note that $x^2-x+1 = x^2+2x+1 = (x+1)^2$, $x^2+x+1 = x^2+4x+4 = (x+2)^2$, and $x-1 = x+2$. Thus we see that

$$x^6 - 1 = (x+2)^3(x+1)^3$$

12. **Solution:** Let $\mathbb{F}$ be a finite field. Then by Solution 6, we see that $\mathbb{F}[x]$ has infinitely many irreducible elements. Since $\mathbb{F}$ is finite, there are only finitely many polynomials of the form $ax+b$, where $a, b \in \mathbb{F}$. Therefore there must be non-linear irreducible polynomials in $\mathbb{F}[x]$. This shows that $\mathbb{F}$ is not algebraically closed.

13. **Solution:** Consider the polynomial $x^4 + x + 1$ in $\mathbb{F}_2[x]$. We claim that this is an irreducible polynomial. Since it has no roots, it can only be reduced into quadratic polynomials. But since the only irreducible quadratic polynomial is $x^2 + x + 1$, and $(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq x^4 + x + 1$, we get that $x^4 + x + 1$ is irreducible. Thus $x^4 + x + 1$ is a maximal ideal and hence $\mathbb{F}_2[x]/(x^4 + x + 1)$ is a field. Moreover by the division algorithm and using the same reasoning as in solution 10, we see that $\mathbb{F}_2/(x^4 + x + 1)$ is a field of 16 elements.

    Since we know that any finite subgroup of the mulitplicative group of a field is cyclic, we get that multiplicative group of $\mathbb{F}_2[x]/(x^4 + x + 1)$ is cyclic of order 15. We can show that $x^3 + x^2 + 1$ is not of the order 3 or 5 hence must have order 15. Moreover since this is a cyclic group of order 15, it has $\phi(15) = 4 \times 2 = 8$ generators.