Math 122, PSET 10 Solutions
By Sam Lewallen, which some additions by Tien Anh

1. (a) $\Rightarrow$: Assume $R' = R/I$ is an integral domain. Take $ab \in I \subset R \Rightarrow \overline{ab} = 0 \in R/I \Rightarrow \overline{a} = 0$ or $\overline{b} = 0 \Rightarrow a \in I$ or $b \in I \Rightarrow I$ is a prime ideal.

   $\Leftarrow$: Assume I is a prime ideal. Then, if $\overline{ab} = 0 \in R'$ ($\overline{ab}$ is what an arbitrary product looks like in R', because $\overline{a}\overline{b} = \overline{ab}$), it follows that $ab \in I \subset R$. Then, either $a \in I$ or $b \in I \Rightarrow$ either $\overline{a} = 0$ or $\overline{b} = 0$, so we conclude that R' is an integral domain.

   (b) Let M be a maximal ideal of R. Then $R/M = R'$ is a field, which is also an integral domain by definition. Thus, by (a), M must be prime.

   (c) Take $ab \in \varphi^{-1}(P')$. Then, $\varphi(ab) = \varphi(a)\varphi(b) \in P'$, so that either $\varphi(a)$ or $\varphi(b)$ is in P', implying that either a or b is in $\varphi^{-1}(P')$.

   (d) Sam's Solution Given the trivial ring R and a field F, the unique homomorphism $\varphi : R \to F$ sends $0 \in R \mapsto 0 \in F$. $\{0_F\}$ is a maximal ideal in F, however, $\varphi^{-1}(0_F) = \{0_R\}$ is not maximal in R, because $\{0_R\} \neq R$ is not satisfied.
   Alternative solution: consider the inclusion homomorphism $f : Z \to Q$, the preimage of the ideal $\{0\}$ is $\{0\}$,but in $Q, \{0\}$ is a maximal ideal, as Q is a field. However, in Z, $\{0\}$ is not maximal (but is a prime ideal as Z is a domain) as it is contained in all other ideals $\{a\}$, for $a \in Z$

2. Take some non-zero element $a \in F$ where F is a finite integral domain. Then, a^m must equal a^n for some $n \neq m \in \mathsf{N}$, because there are only finitely many values that powers of a can attain. Without loss of generality, assume $m > n$. Then,

$$a^m = a^n$$

$$a^m - a^n = 0$$

$$a^n(a^{m-n} - 1) = 0$$

   Thus, $a^n = 0$ or $(a^{m-n} - 1) = 0$. However, a^n cannot equal 0 because $a \neq 0$, and 0 has no non-zero divisors in an integral domain. (Technically, we can build up an induction argument to show that $a \neq 0 \Rightarrow a^2 \neq 0 \Rightarrow \cdots \Rightarrow a^n \neq 0$.) Thus,

$$a^{m-n} - 1 = 0$$

$$a^{m-n} = 1$$

$$a(a^{m-n-1}) = 1$$

   Thus, $(a^{m-n-1}) = a^{-1}$. This is true for arbitrary a, so we conclude that every $a \in F$ has an inverse. It follows that F is a field.
   Alternatively, let $\{0, a_1, a_2, \ldots, a_n\}$ be the elements of F, and consider the set $\{0, a_1 * a_1, a_1 * a_2, a_1 * a_3, \ldots, a_1 * a_n\}$, we can see that $a_1 * a_k - a_1 * a_m = a_1 * (a_k - a_m) \neq 0$ for $k \neq m$ (here we assume that $a_1 \neq 0$ as otherwise it is the trivial case),by the fact that F is an integral domain thus the new set contains n distinct elements, which is equal to the order of F. As such, one of the product $a_1 * a_k$ corresponds to the element 1. Hence we just find the multiplicative

inverse for a_1, and since we can repeat the same argument for all k, we know that all non-zero elements of F has an inverse, or F is indeed a field.

We have shown that the order of any finite field must either be prime or a power of a prime. We have just shown that any finite integral domain is a finite field, so that every finite integral domain must have a prime or a power of a prime's worth of elements. Thus, no integral domain can have 10 elements.

3. (a) Take $g, f \in R[X]$, $f = a_0 + a_1x + a_2x^2 \cdots + a_nx^n$, $g = b_0 + b_1x + b_2x^2 \cdots + b_mx^m$. Assume $g, f \neq 0$, so that, in particular, $a_n, b_m \neq 0$. Then, the degree of the leading term of gf is $n + m$ and it has coefficient a_nb_m, because the only two terms of f and g that multiply to give a multiple of x^{n+m} are a_nx^n and b_mx^m. However, $a_nb_m \neq 0$, because $a_n, b_m \neq 0 \in R$, and R is an integral domain. Thus, $gf \neq 0$. We conclude that $gf \neq 0$ if $g \neq 0$ and $f \neq 0$, so that $R[X]$ is an integral domain.

   (b) By our previous argument, the degree of the product of two polynomials is greater than or equal to the degrees of each of the factors in $R[X]$, if R is an integral domain. Thus, given some non-constant polynomial g, fg has degree greater than or equal to that of g and thus is also a non-constant polynomial, for any $f \in R[X]$. Thus, gf cannot be 1, which is constant. We conclude that the only candidates for units in $R[X]$ are those elements of the subring $R \subset R[X]$. Of course, any element in the subring $R \subset R[X]$ is a unit iff it is a unit in R, because we can construct an isomorphism from R to $R \subset R[X]$. We conclude that the units in $R[X]$ are precisely the units of R.

4. Proposition 11.2.14 of Artin tells us that $R/(p)$ is a field iff p is irreducible in R. Thus, $\mathsf{F}_2[X]/(X^3 + X + 1)$ is a field by problem (6) part (a). However, over F_3, we can discover by computation that $x^3 + x + 1 = (2x^2 + 2x + 1)(2x + 1) = 4x^3 + 6x^2 + 4x + 1 \equiv x^3 + x + 1$, so that $X^3 + X + 1$ is not irreducible in $\mathsf{F}_3[X]$, and thus $\mathsf{F}_3[X]/(X^3 + X + 1)$ is not a field.

5. Assume otherwise, that is, that there are finitely many irreducible monic polynomials in $F[X]$. Thus, is there is some finite set $P = \{p_1, \ldots, p_n\}$ of irreducible monics. Let $f = \Pi p_i$, the product of the p_i's over all i. Thus, f is divisible by each of the p_i. Now, $f + 1$ is not in P, because, in particular, if there is more than one polynomial in P, then $f + 1$ will have degree greater than all the polynomials in P, and if there is only one polynomial in P, then $f + 1$ will be this polynomial plus 1, and thus will not be equal to it. Thus, f is not irreducible, so it can be written as a product of irreducible polynomials, so that, in particular, $\exists i$ s.t. $p_i \mid f + 1$. We already know that $p_i \mid f$, by construction; thus, $p_i \mid (f + 1 - f) = 1$. That is, $\exists$ $h \in F[X]$ s.t. $p_ih = 1$. However, the only elements in $F[X]$ which have inverses are the units in F, which cannot be irreducible by definition $\Rightarrow\Leftarrow$. We conclude that P cannot be finite, so that there must be infinitely many irreducible monics in $F[X]$.

6. (a) If $X^3 + X + 1$ were reducible, we would have

$$X^3 + X + 1 = (AX^2 + BX + C)(DX + E)$$

$$= ADX^3 + (EA + BD)X^2 + (BE + CD)X + EC$$

from which

$$AD = EC = 1 \Rightarrow A = D = E = C = 1$$

Then,

$$B + 1 = 1 \Rightarrow B = 0$$

$$\Rightarrow 1 + 0 = 0 \Rightarrow\Leftarrow$$

We conclude that $X^3 + X + 1$ is irreducible over F_2. (Alternatively, you can list out all possible linear factors and show that none of them divide the polynomial, hence $X^3 + X + 1$ is not factorizable (irreducible).

(b) Here we have $X^2 - 3X - 3 = (AX + B)(CX + D) = ACX^2 + (BC + DA)X + BD$. We can tell by educated trial and error that one solutions is $A = D = 2, C = 3, B = 1$, so that we can factor $X^2 - 3X - 3$ as $(2X + 1)(3X + 2) \equiv 2 \cdot 3(X + 3)(X + 4) \equiv (\mathbf{X} + \mathbf{3})(\mathbf{X} + \mathbf{4}) = X^2 + 7X + 12 \equiv X^2 - 3X - 3$ over F_5. (Alternatively, we could have calculated the roots of $X^2 - 3X - 3$).

(c) $X^2 + 1$ is of degree 2, so, if it is reducible, its irreducible factors will both be linear, and thus, will correspond to roots over F_5. However, $X^2 + 1$ has only imaginary roots, and thus has no roots over F_5. We conclude that it is irreducible in $\mathsf{F}_5[X]$.

7. Let d be the gcd of f and g in $\mathsf{Q}[X]$, and let d' be the gcd in $\mathsf{C}[X]$. Now, we know that $(d) = (a, b)$ in $\mathsf{Q}[X]$, and that $(d') = (a, b)$ in $\mathsf{C}[X]$. Because $\mathsf{Q}[X]$ is naturally contained in $\mathsf{C}[X]$ (because Q is a subfield of C), $(a, b) \subset \mathsf{Q}[X]$ is a subset of $(a, b) \subset \mathsf{C}[X]$. Thus, $(d) \subset (d')$, when d is considered as an element of $\mathsf{C}[X]$ in the natural way. This tells us that d' divides every element in (d), in particular, $d' \mid d$. Now, again consider d as an element of $\mathsf{C}[X]$. d must still divide f and g, so that, by the defining property of gcd, it also divides d'. Thus, we have $d \mid d'$. $d \mid d', d' \mid d \Rightarrow d = d'$, as desired.