Solutions to the Midterm, Math 525

Problem 1. Let $S_5 = \left\{ a + b\left(\frac{1+\sqrt{5}}{2}\right) : a, b \in \mathbb{Z} \right\}$.

a) Explain why S_5 is a UFD.

b) Show that the multiplicative group $S_5^\times$ is infinite (this is very easy!).

c) Let I be a non-zero ideal of S_5. Prove that there is n such that $1 - u^n \in I$ for all units u in $S_5^\times$. Hint: What do you know about S_5/I?

d) Describe all subrings of S_5.

e) Let R be a subring of S_5, $R \neq \mathbb{Z}$. Prove that:

(1) There is a non-zero ideal I of S_5 such that $I \subseteq R$.
(2) The group of units $R^\times$ is infinite.
(3) If P is a non-zero prime ideal of R then P is maximal.

f) Let $R = \mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} : a, b \in \mathbb{Z}\}$. Prove that 2, $1+\sqrt{5}$, $1-\sqrt{5}$ are irreducible in R. Conclude that R is not a UFD.

g) Let R be as in f). Let $I =< 2, 1+\sqrt{5} >$. Show that $I^2 = 2I$. Is there an n such that I^n is principal?.

Solution. a) Write $\omega = (1+\sqrt{5})/2$. Recall that we have a function $N : S_5 \longrightarrow \mathbb{Z}$, $N(a+b\omega) = a^2 + ab - b^2 = (a + b/2)^2 - 5b^2/4$, called the norm. The absolute value $|N|$ of the norm is an Euclidean function on S_5 and therefore S_5 is a Euclidean ring, hence a PID and a UFD.

To see that $|N|$ is a Euclidean function, take $x, y \in S_d$, $x \neq 0$ and consider $y/x = p + q\omega$ for some rational numbers p, q. Take an integer n closest to q, so $|q - n| \leq 1/2$. Then take an integer m closest to $p + (q-n)/2$, so $|((p-m) + (q-n)/2| \leq 1/2$. Then

$$|N((p+q\omega) - (m+n\omega))| = ||((p-m) + (q-n)/2|^2 - 5|q-n|^2/4| \leq$$

$$|((p-m) + (q-n)/2|^2 + 5|q-n|^2/4 \leq 1/4 + 5/16 = 9/16 < 1.$$

Thus $|N(y/x - (m+n\omega))| < 1$, so $|N(y - (m+n\omega)x)| < |N(x)|$. This proves that $|N|$ is a Euclidean function on S_5.

b) Note that $\omega > 1$ and $\omega \in S_5^\times$ (since $\omega(-\omega^*) = 1$). Thus $1 < \omega < \omega^2 < \omega^3 < \ldots$ is an infinite sequence of distinct elements in $S_5^\times$.

c) If I is a non-zero ideal of S_5 take any $a \in I$, $a \neq 0$. Then $aa^* = N(a) \in I$, so I contains an integer $m \geq 1$. Thus $mS_5 \subseteq I$ and $S_5/mS_5 \cong (\mathbb{Z} \times \mathbb{Z})/(m\mathbb{Z} \times m\mathbb{Z})$ is finite (has m^2 elements). Thus S_5/I is a finite ring and its multiplicative group $(S_5/I)^\times$ is a finite group. If n is the order of this group, then $w^n = 1$ for any unit $w \in S_5/I$. If u is a unit in S_5 then $u + I$ is a unit in S_5/I, so $u^n + I = 1 + I$. In other words, $1 - u^n \in I$ for every $u \in S_5^\times$.

d) Let R be a subring of S_5. Since $1 \in R$, $m+n\omega \in R$ if and only if $n\omega \in R$. The set $\{n \in \mathbb{Z} : n\omega \in R\}$ is a subgroup of $\mathbb{Z}$, so it is equal to $k\mathbb{Z}$ for some $k \geq 0$. It follows that $R = R_k = \{m+kn\omega : m, n \in \mathbb{Z}\}$ for some $k \geq 0$. We see that the subrings of R are exactly the rings R_k, $k = 0, 1, \ldots$.

e) We have $R = R_k$ for some $k > 0$ (since $R_0 = \mathbb{Z}$). Then $I = kS_5$ is a non-zero ideal of S_5 contained in R. This justifies (1). Let n be as in part c) for the ideal I. Then $1 - u^n \in I$ for every unit u of S_5. Thus $1 - u^n \in R$, so $u^n \in R$. Thus ω^{dn}, $d = 1, 2, \ldots$ is an infinite collection of units in R. This proves (2).

Remark. Note that if u is a unit in S_5 and $u \in R$ then u is a unit in R since $uu^* = \pm 1$ and $u^* \in R$.

Let $P \neq \{0\}$ be an ideal in R. Then for $a \in P$, $a \neq 0$, we have $aa^* \in P$, so P contains a non-zero integer m. Since additively $R \cong \mathbb{Z} \times \mathbb{Z}$, R/mR is finite, so R/P is finite. If P is a prime ideal then R/P is a finite integral domain, hence a field. This means that P is a maximal ideal. This proves (3).

f) Note that $x \in R$ is invertible iff $N(x) = \pm 1$. Suppose $a \in R$ is not irreducible. Then $a = bc$ for some b, c in R which are not invertible. Taking norms, we have $N(a) = N(b)N(c)$ and $|N(a)| \geq 2$, $|N(c)| \geq 2$. Taking a to be one of $2, 1 \pm \sqrt{5}$, we see that $4 = N(b)N(c)$. This means that $N(b) = N(c) = \pm 2$. Now if $N(m + n\sqrt{5}) = m^2 - 5n^2 = \pm 2$ then $m^2 \equiv \pm 2 \pmod 5$. However ± 2 is not a square modulo 5 ($0, 1, 4$ are the only squares in the field $\mathbb{F}_5$). Thus there is no element in R of norm ± 2 and therefore the elements $2, 1 \pm \sqrt{5}$ are irreducible. Note that 2 is not associated to $1 \pm \sqrt{5}$ (as $1 \pm \sqrt{5} \neq 2a$ for $a \in R$) and $2^2 = -(1 + \sqrt{5})(1 - \sqrt{5})$, so R is not a UFD.

g) We have

$$I^2 =< 2^2, 2(1+\sqrt{5}), (1+\sqrt{5})^2 >=< 2^2, 2(1+\sqrt{5}), 2(3+\sqrt{5}) >= 2 < 2, 1+\sqrt{5}, 3+\sqrt{5} >= 2I.$$

It follows by straightforward induction that $I^n = 2^{n-1}I$ for $n \geq 1$. If $I^n = aR$ was principal for some n then $aR = 2^{n-1}I$, so $b = a/2^{n-1} \in R$ and $I = bR$. Thus $I = bR$ would be a principal ideal. So $b|2$ and $b|1 + \sqrt{5}$ in R. Since 2, $1 + \sqrt{5}$ are irreducible and b is not invertible, b would be associated with both 2 and $1 + \sqrt{5}$. We have seen in part f) that this is not possible.

Problem 2. Consider a polynomial $f = x^2y^{15} + x^{15}y + x^2 - y - 1$ in $\mathbb{Q}[x, y]$. Prove that f is a prime element in $\mathbb{Q}[x, y]$. Hint: Consider f as a polynomial in $R[y]$, where $R = \mathbb{Q}[x]$. Looking at the quotient ring $(R/(1 - x))[y]$ may be helpful.

Solution. Recall the following result.

Eisenstein Criterion. *Let $f(x) = f_0 + f_1x + \ldots + f_nx^n$ be a polynomial in $R[x]$, where R is an integral domain. Suppose that there is a prime ideal P of R such that $f_n \notin P$, $f_0, f_1, \ldots, f_{n-1} \in P$ and $f_0 \notin P^2$. Then if $f = gh$ for some $g, h \in R[x]$, then one of g, h is constant.*

We have $f = x^2y^{15} + (x^{15} - 1)y + (x^2 - 1) \in R[y]$. Not that $R = Q[x]$ is a PID, hence a UFD. It follows that $R[y]$ is a UFD, so it suffices to show that f is irreducible in $R[y]$ (in UFD's irreducible elements are prime). We will use the Eisenstein criterion. Note that $P = (1 - x)R$ is a prime ideal of R as $1 - x \in R$ is irreducible in R (hence prime). Note that $x^2 \notin P$, all the other coefficients of f are in P (as $1 - x$ divides both $x^{15} - 1$ and $x^2 - 1$) and $x^2 - 1$ is not in P^2 (as $(x - 1)^2$ does not divide $x^2 - 1$). By Eisenstein criterion, if $f = gh$ for some $g, h \in R[y]$ then one of g, h is in R (i.e. is constant as a polynomial in y). Since f is primitive (i.e. $\gcd(x^2, x^{2017} - 1, x^2 - 1) = 1$ in R), this constant must be invertible in R. This proves that f is irreducible.

Problem 3. Let p be a prime and let F be a field with p^n elements. Prove that F has a subfield with p^k elements if and only if $k|n$.

Solution. Let $\mathbb{F}_p$ be the prime subfield of F. We know that F consists of all the roots of the polynomial $x^{p^n} - x = x(x^{p^n-1} - 1)$. If $k|n$ then $n = km$ and $p^n - 1 = p^{km} - 1$ is divisible by $p^k - 1$: $p^n - 1 = (p^k - 1)M$ for some positive integer M. Thus $x^{p^n-1} - 1$ is divisible by $x^{p^k-1} - 1$, so $x^{p^k} - x$ divides $x^{p^n} - x$. This means that all roots of $x^{p^k} - x$ are in F, i.e. F contains a subfield with p^k elements.

Slightly different argument: The multiplicative group $F^\times$ is cyclic of order $p^n - 1$. Since $k|n$ we have $p^k - 1|p^n - 1$, so $F^\times$ has a cyclic subgroup S of order $p^k - 1$, and then $S \cup \{0\}$ are roots of $x^{p^k} - x$ so $K = S \cup \{0\}$ is a field with p^k elements.

Conversely, suppose that K is a subfield of F with p^k elements. Then F is a vector space over K of some dimension d, so $F \cong K^d$ as K-vector spaces and therefore $|F| = p^{kd} = p^n$. Thus $n = kd$ and $k|n$.

Slightly different argument: The group $K^\times$ has $p^k - 1$ elements and it is a subgroup of the group $F^\times$ with $p^n - 1$ elements. Thus $p^k - 1$ divides $p^n - 1$. Writing $n = dk + r$ with $0 \leq r < k$ we have $p^n - 1 = (p^{dk} - 1)p^r - (p^r - 1)$ so $p^k - 1$ divides $p^r - 1$ and therefore $r = 0$.

Problem 4. Let I be an ideal in a commutative ring R and let P_1, P_2, P_3 be ideals of R.

a) Suppose that $I \subseteq P_1 \cup P_2$. Prove that $I \subseteq P_1$ or $I \subseteq P_2$.

b) Suppose that $I \subseteq P_1 \cup P_2 \cup P_3$ and P_3 is a prime ideal. Prove that $I \subseteq P_i$ for some i.

Solution. a) Suppose that I is not contained in P_1. Take $s \in I$, $s \notin P_1$. Then $s \in P_2$. Take any $x \in I$, then one of x or $x + s$ is not in P_1 (if both were in P_1 then s would be in P_1). Thus either x or $x + s$ is in P_2. This implies that $x \in P_2$ (since $s \in P_2$). Thus I is contained in P_2.

b) Suppose that $I \subseteq P_1 \cup P_2 \cup P_3$ and P_3 is a prime ideal. If $I \subseteq P_k \cup P_j$ for some j, k then we can use part a) to conclude that $I \subseteq P_i$ for some i. Suppose this is not true for any choice of k, j. We show that this assumption leads to a contradiction. In fact, the following holds:

(1) there is $a \in I$ such that $a \notin P_1$, $a \notin P_2$, $a \in P_3$.
(2) there is $b \in I$ such that $b \in P_1$, $b \notin P_2$, $b \notin P_3$.
(3) there is $b \in I$ such that $c \notin P_1$, $c \in P_2$, $c \notin P_3$.

Since P_3 is prime, we have $bc \notin P_3$, so $a + bc \notin P_3$. Since $bc \in P_1$ and $bc \in P_2$ then $a + bc \notin P_1$ and $a + bc \notin P_2$. Thus $a + bc$ is in I but not in any P_i, a contradiction.

Remark. It is not hard to extend the argument above to show that if $P_1, \ldots, P_n$ are ideals in R such that $P_3, \ldots, P_n$ are prime and $I \subseteq P_1 \cup \ldots \cup P_n$ then $I \subseteq P_i$ for some i.

Problem 5. Let R be a commutative ring.

a) Show that among the ideals which are not principal there is a maximal one (with respect to inclusion). Pick one such ideal and call it I.

b) Prove that either I is a maximal ideal or there is $a \in R$ which is not invertible such that $aI = I$.

c) Prove that if R is a Noetherian integral domain in which every irreducible element generates a maximal ideal then R is a PID.
****
The rest of this problem is optional for extra credit.

d) Suppose that $J =< c_1, \ldots, c_k >$ is a finitely generated ideal in R such that $aJ = J$. Use induction on k to prove that there is $r \in R$ such that $(1 + ra)x_i = 0$ for all i. Hint: Work with R/x_kR for the inductive step. Note that $aI = I$ implies that $x_k = as_1x_1 + \ldots + as_kx_k$ for some $s_i \in R$. (There are also ways of proving this without induction).

e) Returning to part b), assume I is not maximal and I is finitely generated. From part d) we have $(1 + ar)I = 0$ for some $r \in R$. Prove that $1 + ar \notin I$. Let $N = \{s \in R : sI = 0\}$. Prove that N is an ideal of R not contained in I. Conclude that $I + N = dR$ is principal. Prove that $dI = I$. Conclude that there is $w \in I$ such that $wI = I$. Conclude that $I = wR$ is principal, a contradiction.

f) Prove that if R is Noetherian and every maximal ideal in R is principal then every ideal in R is principal (we are not assuming here that R is a domain).

Solution. a) Suppose that we have a chain $(J_s)_{s\in T}$ of ideals which are not principal. The union J of this chain is an ideal. It can not be principal: if $J = aR$ then $a \in J_s$ or some s and therefore $J = J_s$, which must be false as J_s is not principal. Thus, by Zorn's Lemma, if the set of non-principal ideals is not empty then it contains maximal elements.

b) Let I be maximal among the non-principal ideals of R. Then any ideal strictly containing I is principal. If I is not a maximal ideal then $I \subsetneq M$ for some ideal M in R (you can take M maximal, but it does not matter). Thus $M = aR$ is principal, and a in not invertible. Let $J = \{r \in R : ar \in I\}$. Then J is an ideal and $aJ = I$ (since $I \subseteq aR$). Clearly $I \subseteq J$. If $I \neq J$ then $J = bR$ is principal and then $I = aJ = abR$ is principal, a contradiction. This shows that $J = I$ and $I = aI$.

c) Recall that we proved that a commutative domain is a UFD if and only if it has ACCP and every irreducible element is prime. Since maximal ideals are prime and Noetherian rings have ACCP, R is a UFD. Suppose that R is not PID, so R has non-principal ideals. Then by part b) R has a non-zero ideal I such that $aI = I$ and a is not invertible. It follows that $I = a^nI$ for all positive integers n. Let p be an irreducible factor of a. Take any $x \in I$, $x \neq 0$. Then $a^n|x$ for all n, so $p^n|x$ for all n. This clearly contradicts the unique factorization property.

A different argument: We know that R is UFD. If M is a maximal ideal of R and $x \neq 0$ is an element of M then $x = p_1 \ldots p_k$ for some irreducible elements p_i. Since M is maximal, $p_i \in M$ for some i, so $p_iR \subseteq M$. Since p_iR is maximal, we get $M = p_iR$. Thus every maximal ideal in R is principal. Since R is a UFD, for every $a \in R$ which is non-invertible and non-zero we define $\pi(a)$ as the number of irreducible factors in any factorization of a into a product of irreducible elements. For a proper ideal $I \neq \{0\}$ of R we define $m(I)$ as the smallest value $\pi(a)$ among non-zero $a \in I$. Now we prove on induction on $m(I)$ that every proper ideal $I \neq \{0\}$ is principal. If $m(I) = 1$ then I contains an irreducible element p and therefore $pR \subseteq I$. Since pR is maximal, we have $I = pR$ is principal. Suppose now that $m(I) = n \geq 2$. I is contained in a maximal ideal pR for some irreducible p. Then $J = \{a/p : a \in I\}$ is an ideal of R, $I = pJ$, and $m(J) = m(I) - 1$. By inductive assumption, $J = bR$ is principal so $I = pJ = pbR$ is principal.

d) We prove a more general result:

Theorem. Let R be a commutative ring, J a finitely generated ideal of R and K an ideal such that $KJ = J$. Then $(1-k)J = \{0\}$ for some $k \in K$.

Part d) is a special case of this result when $K = aR$.

We prove the Theorem by induction on the number of generators of J. If $J = bR$ is principal, then $KJ = J$ means that $bK = bR$, so $b = bk$ for some $k \in K$, i.e. $(1-k)b = 0$ and $(1-k)J = \{0\}$. Suppose now that $n > 1$ and the Theorem holds for ideals J generated by less than n elements and all rings R. Let $J =< c_1, \ldots, c_n >$ be an ideal in R such that $KI = I$ for some ideal K. Consider the quotient ring R/c_nR and let π be the quotient homomorphism $\pi : R \longrightarrow R/c_nR$. Then $\pi(I)$ is an ideal of R/c_nR generated by $n-1$ elements $\pi(c_1), \ldots, \pi(c_{n-1})$ and $\pi(I)\pi(K) = \pi(IK) = \pi(I)$. Thus there is $s \in \pi(K)$ such that $(1-s)\pi(I) = \{0\}$. We have $s = \pi(l)$ for some $l \in K$. Thus $\pi((1-l)I) = \{0\}$, so $(1-l)I \subseteq \ker \pi = c_nR$. Thus $(1-l)c_i = c_nd_i$ for some $d_i \in R$, $i = 1, \ldots, n$. Since $I = KI = K < c_1, \ldots, c_n >$, we can find $k_1, \ldots, k_n \in K$ such that $c_n = k_1c_1 + \ldots + k_nc_n$. Thus $(1-l)c_n = k_1d_1c_n + \ldots + k_nd_nc_n = tc_n$, where $t = k_1d_1 + \ldots + k_nd_n \in K$. Thus $(1-l-t)c_n = 0$. It follows that $(1-l-t)(1-l)c_i = 0$ for all i. Since $t, l \in K$ we have $(1-l-t)(1-l) = 1-k$, where $k = l + t + l - (l+t)l \in K$. Thus $(1-k)I = \{0\}$.

Remark. It is not hard to conclude from the Theorem that if I is a finitely generated ideal in a commutative ring R such that $I = I^2$ then there is en idempotent $e \in I$ (i.e. $e = e^2$) such that $I = Re$.

e) We have I is finitely generated and $aI = I$ so $(1+ar)I = \{0\}$ for some $r \in R$. If $(1+ar) \in I$ then $0 = (1+ar)^2 = 1 + a(2r + ar^2)$, so a is invertible, a contradiction. Thus $1 + ar \notin I$. Clearly N is an ideal of R and $1 + ar \in N$, so N is not contained in I. The ideal $N + I$ is strictly larger than I, so it is principal: $N + I = dR$. In part b) we proved that if I is contained in a principal ideal aR then $aI = I$. Thus $dI = I$. Now $d = n + w$ for some $n \in N$ and $w \in I$. Since $nI = \{0\}$, we have $di = wi$ for all $i \in I$. Therefore $dI = wI = I$. Since $w \in R$, $I = wI \subseteq wR \subseteq I$, so $I = wR$ is principal, contrary to the definition of I. This proves that I can not be finitely generated. In other words, either I is maximal or I is not finitely generated.

f) If not all ideals in R are principal, then R has an ideal I which is maximal among non-principal ideals. Part e) tells us that I is either a maximal ideal or it is not finitely generated. The latter is not possible since R is Noetherian. The former is not possible, since we are assuming that all maximal ideals are principal. Thus I does not exist, i.e. every ideal in R is principal.