Midterm 1 Solutions

1) [20 points] Let R be a PID and I be an ideal of R. Prove that every ideal of R/I is principal. [In particular, if I is a prime ideal, then R/I is also a PID.]

Proof. Let $\bar{J}$ be an ideal of R/I. By correspondence, we have that $\bar{J} = J/I = \{a + I \ : \ a \in J\}$, for some ideal J of R. Since R is a PID, there exists $b \in R$ such that $J = (b)$.

So,

$$\bar{J} = \{a + I \ : \ a \in (b)\} = \{br + I \ : \ r \in R\} = \{(b + I)(r + I) \ : \ r + I \in R/I\} = (b + I).$$

So, $\bar{J}$ is principal, and since it was arbitrary, R/I is a PID. □

2) [20 points] Let R be a commutative ring with 1 with no non-zero nilpotent element. [So, in R, if $a^n = 0$ for some $n \in \mathbb{Z}_{>0}$, then $a = 0$]. Prove that if $f \in R[x]$ is a zero divisor in $R[x]$, then there exists $b \in R \setminus \{0\}$ such that $b \cdot f = 0$. [Note I said "$b \in R \setminus \{0\}$", not "$b \in R[x] \setminus \{0\}$".]

Proof. Let $f \sum_{i=0}^{m} a_i x^i \in R[x]$ be a nilpotent in $R[x]$. Thus, there exists $g = \sum_{i=0}^{n} b_i x^i \in F[x]$ such that $f \cdot g = 0$. Let m_0 and n_0 be the least indices such that $a_{m_0}, b_{n_0} \neq 0$. Without loss of generality, we may assume $m_0 = n_0 = 0$. [As if $(x^{m_0} f_1)(x^{n_0} g_1) = 0$, then $f_1 \cdot g_1 = 0$.]

Let $b = b_0^{m+1}$ [where $m = \deg f$]. Since $b_0 \neq 0$, we have that $b \neq 0$ by assumption. We prove, by induction on i, that $b_0^{i+1} \cdot a_i = 0$ [and hence $b \cdot a_i = b_0^{m-i} b_0^{i+1} \cdot a_i = 0$].

For $i = 0$, the result follows from the fact that the constant term of $f \cdot g$, namely $a_0 \cdot b_0$, must be zero.

Now, assume $a_j \cdot b_0^{j+1} = 0$ for all $j \in \{0, \ldots, (i-1)\}$. Thus, we also have $b_o^i a_j = 0$ for all $j \in \{0, \ldots, (i-1)\}$.

Now, look at the term of degree i in $f \cdot g$. Since this product is zero we have that

$$\sum_{j=0}^{i} a_j \cdot b_{i-j} = a_i \cdot b_0 + \sum_{j=0}^{i-1} a_j \cdot b_{i-j} = 0.$$

[Here, as usual, we have $a_j = 0$ if $j > m$ and $b_j = 0$ if $j > n$.] Multiplying by b_0^i, we get

$$a_i \cdot b_0^{i+1} + \sum_{j=0}^{i-1} a_j \cdot b_0^i \cdot b_{i-j} = 0.$$

Since $a_j \cdot b_0^i = 0$, we get that $a_i \cdot b_0^{i+1} = 0$, finishing the proof. □

3) [20 points] Prove that the quotient of a UFD by a prime ideal might not be a UFD. [**Hint:** We don't know many non-UFDs, so take a look at those!]

Proof. As we have seen, $\mathbb{Z}[\sqrt{-5}]$ is a domain, but not a UFD [as $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, and all 2, 3, $1 \pm \sqrt{-5}$ are irreducible].

Now, the minimal polynomial of $\sqrt{-5}$ is $x^2 + 5$ and so $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]/(x^2 + 5)$. Since $\mathbb{Z}[x]$ is a UFD [since $\mathbb{Z}$ is and if R is a UFD, then so is $R[x]$], this gives us our example. □

4) [20 points] Let F, K_1, K_2 and L be fields with $F \subseteq K_i \subseteq L$ for $i = 1, 2$.

(a) Prove that the intersection of all subfields of L containing both K_1 and K_2 is a field. [This field is called the *compositum of* K_1 *and* K_2 and it is denoted by $K_1 \cdot K_2$ or $K_1\, K_2$. It is clearly the minimal common extension of K_1 and K_2.]

Proof. Let $K_1 K_2$ be this intersection and $\alpha, \beta \in K_1 K_2$. Then, for *any* subfield E of L containing the K_i, we have that $\alpha, \beta \in E$. Since E is a field, we have that $\alpha \pm \beta$, $\alpha \cdot \beta$ and α/β, if $\beta \neq 0$, are all in E. So, they are also in $K_1 K_2$. □

(b) Prove that $K_1 \cdot K_2$ is the set of all $f(\alpha_1, \ldots, \alpha_k)$, with $f \in F(x_1, \ldots, x_k)$, for some $k \in \mathbb{Z}_{>0}$, defined at $(\alpha_1, \ldots, \alpha_k)$ [i.e., the denominator of the rational function $f(x_1, \ldots, x_k)$ does not vanish at $(\alpha_1, \ldots, \alpha_k)$] and $\alpha_i \in K_1 \cup K_2$ for all i.

Proof. It's easy to see that the set described above, call it K', is a field containing both K_i's. So, $K_1 K_2 \subseteq K'$. But also, any field containing both K_i's [and so also F] contains K'. Hence, they are equal. □

(c) Prove that if K_1 and K_2 are both algebraic over F, then $K_1 \cdot K_2$ [as above] is also algebraic over F.

Proof. Let $\alpha \in K_1 K_2$. By (b) we have that

$$\alpha = \frac{f(\alpha_1, \ldots, \alpha_r)}{g(\beta_1, \ldots, \beta_s)}, \qquad f \in F[x_1, \ldots, x_r],\ g \in F[x_1, \ldots, x_s],\ \alpha_i, \beta_j \in K_1 \cup K_2.$$

Then, $\alpha \in E \stackrel{\text{def}}{=} F[\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s]$. Since each α_i and β_j are either in K_1 or K_2 [both algebraic extensions of F], we have that each α_i and β_j is algebraic, and hence $F[\alpha_i]/F$ and $F[\beta_j]/F$ are finite extensions. So, $E/F = F[\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s]/F$ is finite [of degree less than or equal to the product of $[F[\alpha_i] : F]$ and $[F[\beta_j] : F]$ for all i and j.] Since $\alpha \in E$, this means that α is algebraic over F.

Since α was arbitrary, $K_1 K_2/F$ is algebraic. □

5) [20 points] Let p be a prime, $q = p^r$ for some $r \in \mathbb{Z}_{>0}$, and $\mathbb{F}_q$ be the finite field with q elements [in some fixed algebraic closure of $\mathbb{F}_p$]. Prove that if $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$, then there exists some $t \in \mathbb{Z}_{>0}$ such that $\sigma(\alpha) = \alpha^t$ for all $\alpha \in \mathbb{F}_q$ and $\gcd(t, q-1) = 1$. [It is true, in fact, that t must be a power of p, but you don't need to show that.]

Proof. Remember that since $\mathbb{F}_q$ is a finite field, we have that $\mathbb{F}_q^\times = \langle \alpha \rangle$ [for some $\alpha \in \mathbb{F}_q$]. Since $\alpha \neq 0$, we have that $\sigma(\alpha) \neq 0$, i.e., $\sigma(\alpha) \in \mathbb{F}_q^\times = \langle \alpha \rangle$. Thus, $\sigma(\alpha) = \alpha^t$ for some $r \in \{1, 2, \ldots, (q-1)\}$. Since σ is onto and only 0 is sent to 0 by σ, we have that σ induces an automorphism for the *group* $\mathbb{F}_q^\times$. Since it has to be onto, we must have that $\sigma(\alpha) = \alpha^t$ must be another generator of $\mathbb{F}_q^\times$, and hence $\gcd(t, q-1) = 1$ [from group theory]. $\square$