Math 120B: Sample Final Solutions

Closed book, closed notes, no calculators. Each problem is worth 10 points. Time: 80 minutes. Please explain your solutions. Just giving an answer is not enough.

1. Suppose that $I \subset \mathbb{Z}[x]$ is an ideal and there is a prime $p \in \mathbb{Z}$ which is in I. Show that I can be generated by two elements, i.e. there exists $z \in I$ such that $I = \{r_1 p + r_2 z | r_1, r_2 \in \mathbb{Z}[x]]\}$.

   Solution: Let $\phi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ be the ring homomorphism that reduces coefficients modulo p and let $J = \phi(I)$. Since ϕ is surjective, J in an ideal in $\mathbb{Z}_p[x]$ and thus it is generated by a polynomial $g(x) \in \mathbb{Z}_p[x]$. Let $f(x) \in I$ be any polynomial that maps to $g(x)$.

   We claim that I is generated by p and $f(x)$. Indeed, since p and $f(x)$ are in I, all their linear combinations are also in I. On the other hand, take $h(x) \in I$. Since $\phi(h(x)) \in J = (g(x))$ we have $\phi(h(x)) = g(x)a(x)$. If $b(x)$ is any polynomial that maps to $a(x)$ then $h(x) - f(x)b(x)$ maps to zero. Hence $h(x) - f(x)b(x) \in Ker(\phi)$ is a multiple of p which makes $h(x)$ a linear combination of p and $f(x)$, as required.

2. Is it true that the intersection of two prime ideals is always a prime ideal? Explain.

   Solution: No. If $P_1 \subset \mathbb{Z}$ is the prime ideal of integers divisible by 3 and P_2 of integers divisible by 2, then $Q = P_1 \cap P_2$ is the ideal of all integers divisible by 6. But Q is not prime since 6 is in Q but neither 3 nor 2 is in Q.

3. Let F be a field and assume that $R = F[x]/(f(x))$ is an integral domain for some polynomial $f(x)$. Show that in fact R is a field.

   Solution: If $F[x]/(f(x))$ is an integral domain then $(f(x))$ is a prime ideal. Since it is nonzero and $F[x]$ is a Euclidean Domain, the same ideal is also maximal. But then the quotient R is a field.

4. Let $F \subset E$ be a field extension of finite degree and assume that the degree $[E : F] = p$ is a prime. Show that for any $\alpha \in E$ either $F(\alpha) = F$ or $F(\alpha) = E$.

Solution: We have a chain of embedded fields $F \subset F(\alpha) \subset E$ and hence $p = [E : F] = [E : F(\alpha)][F(\alpha) : F]$. Since p is prime, either $[E : F(\alpha)]$ or $[F(\alpha) : F]$ is equal to 1. In the first case $E = F(\alpha)$, in the second $F(\alpha) = F$.

5. Let $f_1, f_2 \in F[x]$ be two polynomials (and F is a field). Let $g = gcd(f_1, f_2)$. Show that the ideal I generated by f_1, f_2 (i.e.

$$I = \{h_1 f_1 + h_2 f_2 \quad | \quad h_1, h_2 \in F[x]\}$$

satisfies $I = (g(x))$.

Solution. Denote temporarily $J = (g(x))$. Since $g(x)$ divides both f_1 and f_2, it will divide any linear combination of f_1 and f_2. Hence J contains I. On the other hand, by extended Euclidean Division Algorithm we can write $g(x) = a(x)f_1(x)+b(x)f_2(x)$ hence any multiple of $g(x)$ can be re-written as a linear combination of $f_1(x), f_2(x)$ which means that also I contains J. Therefore $I = J$.

6. Construct a field with 32 elements. Prove that what you have constructed indeed has 32 elements and that it is indeed a field.

Solution If $g(x)$ is any irreducible polynomial in $\mathbb{Z}_2[x]$ of degree 2 then $F = \mathbb{Z}_2[x]/(g(x))$ is a field and as s vector space over $\mathbb{Z}_2$ it has dimension 5 (because it has basis $1, x, x^2, x^3, x^4$. Since the coefficients of basis vectors are taken from $\mathbb{Z}_2$, there will be a total of $2^5 = 32$ elements. It remains to give an explicit example of an irreducible degree 5 polynomial. Note that if a degree 5 polynomial is reducible, it must have some irreducible factor of degree 1 (in which case it will have a root) or an irreducible factor of degree 2. In $\mathbb{Z}_2$ only $x^2 + x + 1$ is irreducible of degree 2. So we are looking for $g(x)$ of degree 5 which is not divisible by $x, x+1, x^2+x+1$. There are quite a few possibilities, e.g. $x^5 + x^4 + x^3 + x + 1$.

Thus, one possible model for a field with 32 elements in $\mathbb{Z}_2[x]/(x^5 + x^4 + x^3 + x + 1)$.